

HP FlexFabric 5700 Switch Series

Fundamentals

Configuration Guide

Part number: 5998-6678

Software version: Release 2416

Document version: 6W100-20150130



Legal and notice information

© Copyright 2015 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	4
Entering a text or string type value for an argument	4
Abbreviating commands	4
Configuring and using command keyword aliases	5
Configuring and using command hotkeys	5
Enabling redisplaying entered-but-not-submitted commands	6
Understanding command-line error messages	7
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	12
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	17
CLI overview	17
User lines	17
Login authentication modes	18
User roles	18
FIPS compliance	19
Logging in through the console port locally	19
Disabling authentication for console login	19
Configuring password authentication for console login	20
Configuring scheme authentication for console login	21
Configuring common AUX line settings	21
Logging in through Telnet	23
Configuring Telnet login on the device	24
Using the device to log in to a Telnet server	29
Logging in through SSH	30
Configuring SSH login on the device	30
Using the device to log in to an SSH server	32
Logging in through a pair of modems	32
Displaying and maintaining CLI login	35

Accessing the device through SNMP	37
Controlling user access.....	38
FIPS compliance	38
Controlling Telnet/SSH logins	38
Configuration procedures.....	38
Configuration example	39
Controlling SNMP access.....	39
Configuration procedure	39
Configuration example	40
Configuring command authorization	41
Configuration procedure	41
Configuration example	42
Configuring command accounting.....	44
Configuration procedure	44
Configuration example	45
Configuring RBAC.....	47
Overview.....	47
Permission assignment	47
Assigning user roles	49
FIPS compliance	50
Configuration task list.....	50
Creating user roles.....	50
Configuring user role rules.....	51
Configuration restrictions and guidelines	51
Configuration procedure	52
Configuring feature groups.....	52
Configuring resource access policies	53
Configuring the interface policy of a user role	53
Configuring the VLAN policy of a user role	53
Assigning user roles.....	54
Enabling the default user role feature	54
Assigning user roles to remote AAA authentication users	54
Assigning user roles to local AAA authentication users	55
Assigning user roles to non-AAA authentication users on user lines	55
Configuring temporary user role authorization	56
Configuration guidelines	56
Configuring user role authentication	58
Obtaining temporary user role authorization	58
Displaying RBAC settings	59
RBAC configuration examples.....	59
RBAC configuration example for local AAA authentication users	59
RBAC configuration example for RADIUS authentication users	61
RBAC temporary user role authorization configuration example (HWTACACS authentication)	64
RBAC temporary user role authorization configuration example (RADIUS authentication)	68
Troubleshooting RBAC.....	71
Local users have more access permissions than intended	71
Login attempts by RADIUS users always fail	71
Configuring FTP.....	73
FIPS compliance	73
Using the device as an FTP server.....	73
Configuring basic parameters	74
Configuring authentication and authorization	74
Manually releasing FTP connections	75

Displaying and maintaining the FTP server	75
FTP server configuration example	75
Using the device as an FTP client	77
Establishing an FTP connection	77
Managing directories on the FTP server	78
Working with files on the FTP server	78
Changing to another user account	79
Maintaining and troubleshooting the FTP connection	80
Terminating the FTP connection	80
Displaying command help information	80
Displaying and maintaining FTP client	81
FTP client configuration example	81
Configuring TFTP	83
FIPS compliance	83
Configuring the device as an IPv4 TFTP client	83
Configuring the device as an IPv6 TFTP client	84
Managing the file system	85
FIPS compliance	85
Storage medium naming rules	85
File name formats	85
Managing files	86
Displaying file information	86
Displaying the contents of a text file	87
Renaming a file	87
Copying a file	87
Moving a file	87
Compressing/decompressing a file	87
Archiving/extracting files	88
Deleting/restoring a file	88
Deleting files from the recycle bin	88
Calculating the file digest	89
Managing directories	89
Displaying directory information	89
Displaying the current working directory	89
Changing the current working directory	89
Creating a directory	90
Removing a directory	90
Managing storage media	90
Repairing a storage medium	91
Formatting a storage medium	91
Mounting or unmounting a storage medium	91
Partitioning a USB disk	92
Setting the operation mode for files and folders	92
Managing configuration files	94
Overview	94
Configuration types	94
Startup configuration loading process	95
Configuration file formats	96
Startup configuration file selection	96
Configuration file content organization and format	96
FIPS compliance	97
General configuration restrictions and guidelines	97
Enabling configuration encryption	97

Saving the running configuration	98
Restrictions and guidelines	98
Using different methods to save the running configuration	98
Configuring configuration rollback	99
Configuration task list	99
Configuring configuration archive parameters	100
Enabling automatic configuration archiving	100
Manually archiving the running configuration	101
Rolling back configuration	101
Specifying a next-startup configuration file	102
Backing up the main next-startup configuration file to a TFTP server	103
Restoring the main next-startup configuration file from a TFTP server	103
Deleting a next-startup configuration file	104
Displaying and maintaining configuration files	104
Upgrading software	106
Overview	106
Software types	106
Software file naming conventions	106
Comware image redundancy and loading procedure	107
System startup process	107
Upgrade methods	108
Upgrade procedure summary	109
Upgrade restrictions and guidelines	109
Preparing for the upgrade	109
Preloading the Boot ROM image to Boot ROM	110
Specifying the startup image file and completing the upgrade	110
Specifying the startup image file for all devices in bulk	110
Specifying the startup image file for devices one by one	111
Upgrading software by performing a warm reboot	112
Displaying and maintaining software image settings	112
Non-ISSU software upgrade examples	113
Example of software upgrade through a reboot	113
Example of software upgrade through a warm reboot	114
Performing an ISSU	115
ISSU overview	115
ISSU methods	115
ISSU commands	116
Verifying the device operating status	116
Preparing the upgrade images	116
Identifying the ISSU method	116
Verifying feature status	117
Determining the upgrade procedure	117
Understanding ISSU guidelines	118
Logging in to the device through the console port	118
Saving the running configuration	118
Performing an ISSU by using issu commands	118
Upgrading a multichassis IRF fabric	118
Upgrading a single-chassis IRF fabric	120
Performing an ISSU by using install commands	121
ISSU task list	121
Decompressing an .ipe file	122
Installing or upgrading software images	122
Uninstalling feature or patch images	123

Rolling back the running software images	123
Aborting a software activate/deactivate operation	124
Committing software changes	124
Verifying software images	124
Removing inactive software images	124
Displaying and maintaining ISSU	125
Troubleshooting ISSU	125
Failure to execute the issu load/issu run switchover/issu commit/install activate/install deactivate command	125
ISSU examples for using issu commands	126
Software image upgrade to a compatible version	126
Software image upgrade to an incompatible version	128
Software image rollback example	130
ISSU examples for using install commands	132
Software image upgrade example	132
Software image rollback example	135
Software image patching example	136
Using the emergency shell	138
Managing the file system	138
Obtaining a system image from an FTP/TFTP server	139
Configuring the management Ethernet interface	139
Checking the connectivity to a server	140
Accessing the server	140
Loading the system image	141
Rebooting the device	142
Displaying device information in emergency shell mode	142
Emergency shell usage example	142
Network requirements	142
Usage procedure	143
Managing the device	145
Device management task list	145
Configuring the device name	145
Configuring the system time	146
Specifying the system time source	146
Setting the system time	146
Enabling displaying the copyright statement	147
Configuring banners	147
Banner types	147
Banner input modes	147
Configuration procedure	148
Setting the system operating mode	149
Rebooting the device	150
Configuration guidelines	150
Rebooting devices immediately at the CLI	150
Scheduling a device reboot	150
Scheduling a task	151
Configuration guidelines	151
Configuration procedure	151
Schedule configuration example	153
Disabling password recovery capability	156
Specifying the preferred airflow direction	157
Setting the port status detection timer	157
Configuring CPU usage monitoring	157

Setting memory thresholds	158
Configuring the temperature alarm thresholds	159
Disabling all USB interfaces	160
Verifying and diagnosing transceiver modules	161
Verifying transceiver modules	161
Diagnosing transceiver modules	161
Restoring the factory-default settings and states	161
Displaying and maintaining device management configuration	162
Using Tcl	164
Tcl usage guidelines and restrictions	164
Entering Tcl configuration view from user view	164
Returning from Tcl configuration view to user view	164
Executing Comware commands in Tcl configuration view	165
Using Python	166
Entering the Python shell	166
Executing a Python script	166
Python usage example	166
Comware V7 extended Python API	168
Importing and using the Comware V7 extended Python API	168
Comware V7 extended Python API functions	168
CLI class	168
Transfer class	170
API get_self_slot	171
API get_standby_slot	171
Using automatic configuration	173
Overview	173
Automatic configuration task list	173
Configuring the file server	174
Preparing the files for automatic configuration	174
Configuring the DHCP server	175
Configuring the DNS server	176
Configuring the gateway	177
Selecting the interfaces used for automatic configuration	177
Starting and completing automatic configuration	177
Automatic configuration examples	177
Automatic configuration using TFTP server	177
Automatic configuration using HTTP server and Tcl script	182
Automatic configuration using HTTP server and Python script	183
Automatic IRF setup	184
Support and other resources	188
Contacting HP	188
Subscription service	188
Related information	188
Documents	188
Websites	188
Conventions	189
Index	191

Using the CLI

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

Figure 1 CLI example

```
*****
* Copyright (c) 2010-2014 Hewlett-Packard Development Company, L.P.      *
* Without the owner's prior written consent,                             *
* no decompiling or reverse-engineering shall be allowed.                 *
*****

<Sysname>
```

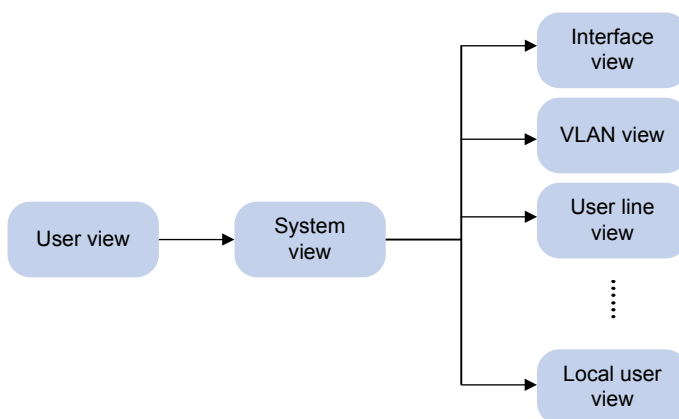
You can use different methods to log in to the CLI, including through the console port, Telnet, and SSH. For more information about login methods, see "[Login overview](#)."

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 2](#). 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 2 CLI views



You are placed in user view immediately after you log in to the CLI. The user view prompt is <Device-name>, where *Device-name* indicates the device name. The device name is **Sysname** by default. You can change it by using the **sysname** command.

In user view, you can perform the following tasks:

- Perform basic operations including display, debug, file management, FTP, Telnet, clock setting, and reboot.
- Enter system view. The system view prompt is *[Device-name]*.

In system view, you can perform the following tasks:

- Configure global settings (such as the daylight saving time, banners, and hotkeys) and some functions.
- Enter different function views. For example, you can perform the following tasks:
 - Enter interface view to *configure* interface parameters.
 - Enter VLAN view to add ports to the VLAN.
 - Enter user line view to configure login user attributes.

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.

In public key view, use the **peer-public-key end** command to return to system view.

Returning to user view

To return directly to user view from any other view, use the **return** command or press **Ctrl+Z**.

Task	Command
Return directly to user view.	return

Accessing the CLI online help

The CLI online help is context sensitive. 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	Software image file management

...

- 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 ?
  debugging  Enable to display debugging logs on the current 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 for 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> q?
quit
<Sysname> display ftp?
ftp
ftp-server
ftp-user
```

Using the undo form of a command

Most configuration commands have an **undo** form for the following tasks:

- Canceling a configuration.
- Restoring the default.
- Disabling a feature.

For example, the **info-center enable** command enables the information center. The **undo info-center enable** command disables the information center.

Entering a command

When you enter a command, you can perform the following tasks:

- Use keys or hotkeys to edit the command line.
- 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.

A command line can have up to 512 characters, including keywords, arguments, spaces, and special characters.

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 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.
Right arrow key (→)	Moves the cursor one character to the right.
Up arrow key (↑)	Displays the previous command in the command history buffer.
Down arrow key (↓)	Displays the next command in the command history buffer.
Tab	If you press Tab after entering part of a keyword, the system automatically completes the keyword. • If a unique match is found, the system displays the complete keyword. • 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 text or string type value for an argument

A text type argument value can contain printable characters other than the question mark (?).

A string type argument value can contain any printable characters except for the following characters:

- Question mark (?).
- Quotation mark (").
- Backward slash (\).
- Space.

A specific argument might have more requirements. For more information, see the relevant command reference.

To enter a printable character, you can enter the character or its ASCII code (in the range of 32 to 126).

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 use your own keywords to replace the following keywords when you execute a command:

- The first keywords of non-undo commands.
- The second keywords of **undo** commands.

For example, if you configure the alias **show** 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

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 you are using to interact with the device, the terminal software definition 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	The following are the defaults: • 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	This command is 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.
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 from the cursor to the end of the line.
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.

Enabling redisplaying entered-but-not-submitted commands

Your input might be interrupted by system information output. If redisplaying entered-but-not-submitted commands is enabled, the system redisplay your input after finishing the output. You can then 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 examines the command syntax.

- If the command passes syntax check, the CLI executes the command.
- If the command fails syntax check, 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 the following two command history buffers:

- Command history buffer for the user line.
- Command history buffer for all user lines.

Table 4 Comparison between the two types of command history buffers

Item	Command history buffer for a user line	Command history buffer for all user lines
What kind of commands are saved in the buffer?	Commands successfully executed by the current user of the user line.	Commands successfully executed by all login users.
Cleared when the user logs out?	Yes.	No.

Item	Command history buffer for a user line	Command history buffer for all user lines
How to view buffered commands?	Use the display history-command command.	Use the display history-command all command.
How to recall buffered commands?	- Navigate to the command in the buffer: - In Windows 200x or Windows XP HyperTerminal or Telnet, use the up or down arrow key (↑ or ↓). - In Windows 9x HyperTerminal, use Ctrl+P and Ctrl+N. - Press Enter.	You cannot call buffered commands.
How to set the buffer size?	Use the history-command max-size size-value command in user line 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 in different formats multiple times, 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 identify the desired output.

Pausing between screens of output

The system automatically pauses after displaying a screen if the output is too long to fit on one 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 limit 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 final 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	By default, a session uses the screen-length <i>screen-length</i> command settings in user line view. 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.

Each line number is displayed as a 5-character string and might be followed by a colon (:) or hyphen (-). If you specify both | **by-linenum** and | **begin** *regular-expression* for a **display** command, a hyphen is displayed for all lines that do not match the regular expression.

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 system time information, numbering each output line.
```

```
<Sysname> display clock | by-linenum
```

```
1: 06:14:21 UTC Sat 01/01/2011
```

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](#).

The required filtering time increases with the complexity of the regular expression. To abort the filtering process, press **Ctrl+C**.

Table 5 Special characters supported in a regular expression

Characters	Meaning	Examples
<code>^</code>	Matches the beginning of a line.	" <code>^u</code> " matches all lines beginning with "u". A line beginning with "Au" is not matched.
<code>\$</code>	Matches the end of a line.	" <code>u\$</code> " matches all lines ending with "u". A line ending with "uA" is not matched.
<code>.</code> (period)	Matches any single character.	" <code>.s</code> " matches "as" and "bs".
<code>*</code>	Matches the preceding character or string zero, one, or multiple times.	" <code>zo*</code> " matches "z" and "zoo", and "(<code>zo</code>)*" matches "zo" and "zozo".
<code>+</code>	Matches the preceding character or string one or multiple times.	" <code>zo+</code> " matches "zo" and "zoo", but not "z".
<code> </code>	Matches the preceding or succeeding string.	" <code>def int</code> " matches a line containing "def" or "int".
<code>()</code>	Matches the string in the parentheses, usually used together with the plus sign (+) or asterisk sign (*).	"(<code>123A</code>)" matches "123A". " <code>408(12)+</code> " matches "40812" and "408121212", but not "408".
<code>\N</code>	Matches the preceding strings in parentheses, with the <i>N</i> th string repeated once.	"(<code>string</code>)\1" matches a string containing "stringstring". "(<code>string1</code>)(<code>string2</code>)\2" matches a string containing "string1string2string2". "(<code>string1</code>)(<code>string2</code>)\1\2" matches a string containing "string1string2string1string2".
<code>[]</code>	Matches a single character in the brackets.	" <code>[16A]</code> " matches a string containing 1, 6, or A; " <code>[1-36A]</code> " matches a string containing 1, 2, 3, 6, or A (- is a hyphen). To match the character "]", put it immediately after "[", for example, <code>[abc]</code> . There is no such limit on "[".
<code>[^]</code>	Matches a single character that is not in the brackets.	" <code>[^16A]</code> " matches a string that contains one or more characters except for 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).
<code>{n}</code>	Matches the preceding character <i>n</i> times. The number <i>n</i> must be a nonnegative integer.	" <code>o{2}</code> " matches "food", but not "Bob".
<code>{n,}</code>	Matches the preceding character <i>n</i> times or more. The number <i>n</i> must be a nonnegative integer.	" <code>o{2,}</code> " matches "fooooood", but not "Bob".

Characters	Meaning	Examples
{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 a string that starts with the pattern following \<. A string that contains the pattern is also a match if the characters preceding the pattern are not digits, letters, or underscores.	"\<do" matches "domain" and "doa".
\>	Matches a string that ends with the pattern preceding \>. A string that contains the pattern is also a match if the characters following the pattern are not digits, letters, or underscores.	"do\">" matches "undo" and "cdo".
\b	Matches a word that starts with the pattern following \b or ends with the pattern preceding \b.	"er\b" matches "never", but not "verb" or "erase". "\ber" matches "erase", but not "verb" or "never".
\B	Matches a word that contains the pattern but does not start or end with the pattern.	"er\B" matches "verb", but not "never" or "erase".
\w	Same as [A-Za-z0-9_], matches a digit, letter, or underscore.	"v\w" matches "vlan" and "service".
\W	Same as [^A-Za-z0-9_], matches a character that is not a digit, letter, or underscore.	"\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 line** for the **display current-configuration** command to match the first line of output that contains **line** to the last line of output.

```
<Sysname> display current-configuration | begin line
line class aux
    user-role network-admin
#
line class vty
    user-role network-operator
#
line aux 0
    user-role network-admin
#
line vty 0 63
    authentication-mode scheme
    user-role network-operator
#
```

```

ssh server enable
#
return
# Use | include snmp for 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 <i>command</i> > <i>filename</i>
Append the output from a display command to the end of a file.	display <i>command</i> >> <i>filename</i>

For example:

Save system time information to a separate file named **clock.txt**.

```
<Sysname> display clock > clock.txt
```

Verify that the system time information is saved to file **clock.txt**.

```
<Sysname> more clock.txt
```

```
06:03:58 UTC Sat 01/01/2014
```

Append system time information to the end of file **clock.txt**.

```
<Sysname> display clock >> clock.txt
```

Verify that the system time information is appended to the end of file **clock.txt**.

```
<Sysname> more clock.txt
```

```
06:03:58 UTC Sat 01/01/2014
```

```
06:04:58 UTC Sat 01/01/2014
```

Viewing and managing the output from a display command effectively

You can use the following methods 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
```

Display the first line that begins with **user-group** in the running configuration and all the following lines.

```
<Sysname> display current-configuration | by-linenum begin user-group
```

```
114: user-group system
```

```
115- #
```

```
116- return
```

Saving the running configuration

To make your configuration take effect after 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 **display** commands used for displaying information and **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 log in to the CLI through the console port. After login, you can change console login parameters or configure other access methods, including Telnet, SSH, modem, and SNMP.

Telnet login is not supported in FIPS mode.

Table 6 Login methods at a glance

Login method	Default settings and minimum configuration requirements
Logging in to the CLI:	
Logging in through the console port locally	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.
Logging in through Telnet	By default, Telnet login is disabled. To enable Telnet login, perform the following tasks: - Enable the Telnet server function. - Assign an IP address to a Layer 3 interface and make sure the interface and the Telnet client can reach each other. - Configure an authentication mode for VTY login users. By default, password authentication is used but no password is configured. - Assign a user role to VTY login users (network-operator by default).
Logging in through SSH	By default, SSH login is disabled. To enable SSH login, perform the following tasks: - Enable the SSH server function and configure SSH attributes. - Assign an IP address to a Layer 3 interface and make sure the interface and the SSH client can reach each other. - Configure scheme authentication for VTY login users (password authentication by default). - Assign a user role to VTY login users (network-operator by default).
Logging in through a pair of modems	By default, modem dial-in is enabled, and you can dial in to the switch. The default user role is network-admin.
Accessing the device through SNMP	By default, SNMP access is disabled. To enable SNMP access, perform the following tasks: - Assign an IP address to a Layer 3 interface, and make sure the interface and the NMS can reach each other. - Configure SNMP basic parameters.

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). Make sure the console terminal has a terminal emulation program, such as HyperTerminal on Windows XP. On Windows Server 2003, you must manually add the HyperTerminal program. On Windows Server 2008, Windows 7, Windows Vista, or other operating systems, you must obtain and install a third-party terminal emulation program. For information about how to use other terminal emulation programs, see the programs' user guides or online help.

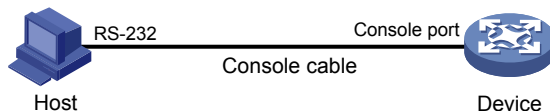
To log in through the console port:

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

! IMPORTANT:

The serial ports on PCs do not support hot swapping. To connect a PC to an operating switch, first connect the PC end. To disconnect a PC from an operating switch, first disconnect the switch end.

Figure 3 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 and create a connection that uses the serial port connected to the device. 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.
5. Power on the device and press **Enter** as prompted.

The default user view prompt <HP> appears. You can enter commands to configure or manage the device. To get help, enter **?**.

```
Press Ctrl-B to enter Boot Menu    0
Auto-booting
Decompress Image
```

OK!

Starting at 0x80100000

Cryptographic algorithms tests passed.

User interface aux0 is available.

Press ENTER to get started.

<HP>%Sep 24 09:48:54:109 2014 HP SHELL/4/LOGIN: Console login from aux0

<HP>

Logging in to the CLI

By default, you can log in to the CLI through the console port. After you log in, you can configure other login methods, including Telnet, SSH, and modem dial-in.

To prevent illegal access to the CLI and control user behavior, perform the following tasks as required:

- Configure login authentication.
- Assign user roles.
- Configure command authorization and command accounting.
- 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 line settings. For more information about command authorization, command accounting, and unauthorized access filtering, see "[Controlling user access](#)."

CLI overview

User lines

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

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

Table 7 CLI login method and user line matrix

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

User line assignment

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

For a CLI login, the device always picks the lowest numbered user line from the idle user lines available for the login type. For example, four VTY lines (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 line identification

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

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

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

Login authentication modes

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

In non-FIPS mode, the device supports the following login authentication modes:

- **None**—Disables authentication. This mode allows access without authentication and 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.

In FIPS mode, the device supports only the scheme authentication mode.

Different login authentication modes require different user line configurations, 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	1. Set the authentication mode to scheme. 2. Configure login authentication methods in ISP domain view. For more information, see <i>Security Configuration Guide</i>.

User roles

A user is assigned user roles at login. The user roles specify the commands that the user can execute. For more information about user roles, see "[Configuring RBAC](#)."

The device assigns user roles based on the login authentication mode, user type, and login method.

- In **none** or **password** authentication mode, the device assigns the user roles specified for the user line.
- In **scheme** authentication mode, the device uses the following rules to assign user roles:
 - For an SSH login user who uses publickey or password-publickey authentication, the device assigns the user roles specified for the local device management user with the same name.
 - For other users, the device assigns user roles according to the user role configuration of the AAA module. If the AAA server does not assign any user roles and the default user role function is disabled, a remote AAA authentication user cannot log in.

FIPS compliance

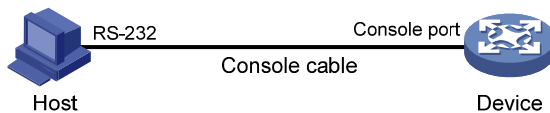
The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

Telnet login is not supported in FIPS mode.

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 4](#). For the login procedure, see "[Logging in through the console port for the first device access](#)."

Figure 4 Logging in through the console port



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

To configure console login, perform the following tasks:

Task	Remarks
(Required.) Configuring login authentication: • Disabling authentication for console login • Configuring password authentication for console login • Configuring scheme authentication for console login	Configure one authentication mode as required. In FIPS mode, only the scheme authentication mode is supported.
(Optional.) Configuring common AUX line settings	N/A

Console login configuration changes do not take effect for current online users. They take effect only for new login users.

Before using multiple devices to form an IRF fabric, enter AUX line class view on each device and perform the following tasks:

- Disable authentication.
- Assign the user role network-admin.

Disabling authentication for console login

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

Step	Command	Remarks
2. Enter AUX line view or class view.	- Enter AUX line view: line aux <i>first-number</i> [<i>last-number</i>] - Enter AUX line class view: line class aux	A setting in user line view is applied only to the user line. A setting in user line class view is applied to all user lines of the class. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view. A setting in user line view takes effect immediately and affects the online user. A setting in user line class view does not affect online users and takes effect only for new login users.
3. Disable authentication.	authentication-mode none	By default, authentication is disabled for the AUX line.
4. Assign a user role.	user-role <i>role-name</i>	By default, an AUX line user is assigned the user role network-admin .

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

Configuring password authentication for console login

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter AUX line view or class view.	- Enter AUX line view: line aux <i>first-number</i> [<i>last-number</i>] - Enter AUX line class view: line class aux	A setting in user line view is applied only to the user line. A setting in user line class view is applied to all user lines of the class. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view. A setting in user line view takes effect immediately and affects the online user. A setting in user line class view does not affect online users and takes effect only for new login users.
3. Enable password authentication.	authentication-mode password	By default, authentication is disabled for the AUX line.
4. Set a password.	set authentication password { hash simple } <i>password</i>	By default, no password is set.
5. Assign a user role.	user-role <i>role-name</i>	By default, an AUX line user is assigned the user role network-admin .

The next time you 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 line view or class view.	- Enter AUX line view: line aux <i>first-number</i> [<i>last-number</i>] - Enter AUX line class view: line class aux	A setting in user line view is applied only to the user line. A setting in user line class view is applied to all user lines of the class. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view. A setting in user line view takes effect immediately and affects the online user. A setting in user line class view does not affect online users and takes effect only for new login users.
3. Enable scheme authentication.	authentication-mode scheme	By default, authentication is disabled for the AUX line.

To use scheme authentication, you must also perform the following tasks:

- Configure login authentication methods in ISP domain view.
- To use remote authentication, configure the scheme to be used.
- To use local authentication, configure a local user and the relevant attributes.

For more information, see Security Configuration Guide.

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

Configuring common AUX line settings

Some common settings configured for an AUX line take effect immediately and can interrupt the current session. Use a login method different from console login to log in to the device before you change AUX line settings.

To log in through the console port after you configure AUX line settings, change the terminal settings on the configuration terminal to match the line settings.

To configure common settings for an AUX line:

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

Step	Command	Remarks
2. Enter AUX line view or class view.	- Enter AUX line view: line aux <i>first-number</i> [<i>last-number</i>] - Enter AUX line class view: line class aux	A setting in user line view is applied only to the user line. A setting in user line class view is applied to all user lines of the class. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view. A setting in user line view takes effect immediately and affects the online user. A setting in user line class view does not affect online users and takes effect only for new login users.
3. Set the baud rate.	speed <i>speed-value</i>	By default, the baud rate is 9600 bps. This command is not available in AUX line class view.
4. Specify the parity check mode.	parity { even mark none odd space }	By default, the parity check mode is none, and no parity check is performed. This command is not available in AUX line class view.
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. This command is not available in AUX line class view.
6. Specify the number of data bits for each character.	databits { 5 6 7 8 }	The default is 8. Configure this command depending the character coding type. For example, set the number of data bits to 7 for standard ASCII characters. Set the number of data bits to 8 for extended ASCII characters. This command is not available in AUX line class view.
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 }	This command is not available in AUX line class view. By default, the flow control mode is none.

Step	Command	Remarks
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. HP recommends that you set the display type to VT100 on both the device and the configuration terminal. If either side uses the ANSI type, a display problem such as cursor positioning error might occur when a command line has more than 80 characters.
11. Set the maximum number of lines to be displayed on a screen.	screen-length <i>screen-length</i>	By default, a screen displays up to 24 lines. 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 up to 10 history commands.
13. Set the session idle timeout.	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, the system automatically terminates the user connection on the user line. If you set the idle timeout 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 perform the following tasks:

- Log in to the device through any other method.
- Enable the Telnet server.
- Configure Telnet login authentication on the device.

NOTE:

Telnet login is not supported in FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

Configuring Telnet login on the device

Task	Remarks
(Required.) Configuring login authentication: - Disabling authentication for Telnet login - Configuring password authentication for Telnet login - Configuring scheme authentication for Telnet login	Configure one authentication mode as required.
(Optional.) Setting the maximum number of concurrent Telnet users	N/A
(Optional.) Setting the DSCP value for outgoing Telnet packets	N/A
(Optional.) Configuring common VTY line settings	N/A

Telnet login configuration changes do not take effect for current online users. They take effect only for new login users.

Disabling 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 VTY line view or class view.	- Enter VTY line view: line vty <i>first-number</i> [<i>last-number</i>] - Enter VTY line class view: line class vty	A setting in user line view is applied only to the user line. A setting in user line class view is applied to all user lines of the class. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view. A setting in user line view takes effect immediately and affects the online user. A setting in user line class view does not affect online users and takes effect only for new login users.
4. Disable authentication.	authentication-mode none	By default, password authentication is enabled for VTY lines. In VTY line view, this command is associated with the protocol inbound command. If you specify a non-default value for only one of the two commands in VTY line view, the other command uses the default setting, regardless of the setting in VTY line class view.
5. (Optional.) Assign a user role.	user-role <i>role-name</i>	By default, a VTY line user is assigned the user role network-operator .

The next time you Telnet to the device, you do not need to provide a username or password, as shown in [Figure 5](#). If the maximum number of login users has been reached, your login attempt fails and the message "All user lines are used, please try later!" appears.

Figure 5 Telnetting to the device without authentication

```
*****
* Copyright (c) 2010-2014 Hewlett-Packard Development Company, L.P.      *
* Without the owner's prior written consent,                             *
* no decompiling or reverse-engineering shall be allowed.                 *
*****

<Sysname>
```

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 VTY line view or class view.	- Enter VTY line view: line vty <i>first-number</i> [<i>last-number</i>] - Enter VTY line class view: line class vty	A setting in user line view is applied only to the user line. A setting in user line class view is applied to all user lines of the class. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view. A setting in user line view takes effect immediately and affects the online user. A setting in user line class view does not affect online users and takes effect only for new login users.
4. Enable password authentication.	authentication-mode password	By default, password authentication is enabled for VTY lines. In VTY line view, this command is associated with the protocol inbound command. If you specify a non-default value for only one of the two commands in VTY line view, the other command uses the default setting, regardless of the setting in VTY line class view.
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 line user is assigned the user role network-operator .

The next time you Telnet to the device, you must provide the configured login password, as shown in Figure 6. If the maximum number of login users has been reached, your login attempt fails and the message "All user lines are used, please try later!" appears.

Figure 6 Password authentication interface for Telnet login

```

*****
* Copyright (c) 2010-2014 Hewlett-Packard Development Company, L.P.      *
* Without the owner's prior written consent,                             *
* no decompiling or reverse-engineering shall be allowed.                 *
*****

Login authentication

Password:
<Sysname>

```

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 VTY line view or class view.	- Enter VTY line view: line vty first-number [last-number] - Enter VTY line class view: line class vty	A setting in user line view is applied only to the user line. A setting in user line class view is applied to all user lines of the class. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view. A setting in user line view takes effect immediately and affects the online user. A setting in user line class view does not affect online users and takes effect only for new login users.
4. Enable scheme authentication.	authentication-mode scheme	By default, password authentication is enabled for VTY lines. In VTY line view, this command is associated with the protocol inbound command. If you specify a non-default value for only one of the two commands in VTY line view, the other command uses the default setting, regardless of the setting in VTY line class view.

To use scheme authentication, you must also perform the following tasks:

- Configure login authentication methods in ISP domain view.
- To use remote authentication, configure the scheme to be used.
- To use local authentication, configure a local user and the relevant attributes.

For more information, see *Security Configuration Guide*.

The next time you Telnet to the CLI, you must provide the configured login username and password, as shown in Figure 7. If the maximum number of login users has been reached, your login attempt fails and the message "All lines are used, please try later!" appears.

Figure 7 Scheme authentication interface for Telnet login

```

*****
* Copyright (c) 2010-2014 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                *
* no decompiling or reverse-engineering shall be allowed.                    *
*****

Login authentication

Username:admin
Password:
<Sysname>

```

Setting the maximum number of concurrent Telnet users

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the maximum number of concurrent Telnet users.	aaa session-limit telnet max-sessions	By default, the maximum number of concurrent Telnet users is 32. Changing this setting does not affect online users. If the current number of online Telnet users is equal to or greater than the new setting, no additional Telnet users can log in until online users log out. For more information about this command, see <i>Security Command Reference</i>.

Setting the DSCP value for outgoing Telnet packets

The DSCP value is carried in the ToS/Traffic class field of an IP or IPv6 packet, and it indicates the transmission priority of the packet.

To set the DSCP value for outgoing Telnet packets:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the DSCP value for outgoing Telnet packets.	- For a Telnet server running IPv4: telnet server dscp dscp-value - For a Telnet server running IPv6: telnet server ipv6 dscp dscp-value	By default, the DSCP value is 48.

Configuring common VTY line settings

For a VTY line, 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 line.

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 lines:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter VTY line view or class view.	- Enter VTY line view: line vty <i>first-number</i> [<i>last-number</i>] - Enter VTY line class view: line class vty	A setting in user line view is applied only to the user line. A setting in user line class view is applied to all user lines of the class. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view. A setting in user line view takes effect immediately and affects the online user. A setting in user line class view does not affect online users and takes effect only for new login users.
3. Enable the terminal service.	shell	By default, terminal service is enabled.
4. Specify the protocols for the user lines to support.	protocol inbound { all ssh telnet }	By default, both Telnet and SSH are supported. A protocol change does not take effect for current online users. It takes effect only for new login users. In VTY line view, this command is associated with the authentication-mode command. If you specify a non-default value for only one of the two commands in VTY line view, the other command uses the default setting, regardless of the setting in VTY line class view.
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 <i>screen-length</i>	By default, up to 24 lines is displayed on a screen. A value of 0 disables the function.
8. Set the size of command history buffer.	history-command max-size <i>value</i>	By default, the buffer saves 10 history commands.

Step	Command	Remarks
9. Set the session idle timeout.	idle-timeout <i>minutes</i> [<i>seconds</i>]	By default, the session idle timeout is 10 minutes for all user lines. If there is no interaction between the device and the user within the idle timeout, the system automatically terminates the user connection on the user line. If you set the idle timeout to 0, the session will not be aged out.
10. Specify a command to be automatically executed when users log in to the user lines.	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 8 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
4. Use the device to log in to a Telnet server.	- Log in to an IPv4 Telnet server: telnet <i>remote-host</i> [<i>service-port</i>] [source { interface <i>interface-type interface-number</i> ip <i>ip-address</i> }] [dscp <i>dscp-value</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>] [dscp <i>dscp-value</i>]	N/A

Logging in through SSH

SSH offers a secure method 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 ecdsa } [name key-name]	By default, no local key pairs are created.
3. Enable SSH server.	ssh server enable	By default, SSH server is disabled.
4. (Optional.) Create an SSH user and specify the authentication mode.	- In non-FIPS mode: ssh user username service-type stelnet authentication-type { password { any password-publickey publickey } assign publickey keyname } - In FIPS mode: ssh user username service-type stelnet authentication-type { password password-publickey assign publickey keyname }	By default, no SSH user is configured on the device.

Step	Command	Remarks
5. Enter VTY line view or class view.	- Enter VTY line view: line vty <i>first-number</i> [<i>last-number</i>] - Enter VTY line class view: line class vty	A setting in user line view is applied only to the user line. A setting in user line class view is applied to all user lines of the class. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view. A setting in user line view takes effect immediately and affects the online user. A setting in user line class view does not affect online users and takes effect only for new login users.
6. Enable scheme authentication.	authentication-mode scheme	In non-FIPS mode, password authentication is enabled for VTY lines by default. In FIPS mode, scheme authentication is enabled for VTY lines by default. In VTY line view, this command is associated with the protocol inbound command. If you specify a non-default value for only one of the two commands in VTY line view, the other command uses the default setting, regardless of the setting in VTY line class view.
7. (Optional.) Specify the protocols for the user lines to support.	- In non-FIPS mode: protocol inbound { all ssh telnet } - In FIPS mode: protocol inbound ssh	In non-FIPS mode, Telnet and SSH are supported by default. In FIPS mode, SSH is supported by default. A protocol change does not take effect for current online users. It takes effect only for new login users. In VTY line view, this command is associated with the authentication-mode command. If you specify a non-default value for only one of the two commands in VTY line view, the other command uses the default setting, regardless of the setting in VTY line class view.
8. (Optional.) Set the maximum number of concurrent SSH users.	aaa session-limit ssh <i>max-sessions</i>	By default, the maximum number of concurrent SSH users is 32. Changing this setting does not affect online users. If the current number of online SSH users is equal to or greater than the new setting, no additional SSH users can log in until online users log out. For more information about this command, see <i>Security Command Reference</i>.
9. Exit to system view.	quit	N/A
10. (Optional.) Configure common settings for VTY lines.	See " Configuring common VTY line 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 9 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.	<code>ssh2 server</code>
Log in to an IPv6 SSH server.	<code>ssh2 ipv6 server</code>

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*.

Logging in through a pair of modems

You can use a pair of modems to remotely connect to the console port of the device over PSTN when the IP network connection is broken.

By default, modem dial-in is enabled, and you can dial in to the switch. The default user role is network-admin. To change modem dial-in parameters, see "[Logging in through the console port locally](#)."

To use a pair of modems to remotely log in to the device:

1. Connect one modem to the serial port of the PC and another modem to the console port of the device.
2. Connect each modem to the PSTN through a telephone cable.

Figure 10 Connecting the PC to the device through modems



3. Obtain the telephone number of the device-side modem.
4. Configure the following settings on the device-side modem:
 - **AT&F**—Restores the factory default.
 - **ATS0=1**—Configures auto-answer on first ring.
 - **AT&D**—Ignores DTR signals.
 - **AT&K0**—Disables local flow control.
 - **AT&R1**—Ignores RTS signals.
 - **AT&S0**—Forces **DSR** to remain on.

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

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

NOTE:

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

5. To ensure successful communication and to avoid data loss, verify that the modems are using a transmission rate higher than the console port's baud rate.
6. Launch the terminal emulation program on the PC and create a connection using the telephone number of the device-side modem.

Figure 11 through Figure 14 show the configuration procedure in Windows XP HyperTerminal. On Windows Server 2003, add the HyperTerminal program first, and then log in to and manage the device as described in this document. On Windows Server 2008, Windows 7, Windows Vista, or another operating system, obtain a third-party terminal control program first. Then, follow the user guide or online help of that program to log in to the device.

Figure 11 Creating a connection

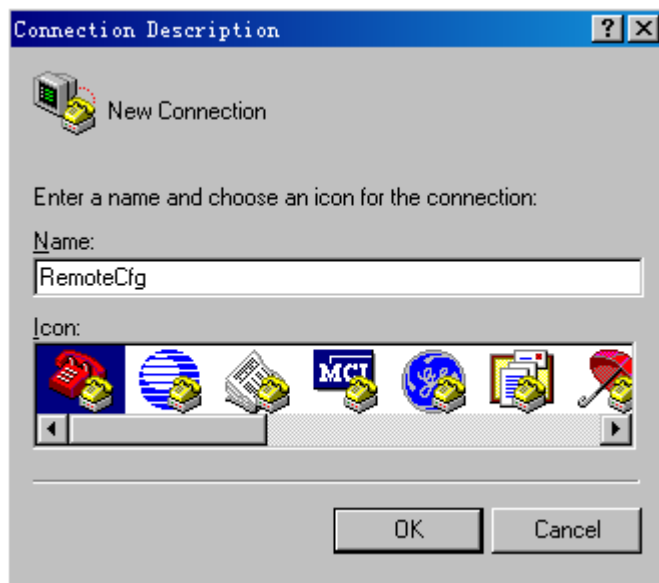
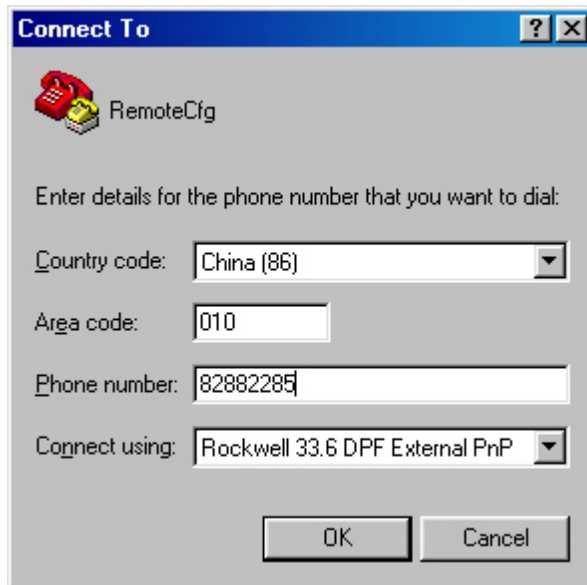
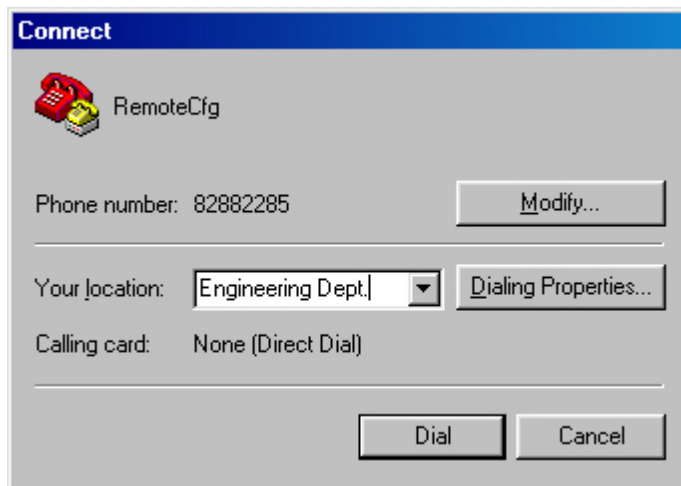


Figure 12 Configuring the dialing parameters



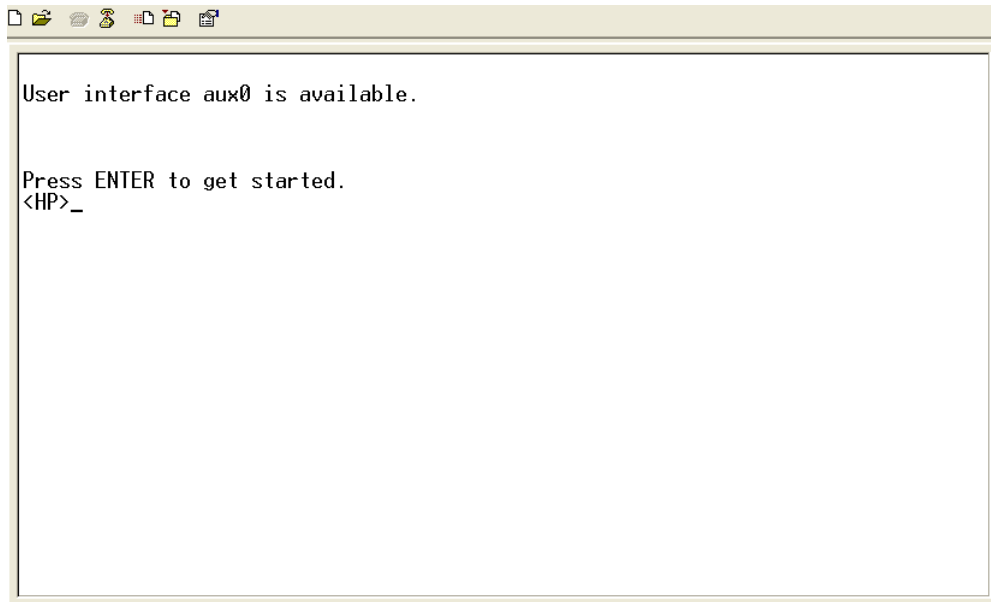
7. Dial the telephone number to establish a connection to the device.

Figure 13 Dialing the number



8. After you hear the dial tone, press **Enter** as prompted.
If the authentication mode is none, the prompt <HP> appears. If the authentication mode is password or scheme, you must enter the correct authentication information as prompted.

Figure 14 Login page



ⓘ **IMPORTANT:**

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

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

Displaying and maintaining CLI login

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

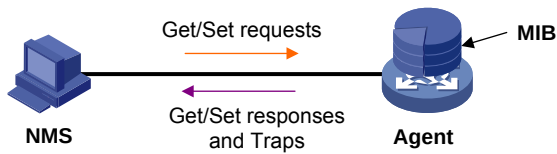
Task	Command	Remarks
Display online CLI user information.	display users [<i>all</i>]	N/A
Display user line information.	display line [<i>num1</i> { <i>aux</i> <i>vty</i> } <i>num2</i>] [<i>summary</i>]	N/A
Display the source address or interface for outgoing Telnet packets when the device acts as a Telnet client.	display telnet client	N/A
Release a user line.	free line { <i>num1</i> { <i>aux</i> <i>vty</i> } <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.

Task	Command	Remarks
Lock the current user line.	lock	By default, the system does not lock any user lines. This command is not supported in FIPS mode.
Send messages to user lines.	send { all <i>num1</i> { aux vty } <i>num2</i> }	Use this command in user view.

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 15 SNMP access diagram



The device supports SNMPv1, SNMPv2c, and SNMPv3, and can cooperate 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.

Controlling user access

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

FIPS compliance

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

Telnet is not supported in FIPS mode.

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 does not have any 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.	telnet server acl <i>acl-number</i> telnet server ipv6 acl [ipv6] <i>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.	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> .

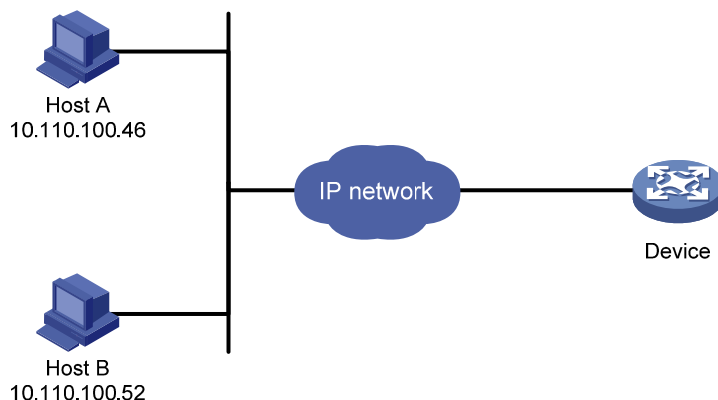
Configuration example

Network requirements

As shown in Figure 16, the device is a Telnet server.

Configure the device to permit only Telnet packets sourced from Host A and Host B.

Figure 16 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 SNMPv1 or SNMPv2c access, configure ACLs and perform the following tasks:

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

Step	Command	Remarks
4. Configure the SNMP access right.	(Method 1.) Create an SNMP community and specify ACLs for the community: - In VACM mode: snmp-agent community { read write } [simple cipher] community-name [mib-view view-name] [acl acl-number acl ipv6 ipv6-acl-number] * - In RBAC mode: snmp-agent community [simple cipher] community-name user-role role-name [acl acl-number acl ipv6 ipv6-acl-number] * (Method 2.) Create an SNMPv1/v2c group and add a user to the group, specifying ACLs for the group and user: a. 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] * b. snmp-agent usm-user { v1 v2c } user-name group-name [acl acl-number acl ipv6 ipv6-acl-number] *	For more information about SNMP, see <i>Network Management and Monitoring Configuration Guide</i> .

To control SNMPv3 access, configure ACLs and perform the following tasks:

Step	Command	Remarks
5. Enter system view.	system-view	N/A
6. Create an SNMPv3 group, specifying ACLs for the 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] *	N/A
7. Create an SNMPv3 user, specifying ACLs for the user.	- In VACM mode: snmp-agent usm-user v3 user-name group-name [remote { ip-address ipv6 ipv6-address }] [{ cipher simple } authentication-mode { md5 sha } auth-password [privacy-mode { aes128 3des des56 } priv-password] [acl acl-number acl ipv6 ipv6-acl-number] * - In RBAC mode: snmp-agent usm-user v3 user-name user-role role-name [remote { ip-address ipv6 ipv6-address }] [{ cipher simple } authentication-mode { md5 sha } auth-password [privacy-mode { aes128 3des des56 } priv-password] [acl acl-number acl ipv6 ipv6-acl-number] *	For more information about SNMP, see <i>Network Management and Monitoring Configuration Guide</i> .

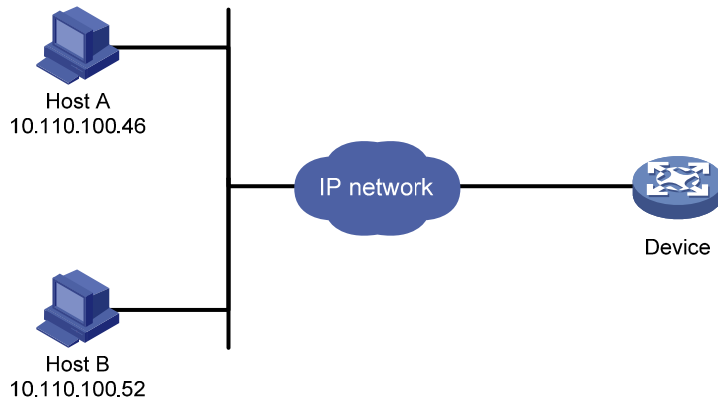
Configuration example

Network requirements

As shown in [Figure 17](#), the device is running SNMP.

Configure the device to allow Host A and Host B to access the device through SNMP.

Figure 17 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 user can use only commands that are permitted by both the AAA scheme and user role.

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

Step	Command	Remarks
2. Enter user line view or user line class view.	- Enter user line view: line { <i>first-number1</i> [<i>last-number1</i>] { aux vty } <i>first-number2</i> [<i>last-number2</i>] } - Enter user line class view: line class { aux vty }	A setting in user line view is applied only to the user line. A setting in user line class view is applied to all user lines of the class. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view. A setting in user line view takes effect immediately and affects the online user. A setting in user line class view does not affect online users and takes effect only for new login users.
3. Enable scheme authentication.	authentication-mode scheme	By default, authentication is disabled for AUX lines, and password authentication is enabled for VTY lines. In VTY line view, this command is associated with the protocol inbound command. If you specify a non-default value for only one of the two commands in VTY line view, the other command uses the default setting, regardless of the setting in VTY line class view.
4. Enable command authorization.	command authorization	By default, command authorization is disabled, and the commands available for a user vary only by user role. If the command authorization command is configured in user line class view, command authorization is enabled on all user lines in the class. You cannot configure the undo command authorization command in the view of a user line in the class.

Configuration example

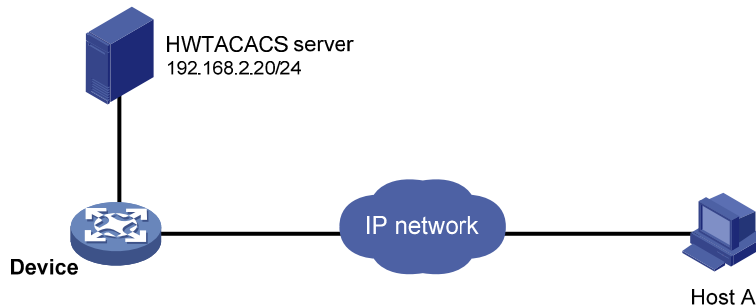
Network requirements

As shown in [Figure 18](#), Host A needs to log in to the device to manage the device.

Configure the device to perform the following tasks:

- Allows Host A to Telnet in after authentication.
- Uses the HWTACACS server to control the commands that the user can execute.
- If the HWTACACS server is not available, uses local authorization.

Figure 18 Network diagram



Configuration procedure

Assign IP addresses to relevant interfaces. Make sure the device and the HWTACACS server can reach each other. Make sure the device and Host A can reach each other. (Details not shown.)

Enable the Telnet server.

```
<Device> system-view
[Device] telnet server enable
```

Enable scheme authentication for user lines VTY 0 through VTY 63.

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
```

Enable command authorization for the user lines.

```
[Device-line-vty0-63] command authorization
[Device-line-vty0-63] quit
```

Create HWTACACS scheme **tac**.

```
[Device] hwtacacs scheme tac
```

Configure the scheme to use the HWTACACS server at 192.168.2.20:49 for authentication and authorization.

```
[Device-hwtacacs-tac] primary authentication 192.168.2.20 49
[Device-hwtacacs-tac] primary authorization 192.168.2.20 49
```

Set the shared keys to **expert**.

```
[Device-hwtacacs-tac] key authentication expert
[Device-hwtacacs-tac] key authorization expert
```

Remove domain names from usernames sent to the HWTACACS server.

```
[Device-hwtacacs-tac] user-name-format without-domain
[Device-hwtacacs-tac] quit
```

Configure the system-predefined domain **system**. Use the HWTACACS scheme **tac** for login user authentication and command authorization. Use local authentication and local authorization as the backup method.

```
[Device] domain system
[Device-isp-system] authentication login hwtacacs-scheme tac local
[Device-isp-system] authorization command hwtacacs-scheme tac local
[Device-isp-system] quit
```

Create local user **monitor**. Set the password to 123, the service type to Telnet, and the default user role to level-1.

```
[Device] local-user monitor
```

```
[Device-luser-manage-admin] password cipher 123
[Device-luser-manage-admin] service-type telnet
[Device-luser-manage-admin] authorization-attribute user-role level-1
```

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 behavior 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 line view or user line class view.	- Enter user line view: line { <i>first-number1</i> [<i>last-number1</i>] { aux vty } <i>first-number2</i> [<i>last-number2</i>] } - Enter user line class view: line class { aux vty }	A setting in user line view is applied only to the user line. A setting in user line class view is applied to all user lines of the class. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view. A setting in user line view takes effect immediately and affects the online user. A setting in user line class view does not affect online users and takes effect only for new login users.
3. Enable scheme authentication.	authentication-mode scheme	By default, authentication is disabled for AUX lines, and password authentication is enabled for VTY lines. In VTY line view, this command is associated with the protocol inbound command. If you specify a non-default value for only one of the two commands in VTY line view, the other command uses the default setting, regardless of the setting in VTY line class view.

Step	Command	Remarks
4. Enable command accounting.	command accounting	By default, command accounting is disabled, and the accounting server does not record the commands executed by users. If the command accounting command is configured in user line class view, command accounting is enabled on all user lines in the class. You cannot configure the undo command accounting command in the view of a user line in the class.

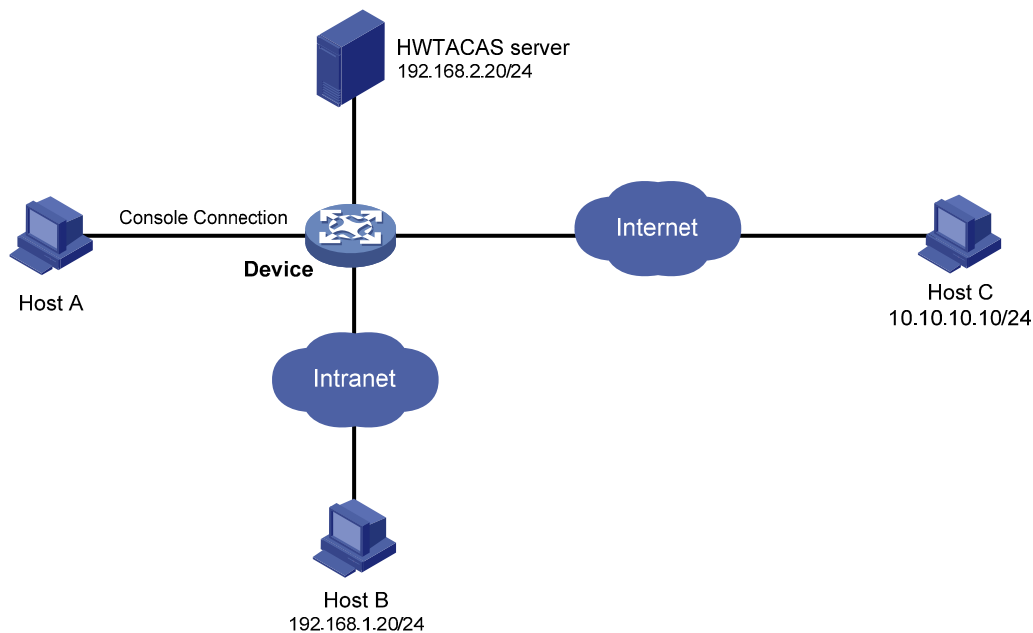
Configuration example

Network requirements

As shown in Figure 19, users need to log in to the device to manage the device.

Configure the device to send commands executed by users to the HWTACACS server to monitor and control user operations on the device.

Figure 19 Network diagram



Configuration procedure

```

# Enable the Telnet server.
<Device> system-view
[Device] telnet server enable

# Enable command accounting for user line AUX 0.
[Device] line aux 0
[Device-line-aux0] command accounting

```

```
[Device-line-aux0] quit
# Enable command accounting for user lines VTY 0 through VTY 63.
[Device] line vty 0 63
[Device-line-vty0-63] command accounting
[Device-line-vty0-63] quit
# Create HWTACACS scheme tac.
[Device] hwtacacs scheme tac
# Configure the scheme to use the HWTACACS server at 192.168.2.20:49 for accounting.
[Device-hwtacacs-tac] primary accounting 192.168.2.20 49
# Set the shared key to expert.
[Device-hwtacacs-tac] key accounting expert
# Remove domain names from usernames sent to the HWTACACS server.
[Device-hwtacacs-tac] user-name-format without-domain
[Device-hwtacacs-tac] quit
# Configure the system-predefined domain system to use the HWTACACS scheme for command accounting.
[Device] domain system
[Device-isp-system] accounting command hwtacacs-scheme tac
[Device-isp-system] quit
```

Configuring RBAC

Overview

Role based access control (RBAC) controls user access to items and system resources based on user role. Items include commands, XML elements, and MIB nodes. System resources include interfaces, and VLANs.

On devices that support multiple users, RBAC is used to assign access permissions to user roles that are created for different job functions. Users are given permission to access a set of items and resources based on the users' 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 determine accessible or inaccessible items for the user role. (See "[User role rules](#).")
- Configure resource access policies to specify which interfaces, and VLANs are accessible to the user role. (See "[Resource access policies](#).")

To use a command related to a resource (an interface, or VLAN), a user role must have access to both the command and the resource.

For example, a user role has access to the **qos apply policy** command and access only to 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. However, 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, XML elements, or MIB nodes. 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.
- **Feature group rule**—Controls access to commands of a group of features by command type.
- **XML element rule**—Controls access to XML elements used for configuring the device.
- **OID rule**—Controls SNMP access to a MIB node and its child nodes. An OID is a dotted numeric string that uniquely identifies the path from the root node to a leaf node.

The commands, XML elements, and MIB nodes are controlled based on the following types:

- **Read**—Commands, XML elements, or MIB nodes that display configuration and maintenance information. For example, the **display** commands and the **dir** command.

- **Write**—Commands, XML elements, or MIB nodes that configure the features in the system. For example, the **info-center enable** command and the **debugging** command.
- **Execute**—Commands, XML elements, or MIB nodes that execute specific functions. For example, the **ping** command and the **ftp** command.

A user role can access the set of permitted commands, XML elements, and MIB nodes specified in the user role rules. The user role rules include predefined (identified by sys-*n*) and user-defined user role rules. For more information about the user role rule priority, see "[Configuring user role rules](#)."

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.

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

Predefined user roles

The system provides predefined user roles. These user roles have access to all system resources (interfaces, and VLANs). However, their access permissions differ, as shown in [Table 9](#).

Among all of the predefined user roles, only network-admin, and level-15 can perform the following tasks:

- Access the RBAC feature.
- Change the settings in user line view, including **user-role**, **authentication-mode**, **protocol inbound**, and **set authentication password**.
- Create, modify, and delete local users and local user groups. The other user roles can only modify their own password if they have permissions to configure local users and local user groups.

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, except for the display security-logfile summary , info-center security-logfile directory , and security-logfile save commands.
network-operator	• Accesses the display commands for features and resources in the system. To display all accessible commands of the user role, use the display role command. • Enables local authentication login users to change their own password. • Accesses the command used for entering XML view. • Accesses all read-type XML elements. • Accesses all read-type MIB nodes.

User role name	Permissions
level- <i>n</i> (<i>n</i> = 0 to 15)	• level-0—Has access to diagnostic commands, including ping, quit, ssh2, super, system-view, telnet, and tracert. Level-0 access rights are configurable. • level-1—Has access to the display commands of all features and resources in the system except display history-command all. The level-1 user role also has all access rights of the level-0 user role. 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 those in the following list. 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. ◦ RBAC non-debugging commands. ◦ Local users. ◦ File management. ◦ Device management. ◦ The display history-command all command. • level-15—Has the same rights as network-admin.
security-audit	Security log manager. The user role has the following access to security log files: • Accesses to the commands for displaying and maintaining security log files (for example, the dir, display security-logfile summary, and more commands). • Accesses to the commands for managing security log files and security log file system (for example, the info-center security-logfile directory, mkdir, and security-logfile save commands). For more information about security log management, see <i>Network Management and Monitoring Configuration Guide</i>. For more information about file system management, see "Managing the file system."  IMPORTANT: Only the security-audit user role has access to security log files.

Assigning user roles

You assign access rights to users by assigning a minimum of one user role. The users can use the collection of system items and resources accessible to any user role assigned to them. For example, you can access any interface to use the **qos apply policy** command if you are assigned the following user roles:

- User role A denies access to the **qos apply policy** command and permits access only to interface Ten-GigabitEthernet 1/0/1.
- User role B permits access to the **qos apply policy** command and all interfaces.

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

- **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. The AAA server can be a RADIUS or HWTACACS server.
- **Non-AAA authorization**—When the user accesses the device without authentication or by passing password authentication, the device assigns user roles specified on the user line. This method 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 device management user accounts.

For more information about AAA and SSH, see *Security Configuration Guide*. For more information about user line, see "[Login overview](#)" and "[Logging in to the CLI](#)."

FIPS compliance

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

Configuration task list

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

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 the following predefined user roles: • network-admin. • network-operator. • level-<i>n</i> (where <i>n</i> equals an integer in the range 0 to 15). • security-audit. Among these user roles, only the permissions and description of the level-0 to level-14 user roles are configurable.
3. (Optional.) Configure a description for the user role.	description <i>text</i>	By default, a user role does not have a description.

Configuring user role rules

You can configure command, feature, feature group, XML element, and OID rules to permit or deny the access of a user role to specific commands, XML elements, and MIB nodes.

Configuration restrictions and guidelines

When you configure RBAC user role rules, follow these restrictions and guidelines:

- You can configure up to 256 user-defined rules for a user role. The total number of user-defined user role rules cannot exceed 1024.
- Any rule modification, addition, or removal for a user role takes effect only on users who are logged in with the user role after the change.

The following guidelines apply to non-OID rules:

- If two user-defined rules of the same type conflict, the rule with the higher ID takes effect. For example, the user role can use the **tracert** command but not the **ping** command if the user role contains rules configured by using the following commands:
 - **rule 1 permit command ping**
 - **rule 2 permit command tracert**
 - **rule 3 deny command ping**
- For level-0 to level-14 user roles, if a predefined user role rule and a user-defined user role rule conflict, the user-defined user role rule takes effect.

The following guidelines apply to OID rules:

- The system compares an OID with the OIDs specified in user role rules, and it uses the longest match principle to select a rule for the OID. For example, a user role cannot access the MIB node with OID 1.3.6.1.4.1.25506.141.3.0.1 if the user role contains rules configured by using the following commands:
 - **rule 1 permit read write oid 1.3.6**
 - **rule 2 deny read write oid 1.3.6.1.4.1**

- **rule 3 permit read write oid 1.3.6.1.4**
- If the same OID is specified in multiple rules, the rule with the higher ID takes effect. For example, the user role can access the MIB node with OID 1.3.6.1.4.1.25506.141.3.0.1 if the user role contains rules configured by using the following commands:
 - **rule 1 permit read write oid 1.3.6**
 - **rule 2 deny read write oid 1.3.6.1.4.1**
 - **rule 3 permit read write oid 1.3.6.1.4.1**

Configuration procedure

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.	● 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> ● Configure an XML element rule: rule <i>number</i> { deny permit } { execute read write } * xml-element [<i>xml-string</i>] ● Configure an OID rule: rule <i>number</i> { deny permit } { execute read write } * oid [<i>oid-string</i>]	By default, a user-defined user role does not have any rules or access to any commands, XML elements, or MIB nodes. Repeat this step to add up to 256 rules to the user role. ! IMPORTANT: When you configure feature rules, you can specify only features available in the system. Enter feature names the same as the feature names are displayed, including the case.

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

Step	Command	Remarks
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: • 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 does not have any features.  IMPORTANT: You can specify only features available in the system. Enter feature names the same as the feature names are displayed, including the case.

Configuring resource access policies

Every user role has one interface policy, and VLAN policy. By default, these policies permit user roles to access any interface, and VLAN. You can configure the policies of a user-defined user role or a predefined level-*n* user role to limit its access to interfaces, and VLANs. The policy configuration takes effect only on users who are logged in with the user role after the configuration.

Configuring 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 policy of the user role permits access to all interfaces. This command denies the access of the user role to all interfaces if the permit interface command is not configured.
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 in user role interface policy view. Repeat this step to add more accessible interfaces.

Configuring 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

Step	Command	Remarks
3. Enter user role VLAN policy view.	vlan policy deny	By default, the VLAN policy of the user role permits access to all VLANs. This command denies the access of the user role to all VLANs if the permit vlan command is not configured.
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 in user role VLAN policy view. Repeat this step to add more accessible VLANs.

Assigning user roles

To control user access to the system, you must assign a minimum of one user role. Make sure a minimum of one user role among the user roles assigned by the server exists on the device. User role assignment procedure varies for 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 feature

The default user role feature allows AAA-authenticated users to access the system if the AAA server does not authorize any user roles to the users.

You can configure this feature to enable an AAA-authenticated user that has not been assigned any user role to log in with the default user role network-operator.

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

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the default user role feature.	role default-role enable	By default, the default user role feature is disabled. If the none authorization method is used for local users, you must enable the default user role feature.

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.

If the AAA server assigns the security-audit user role and other user roles to the same user, only the security-audit user role takes effect.

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 the default user role.

If a local user is the only user with the security-audit user role, the user cannot be deleted.

The **security-audit** user role is mutually exclusive with other user roles.

- When you assign the security-audit user role to a local user, the system requests confirmation to delete all the other user roles of the local user first.
- When you assign the other user roles to a local user who has been assigned the security-audit user role, the system requests confirmation to delete the security-audit user role for the local user first.

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 <i>user-name</i> 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 or level-15 user.
4. (Optional.) Remove undesirable user roles.	undo authorization-attribute user-role <i>role-name</i>	A user can use the collection of system items and resources accessible to any user role assigned to the user. If a user role is undesirable (for example, the default user role), you must use this command to delete the user role.

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

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

- Users who 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 device management user accounts.

For more information about user lines, 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 line:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter user line view or use line class view.	- Enter user line view: line { <i>first-num1</i> [<i>last-num1</i>] { aux vty } <i>first-num2</i> [<i>last-num2</i>] } - Enter user line class view: line class { aux vty }	For information about the priority order and application scope of the configurations in user line view and user line class view, see "Logging into the CLI."
3. Specify a user role on the user line.	user-role <i>role-name</i>	Repeat this step to specify up to 64 user roles on a user line. By default, network-admin is specified on the AUX user line, and network-operator is specified on any other user line. The device cannot assign the security-audit user role to non-AAA authentication users.

Configuring temporary user role authorization

Temporary user role authorization allows you to obtain another user role without reconnecting to the device. This feature is useful when you want to use a user role temporarily to configure a feature.

Temporary user role authorization is effective only on the current login. This feature does not change the user role settings in the user account that you have been logged in with. The next time you are logged in with the user account, the original user role settings take effect.

Configuration guidelines

When you configure temporary user role authorization, follow these guidelines:

- To enable users to obtain another user roles without reconnecting to the device, you must configure user role authentication. [Table 10](#) describes the available authentication modes and configuration requirements.
- If HWTACACS authentication is used, the following rules apply:
 - The device uses the entered username and password to request role authentication, and it sends the username to the server in the format *username* or *username@domain-name*. Whether the domain name is included in the username depends on the **user-name-format** command in the HWTACACS scheme.
 - To obtain a level-*n* user role, the user account on the server must have the target user role level or a user role level higher than the target user role. A user account that obtains the level-*n* user role can obtain any user roles among level 0 through level-*n*.
 - To obtain a non-level-*n* user role, make sure the user account on the server meets the following requirements:

- The account has a user privilege level.
 - The HWTACACS custom attribute is configured for the account in the form of **allowed-roles="role"**. The variable *role* represents the target user role.
- If RADIUS authentication is used, the following rules apply:
 - The device does not use the username you enter to request user role authentication. and it uses a username in the **\$enabn\$** format. The variable *n* represents a user role level, and a domain name is not included in the username. You can always pass user role authentication when the password is correct.
 - To obtain a level-*n* user role, you must create a user account for the level-*n* user role in the **\$enabn\$** format on the RADIUS server. The variable *n* represents the target user role level. For example, to obtain the authorization of the level-3 user role, you can enter any username. The device uses the username **\$enab3\$** to request user role authentication from the server.
 - To obtain a non-level-*n* user role, you must perform the following tasks:
 - Create the user account **\$enab0\$** on the server.
 - Configure the cisco-av-pair attribute for the account in the form of **allowed-roles="role"**. The variable *role* represents the target user role.
- The device selects an authentication domain for user role authentication in the following order:
 - a. The ISP domain included in the entered username.
 - b. The default ISP domain.
- If you execute the **quit** command after obtaining user role authorization, you are logged out of the device.

Table 10 User role authentication modes

Keywords	Authentication mode	Description
local	Local password authentication only (local-only)	The device uses the locally configured password for authentication. If no local password is configured for a user role in this mode, an AUX user can obtain the user role authorization by either entering a string or not entering anything.
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: • 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 local password is configured for the user role in this mode: • The device performs remote AAA authentication for VTY users. • An AUX user can obtain another user role by either entering a string or not entering anything.

Keywords	Authentication mode	Description
scheme local	Remote AAA authentication first, and then local password authentication (remote-then-local)	Remote AAA authentication is performed first. Local password authentication is performed in either of the following situations: - The HWTACACS or RADIUS server does not respond. - The remote AAA configuration on the device is invalid.

Configuring user role 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. (Optional.) Specify the default target user role for temporary user role authorization.	super default role <i>rolename</i>	By default, the default target user role is network-admin.
4. Set a local authentication password for a user role.	- In non-FIPS mode: super password [role <i>rolename</i>] [{ hash simple } <i>password</i>] - In FIPS mode: super password [role <i>rolename</i>]	Use this step for local password authentication. By default, no password is configured. If you do not specify the role <i>rolename</i> option, the command sets a password for the default target user role.

Obtaining temporary user role authorization

AUX or VTY users must pass authentication before they can use a user role that is not included in the user account they are logged in with.

Perform the following task in user view:

Task	Command	Remarks
Obtain the temporary authorization to use a user role.	super [<i>rolename</i>]	If you do not specify the <i>rolename</i> argument, you obtain the default target user role for temporary user role authorization. The operation fails after three consecutive unsuccessful password attempts. The user role must have the permission to execute the super command to obtain temporary user role authorization.

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 examples

RBAC configuration example for local AAA authentication users

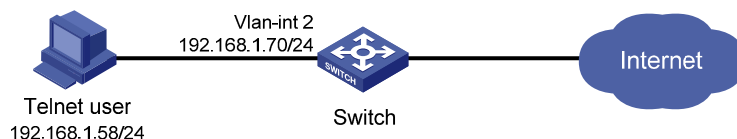
Network requirements

As shown in [Figure 20](#), the switch performs local AAA authentication for the Telnet user at 192.168.1.58. The Telnet user has the username **user1@bbb** and is assigned the user role **role1**.

Configure role1 to have the following permissions:

- Can execute the read commands of any feature.
- Cannot configure any VLAN except VLANs 10 to 20.

Figure 20 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 lines for Telnet users.

```
[Switch] line vty 0 63
```

```
[Switch-line-vty0-63] authentication-mode scheme
```

```
[Switch-line-vty0-63] 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 device management user named user1 and enter local user view.
[Switch] local-user user1 class manage
New local user added.

# 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

# Remove the default user role network-operator from the user. This operation ensures that the user has
only the permissions of role1.
[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 switch. (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 Tues 01/01/2013
[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

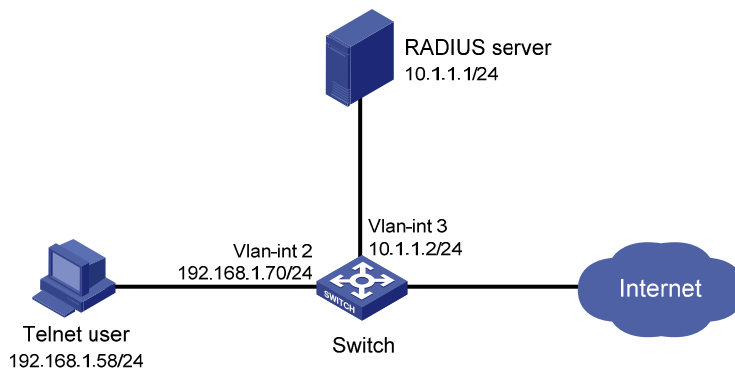
As shown in Figure 21, the switch uses the FreeRADIUS server at 10.1.1.1/24 to provide AAA service for login users, including the Telnet user at 192.168.1.58. The Telnet user uses the username **hello@bbb** and is assigned the user role **role2**.

The user role role2 has the following permissions:

- Can use all commands in ISP view.
- Can use the read and write commands of the **arp** and **radius** features.
- Cannot access the read commands of the **acl** feature.
- Can configure only VLANs 1 to 20 and interfaces Ten-GigabitEthernet 1/0/1 to Ten-GigabitEthernet 1/0/20.

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 21 Network diagram



Configuration procedure

Make sure 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 lines for Telnet users.
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
[Switch-line-vty0-63] quit
# Create the RADIUS scheme rad and enter RADIUS scheme 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:

Because RADIUS user authorization information is piggybacked in authentication responses, the authentication and authorization methods must use the same RADIUS scheme.

```

[Switch] domain bbb
[Switch-isp-bbb] authentication login radius-scheme rad
[Switch-isp-bbb] authorization login radius-scheme rad
[Switch-isp-bbb] quit
# Create feature group fgroup1.
[Switch] role feature-group name fgroup1
# Add the arp and radius features 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 1/0/20.
[Switch-role-role2] interface policy deny
[Switch-role-role2-ifpolicy] permit interface ten-gigabitethernet 1/0/1 to
ten-gigabitethernet 1/0/20
[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 switch. (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 **radius** and **arp** features. This example uses **radius**.

```
[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 1/0/20. Take Ten-GigabitEthernet 1/0/2 and Ten-GigabitEthernet 1/0/22 as examples.

```
[Switch] vlan 10
[Switch-vlan10] port ten-gigabitethernet 1/0/2
[Switch-vlan10] port ten-gigabitethernet 1/0/22
```

Permission denied.

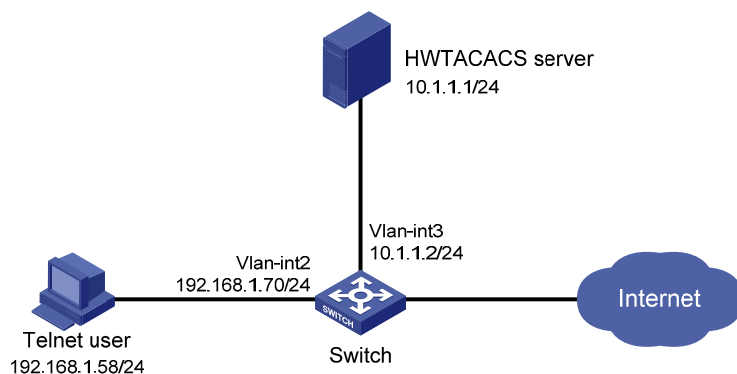
RBAC temporary user role authorization configuration example (HWTACACS authentication)

Network requirements

As shown in Figure 22, the switch uses local authentication for login users, including the Telnet user at 192.168.1.58. The Telnet user uses the username **test@bbb** and is assigned the user role **level-0**.

Configure the remote-then-local authentication mode for temporary user role authorization. The switch uses the HWTACACS server to provide authentication for changing the user role among **level-0** through **level-3** or changing the user role to **network-admin**. If the AAA configuration is invalid or the HWTACACS server does not respond, the switch performs local authentication.

Figure 22 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 lines for Telnet users.

```
[Switch] line vty 0 63
```

```
[Switch-line-vty0-63] authentication-mode scheme
```

```
[Switch-line-vty0-63] quit
```

Enable remote-then-local authentication for temporary user role authorization.

```
[Switch] super authentication-mode scheme local
```

Create the HWTACACS scheme **hwtac** and enter HWTACACS scheme 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 ISP domain 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 for user role authentication.
[Switch-isp-bbb] authentication super hwtacacs-scheme hwtac
[Switch-isp-bbb] quit
# Create a device management user named test and enter local user view. Set the service type to
Telnet, and set the password to aabbcc.
[Switch] local-user test class manage
New local user added.
[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-operator.
[Switch-luser-manage-test] undo authorization-attribute user-role network-operator
[Switch-luser-manage-test] quit
# Set the local authentication password to 654321 for the user role level-3.
[Switch] super password role level-3 simple 654321
# Set the local authentication password to 654321 for the user role network-admin.
[Switch] super password role network-admin simple 654321
[Switch] quit

```

2. Configure the HWTACACS server:

This example uses ACSv4.0.

- a. Access the **User Setup** page.
- b. Add a user account **test**. (Details not shown.)
- c. In the **Advanced TACACS+ Settings** area, configure the following parameters:
 - Select **Level 3** for the **Max Privilege for any AAA Client** option.
If the target user role is only **network-admin** for temporary user role authorization, you can select any level from the **Max Privilege for any AAA Client** option.
 - Select the **Use separate password** option, and specify **enabpass** as the password.

Figure 23 Configuring advanced TACACS+ settings

Advanced TACACS+ Settings

TACACS+ Enable Control:

☐ Use Group Level Setting

☐ No Enable Privilege

☒ Max Privilege for any AAA Client

Level 3

TACACS+ Enable Password

☐ Use CiscoSecure PAP password

☐ Use external database password

Windows Database

☒ Use separate password

Password

Confirm Password

TACACS+ Outbound Password

(Used for SendPass and SendAuth clients such as routers)

Password

Confirm Password

- d. Select **Shell (exec)** and **Custom attributes**, and enter **allowed-roles="network-admin"** in the **Custom attributes** field.

Use a blank space to separate the allowed roles.

Figure 24 Configuring custom attributes for the Telnet user

☒ Shell (exec)

☐ Access control list

☐ Auto command

☐ Callback line

☐ Callback rotary

☐ Idle time

☐ No callback verify

☐ No escape

☐ No hangup

☐ Privilege level

☐ Timeout

☒ Custom attributes

allowed-roles="network-admin"

Verifying the configuration

1. Telnet to the switch, and enter the username **test@bbb** and password **aabbcc** to access the switch. 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) 2010-2014 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>?
```

```
User view commands:
```

```
ping          Ping function
quit          Exit from current command view
ssh2          Establish a secure shell client connection
super         Switch to a user role
system-view   Enter the System View
telnet        Establish a telnet connection
tracert       Tracert function
```

<Switch>

2. Verify that you can obtain the level-3 user role:

Use the super password to obtain the level-3 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 obtained the level-3 user role.

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 obtained the level-3 user role.

3. Use the method in step 2 to verify that you can obtain the user roles level 0, level 1, level 2, and network-admin. (Details not shown.)

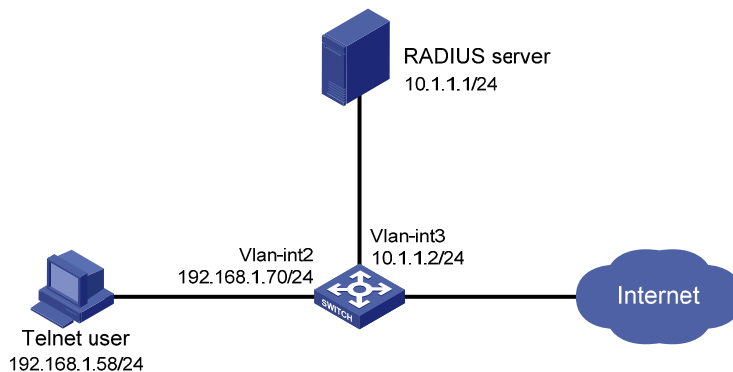
RBAC temporary user role authorization configuration example (RADIUS authentication)

Network requirements

As shown in Figure 25, the switch uses local authentication for login users, including the Telnet user at 192.168.1.58. The Telnet user uses the username **test@bbb** and is assigned the user role **level-0**.

Configure the remote-then-local authentication mode for temporary user role authorization. The switch uses the RADIUS server to provide authentication for the network-admin user role. If the AAA configuration is invalid or the RADIUS server does not respond, the switch performs local authentication.

Figure 25 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 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 lines for Telnet users.
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
[Switch-line-vty0-63] quit

# Enable remote-then-local authentication for temporary user role authorization.
[Switch] super authentication-mode scheme local

# Create RADIUS scheme radius and enter RADIUS scheme view.
[Switch] radius scheme radius

# Specify the primary authentication server address 10.1.1.1, and set the shared key to expert in
the scheme for secure communication between the switch and the server.
[Switch-radius-radius] primary authentication 10.1.1.1 key simple expert

# Exclude the ISP domain name from the username sent to the RADIUS server.
[Switch-radius-radius] user-name-format without-domain
[Switch-radius-radius] quit

# Create ISP domain bbb and enter ISP domain 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 RADIUS scheme radius to the ISP domain for user role authentication.
[Switch-isp-bbb] authentication super radius-scheme radius
[Switch-isp-bbb] quit

# Create a device management user named test and enter local user view.
[Switch] local-user test class manage
New local user added.

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

# Set the user password to aabbcc.
[Switch-luser-manage-test] password simple aabbcc

# Assign level-0 to the user.
[Switch-luser-manage-test] authorization-attribute user-role level-0

# Remove the default user role network-operator.
[Switch-luser-manage-test] undo authorization-attribute user-role network-operator

```

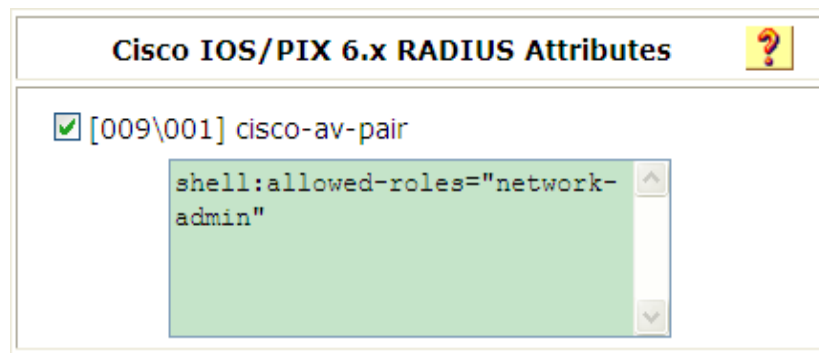
```
[Switch-luser-manage-test] quit
# Set the local authentication password to abcdef654321 for the user role network-admin.
[Switch] super password role network-admin simple abcdef654321
[Switch] quit
```

2. Configure the RADIUS server:

This example uses ACSv4.2.

- a. Add a user account **\$enab0\$** and set the password to **123456**. (Details not shown.)
- b. Access the **Cisco IOS/PIX 6.x RADIUS Attributes** page.
- c. Configure the **cisco-av-pair** attribute, as shown in [Figure 26](#).

Figure 26 Configuring the cisco-av-pair attribute



Verifying the configuration

1. Telnet to the switch, and enter the username **test@bbb** and password **aabbcc** to access the switch. 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) 2010-2014 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>?
User view commands:
ping          Ping function
quit          Exit from current command view
ssh2          Establish a secure shell client connection
super         Switch to a user role
system-view   Enter the System View
telnet        Establish a telnet connection
tracert        Tracert function
```

<switch>

2. Verify that you can obtain the network-admin user role:

Use the super password to obtain the network-admin user role. When the system prompts for a username and password, enter the username **test@bbb** and password **123456**.

```
<Switch> super network-admin
```

```
Username: test@bbb
```

```
Password:
```

The following output shows that you have obtained the network-admin user role.

User privilege role is network-admin, and only those commands that authorized to the role can be used.

If the ACS server does not respond, enter the local authentication password **abcdef654321** at the prompt.

Invalid configuration or no response from the authentication server.

Change authentication mode to local.

```
Password:
```

User privilege role is network-admin, and only those commands that authorized to the role can be used.

The output shows that you have obtained the network-admin user role.

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 the local user.

Solution

To resolve the problem:

1. Use the **display local-user** command to examine the local user accounts for undesirable user roles, and delete them.
2. If the problem persists, contact HP Support.

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 following conditions exist:

- The network access device and the RADIUS server can communicate with one another.
- All AAA settings are correct.

Analysis

RBAC requires that a login user have a minimum of 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

To resolve the problem:

1. Use one of the following methods:
 - Configure the **role default-role enable** command. 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.
2. If the problem persists, contact HP Support.

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

By default, the transfer mode is binary.

FTP can operate in either of the following modes:

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

The FTP operation mode varies by 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 27 FTP application scenario



FIPS compliance

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

FTP is not supported in FIPS mode.

Using the device as an FTP server

To use the device as an FTP server, you must enable the FTP server and configure authentication and authorization on the device. Other commands are optional.

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 { <i>acl-number</i> ipv6 <i>acl-number6</i> }	By default, no ACL is used for access control.
4. (Optional.) Associate an SSL server policy with the FTP server to ensure data security.	ftp server ssl-server-policy <i>policy-name</i>	By default, no SSL server policy is associated with the FTP server.
5. (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.
6. (Optional.) Set the DSCP value for outgoing FTP packets.	- For an FTP server running IPv4: ftp server dscp <i>dscp-value</i> - For an FTP server running IPv6: ftp server ipv6 dscp <i>dscp-value</i>	By default, the DSCP value is 0.
7. (Optional.) Set the maximum number of concurrent FTP users.	aaa session-limit ftp <i>max-sessions</i>	By default, the maximum number of concurrent FTP users is 32. Changing this setting does not affect online users. If the current number of online FTP users is equal to or greater than the new setting, no additional FTP users can log in until online users log out. For more information about this command, see <i>Security Command Reference</i> .

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.	• 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.

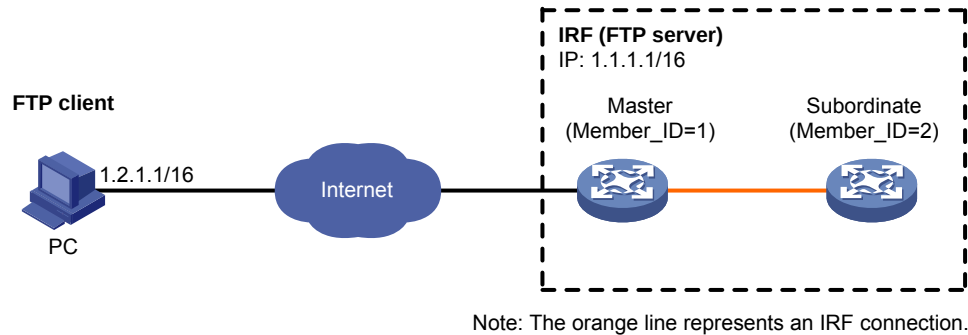
Task	Command
Display FTP server configuration and status information.	display ftp-server
Display detailed information about online FTP users.	display ftp-user

FTP server configuration example

Network requirements

- Configure the device as an FTP server.
- 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.
- Download the configuration file **config.cfg** from the FTP server to the FTP client for backup.

Figure 28 Network diagram



Configuration procedure

1. Configure IP addresses as shown in Figure 28. 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. 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:/**.)
 - # Create a local user with the username **abc** and password **123456**.

```
<Sysname> system-view
[Sysname] local-user abc class manage
[Sysname-luser-manage-abc] password simple 123456

# Assign the user role network-admin to the user. Set the working directory to the root directory of the flash memory.
[Sysname-luser-manage-abc] authorization-attribute user-role network-admin
work-directory flash:/

# Assign the service type FTP to the user.
[Sysname-luser-manage-abc] service-type ftp
[Sysname-luser-manage-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.
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

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.	(Method 1.) Log in to the FTP server from user view: ftp <i>ftp-server</i> [<i>service-port</i>] [dscp <i>dscp-value</i> source { interface { <i>interface-name</i> <i>interface-type interface-number</i> } ip <i>source-ip-address</i> }] * (Method 2.) Log in to the FTP server from FTP client view: a. ftp b. open <i>server-address</i> [<i>service-port</i>]	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

Step	Command	Remarks
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.	(Method 1.) Log in to the FTP server from user view: ftp ipv6 <i>ftp-server</i> [<i>service-port</i>] [dscp <i>dscp-value</i>] source { interface <i>interface-type interface-number</i> ipv6 <i>source-ipv6-address</i> }] * [-i <i>interface-type interface-number</i>] (Method 2.) Log in to the FTP server from FTP client view: a. ftp ipv6 b. open <i>server-address</i> [<i>service-port</i>]	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.	- Display the detailed information of a directory or file on the FTP server: dir [<i>remote file</i> [<i>local file</i>]] - Display the name of a directory or file on the FTP server: ls [<i>remote file</i> [<i>local file</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.	- Display detailed information about 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.	- Set the file transfer mode to ASCII: ascii - Set the file transfer mode to binary: binary	The default file transfer mode is binary.
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

Changing to another user account

After you log in to the FTP server, you can change 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 change to another user account, execute the following command in user view:

Task	Command
Change 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.	rhel	N/A
Display FTP commands help information on the FTP server.	rhel <i>protocol-command</i>	N/A
Display FTP server status.	rstatus	N/A
Display detailed information about a directory or file on the FTP server.	rstatus <i>remote file</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
Terminate the connection to the FTP server without exiting FTP client view.	• disconnect • close
Terminate the connection to the FTP server and return to user view.	• bye • quit

Displaying command help information

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

Task	Command
Display command help information	• help [<i>command-name</i>] • ? [<i>command-name</i>]

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

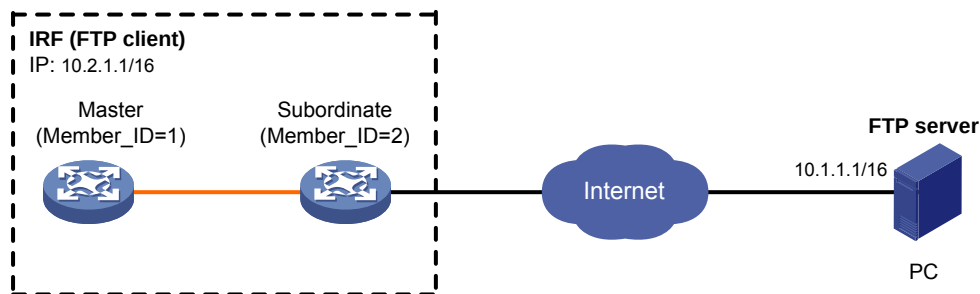
FTP client configuration example

Network requirements

As shown in Figure 29, the PC is acting as an FTP server. A user account with the username **abc** and password **123456** has been created on the PC.

- Use the IRF fabric as an FTP client to log in to the FTP server.
- Download the file **temp.bin** from the FTP server to the FTP client.
- Upload the configuration file **config.cfg** from the FTP client to the FTP server for backup.

Figure 29 Network diagram



Note: The orange line represents an IRF connection.

Configuration procedure

Configure IP addresses as shown in Figure 29. Make sure the IRF fabric and PC can reach each other. (Details not shown.)

Examine the storage space on the member devices. 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
```

```
Press CTRL+C to abort.
```

```
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
227 Entering Passive Mode (192,168,0,20,207,117)
150 "C:\Users\wKF5122\Desktop\FTP\temp.bin" file ready to send (13507003 bytes) in IMAGE / Binary mode
226 Transfer finished successfully.
13507003 bytes received in 17.188 seconds (767.42 Kbytes/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

# Use the ASCII mode to 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
227 Entering Passive Mode (192,168,0,20,207,237)
150 "C:\Users\wKF5122\Desktop\FTP\config.cfg" file ready to receive in ASCII mode
226 Transfer finished successfully.
5205 bytes sent in 0.000 seconds (11.28 Mbytes/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 does not require 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 30 TFTP application scenario



FIPS compliance

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

TFTP is not supported in FIPS mode.

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.	tftp-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.	tftp 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

Step	Command	Remarks
5. Download or upload a file in an IPv4 network.	tftp tftp-server { get put sget } <i>source-filename</i> [<i>destination-filename</i>] [dscp <i>dscp-value</i> source { interface <i>interface-type</i> <i>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 tftp 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</i> <i>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 tftp-server [-i <i>interface-type</i> <i>interface-number</i>] { get put sget } <i>source-filename</i> [<i>destination-filename</i>] [dscp <i>dscp-value</i> source { interface <i>interface-type</i> <i>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.
-

FIPS compliance

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

Storage medium naming rules

The device supports one flash memory and one USB disk. The name of the flash memory is **flash**. The name of the USB disk is **usba0**.

If the USB disk is partitioned, a partition is named by the storage medium type **usb**, the sequence number **a**, and the partition number. The partitions start at 0 and increment by 1. For example, the first partition of the USB disk is named **usba0**, and the second partition is named **usba1**.

File name formats

❗ IMPORTANT:

- Storage medium names and the **chassis** and **slot** strings are case sensitive and must be entered in lower case. The system will display that the file or directory does not exist if you enter a storage name, the **chassis** string, or the **slot** string in upper case.
 - Folder names and file names are case insensitive.
-

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.

Format	Description	Example
<code>[path/]file-name</code>	Specifies a file in a 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 (/).	- 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.
<code>drive:/[path/]file-name</code>	Specifies a file in a storage medium on the device. The <i>drive</i> argument represents the storage medium name. Typically, the storage medium name is flash or usb0. If the device has only one storage medium, the <i>drive</i> argument is optional.	flash:/test/a.cfg indicates a file named a.cfg in the test folder in the root directory of the flash memory.

Managing files

⚠ CAUTION:

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

The device provides the following file management functions:

- Display directory and file information.
- Display file contents.
- Rename, copy, move, remove, restore, delete, compress, decompress, archive, and extract files.
- Calculate the digests of files for file integrity verification.
- 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*.

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

Displaying file information

Perform this task in user view.

Task	Command
Display folder or file information.	dir [<i>/all</i>] [<i>file-url</i> <i>/all-file systems</i>]

Displaying the contents of a text file

Perform this task in user view.

Task	Command
Display the contents of a text file.	more <i>file-url</i>

Renaming a file

Perform this task in user view.

Task	Command
Rename a file.	rename <i>fileurl-source fileurl-dest</i>

Copying a file

Perform this task in user view.

Task	Command
Copy a file.	- In non-FIPS mode: copy <i>fileurl-source fileurl-dest</i> [source interface <i>interface-type interface-number</i>] - In FIPS mode: copy <i>fileurl-source fileurl-dest</i>

Moving a file

Perform this task in user view.

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

Compressing/decompressing a file

Perform the following tasks in user view:

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

Archiving/extracting files

Perform the following tasks in user view:

Task	Command
Archive files.	tar create [gz] archive-file <i>fileurl-dest</i> [verbose] source <i>fileurl-source-list</i> &<1-5>
Extract files.	tar extract archive-file <i>fileurl-dest</i> [verbose] [screen to <i>directory-name</i>]
Display the names of archived files.	tar list archive-file <i>fileurl-dest</i>

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 save storage space, periodically empty the recycle bin with the **reset recycle-bin** command.

Perform the following tasks in user view:

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



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 device supports multiple storage media. Each storage medium has a recycle bin of its own.

The device supports multiple storage media. If a storage medium is not partitioned, it has a recycle bin of its own. If a storage medium is partitioned, each partition has its own recycle bin.

A recycle bin is a folder named **.trash** in the root directory of the storage medium or partition.

To view which files or directories are in a recycle bin, use either of the following methods:

- Enter the storage medium or partition 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.	reset recycle-bin [/force]

Calculating the file digest

The digest of a file can be used to verify file integrity.

Perform this task in user view.

Task	Command
Calculate the digest of a file.	- Use the SHA-256 digest algorithm: sha256sum <i>file-url</i> - Use the MD5 digest algorithm: md5sum <i>file-url</i>

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, display, or remove a directory, and display or change the current working directory.

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

Displaying directory information

Perform this task in user view.

Task	Command
Display directory or file information.	dir [<i>/all</i>] [<i>file-url</i> <i>/all-file systems</i>]

Displaying the current working directory

Perform this task in user view.

Task	Command
Display the current working directory.	pwd

Changing the current working directory

Perform this task in user view.

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

Creating a directory

Perform this task in user view.

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

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.	rmdir <i>directory</i>

Managing storage media

CAUTION:

To avoid file system corruption:

Do not install or remove storage media or perform master/subordinate switchover while the system is repairing, formatting, partitioning, mounting, or unmounting a storage medium.

If you remove a storage medium while a folder or file on the storage medium is being accessed, the device might not recognize the storage medium when you reinstall it. To reinstall this kind of storage medium, complete one of the following tasks:

- If you were accessing a folder on the storage medium, change the current directory.
- If you were accessing a file on the storage medium, close the file.
- If another administrator was accessing the storage medium, unmount all partitions on the storage medium.

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

You cannot access a storage medium while another user is repairing, formatting, or partitioning the medium.

To access a storage medium after the medium is repaired, formatted, or partitioned, use one of the following methods:

- Specify the storage medium name for the command. For example, use **dir flash:/** to display all files and folders on the flash memory.
- Use the **cd** command to change to the storage medium before using the command. For example, use **cd flash:/** to change to the root directory of the flash memory, and then use **dir** to display all files and folders.

Repairing a storage medium

If part of a storage medium is inaccessible, use the **fixdisk** command to examine 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.

To format a storage medium that has been partitioned, you must format all the partitions individually, instead of formatting the medium as a whole. You can format a storage medium only when no one is accessing the medium.

Perform this task in user view.

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

Mounting or unmounting a storage medium

Generally, a hot-swappable storage medium is automatically mounted when it is connected to the device. If the system cannot recognize the storage medium, however, you must mount the storage medium before you can access it.

To remove a hot-swappable storage medium from the device, you must first unmount it to disconnect it from the device. Otherwise, files on the storage medium or even the storage medium itself might be damaged.

Restrictions and guidelines

To mount/unmount a partitioned storage medium, you must mount/unmount all the partitions individually, instead of mounting/unmounting the medium as a whole. To unmount a USB disk, make sure the system has recognized the USB disk and the USB disk LED is not blinking. Otherwise, the USB interface or USB disk might be damaged.

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

Configuration procedure

Perform one of the following tasks in user view as appropriate:

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

Partitioning a USB disk

A USB disk can be divided into logical devices called partitions. Operations on one partition do not affect the other partitions.

The following partitioning modes are available for USB disks:

- **Simple**—Specify the number of partitions. The system divides a USB disk into the specified number of partitions with the same size.
- **Interactive**—The system partitions a USB disk according to user input. Each partition must have a minimum of 32 MB of storage space.

Restrictions and guidelines

It is normal that the specified partition size and the actual partition size have an error less than 5% of the total memory.

Before partitioning a USB disk, perform the following tasks:

- Back up the files in the storage medium. The partition operation clears all data in the medium.
- If you are partitioning a USB disk, make sure the disk is not write protected. Otherwise, the partition operation will fail, and you must remount or reinstall the disk to restore access to the USB disk.
- Make sure no other users are accessing the medium. Otherwise, the partition operation fails.

After partitioning a USB disk, perform the following tasks:

- Reconfigure paths of application files to include the correct partition information.
- To make sure the first partition has sufficient storage space for startup system software image and configuration files, set the log file path to a different partition. By default, the system automatically saves log files to the second partition. If the path does not exist, use the **info-center logfile directory** command to change the path to avoid log loss. For more information about this command, see *Network Management and Monitoring Command Reference*.

Configuration procedure

Perform this task in user view.

Task	Command	Remarks
Partition a storage medium.	fdisk <i>medium-name</i> [<i>partition-number</i>]	By default, only one partition <code>usba0:/</code> is available on a USB disk.

Setting the operation mode for files and folders

The device supports the following file and folder operation modes:

- **alert**—The system prompts for confirmation when your operation might cause problems such as file corruption and data loss. This mode provides an opportunity to cancel a disruptive operation.
- **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

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.

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

Configuration types

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

Startup configuration

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

The following are sources of startup configuration:

- **Initial settings**—Initial values or states for parameters. If the device starts up with empty configuration, all parameters use their initial settings at startup.
No commands are available to display the initial settings. For more information about these settings, see the Default sections in the command references.
- **Factory defaults**—Product-specific default settings that are different from initial settings. The factory defaults are included in the .ipe software image file. If you do not configure the device to start up with the initial settings or a startup configuration file, the device loads the factory defaults to configure features at startup. If a parameter is not included in the factory defaults, the device uses its initial settings.
To display the factory defaults, use the **display default-configuration** command.
- **Startup configuration file**—Configuration file you specify in the Boot menus or CLI for startup. The file is called the "next-startup configuration file." After the file is loaded at startup, it is also called the "current startup configuration file." For high availability, you can specify two next-startup configuration files, one main and one backup (see "[Specifying a next-startup configuration file](#)").
To display the current startup configuration file and the next-startup configuration files, use the **display startup** command.
To display the contents of the configuration file for the next system startup, use the **display saved-configuration** command. This command does not display settings that have not been saved to the configuration file.

Running configuration

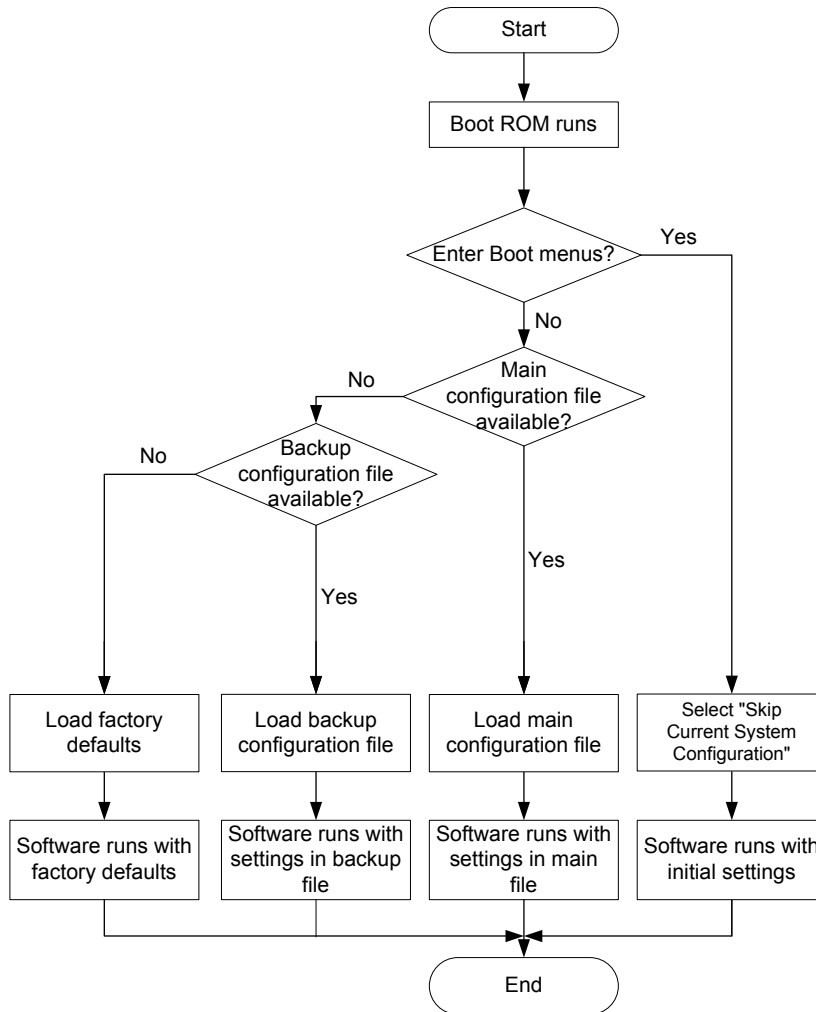
The running configuration includes unchanged startup settings and new settings. The running configuration is stored in the memory and is cleared at a device reboot or power off. To use the running configuration after a power cycling or reboot, save it to a configuration file.

To display the running configuration, use the **display current-configuration** command. The displayed configuration does not include parameters that use initial settings.

Startup configuration loading process

Figure 31 shows the configuration loading process during startup.

Figure 31 Configuration loading process during startup



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

1. If you access the Boot menu to select the **Skip Current System Configuration** option, the device starts up with empty configuration. All parameters use their initial settings.
2. If you do not access the Boot menus to select the **Skip Current System Configuration** option, the following process applies:
 - a. If you have specified a main startup configuration file, and this configuration file is available, the device starts up with this startup configuration file.
 - b. If you have not specified a main startup configuration file, or the specified main startup configuration file is not available, the device searches for the backup startup configuration file.

- c. If you have not specified a backup startup configuration file, or the specified file is not available, the device starts up with the factory defaults. If a parameter is not included in the factory defaults, its initial setting is used.

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. The device searches for a valid .cfg next-startup configuration file.
2. If one is found, the device 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, the device starts up with the .mdb file. If none is found, the device 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. To ensure a successful configuration load at startup, use a configuration file that was automatically created on the device or created by using the **save** command. If you edit the configuration file, make sure all edits are compliant with the requirements.

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:

```
#
local-user root class manage
password hash
$h$6$Twd73mLrN802vvD5$Cz1vgdpR4KoTiRQNE9pg33gU14Br2p1VgucZLSVyJL02huV5Syx/LfDI8R0LtV
ErJ/C31oq2rFtmNuyZf4STw==
service-type ssh telnet terminal
authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
#
interface Ten-GigabitEthernet1/0/1
```

```
port link-mode route
ip address 1.1.1.1 255.255.255.0
#
```

FIPS compliance

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

General configuration restrictions and guidelines

When you manage the next-startup configuration files, follow these restrictions and guidelines:

- Save the next-startup configuration files to the root directory of the default storage medium. The device loads startup configuration files only from the default storage medium. You can access the Boot menus to specify the built-in flash memory or the USB disk as the default storage medium.
- In a multichassis IRF fabric, make sure all member devices use the same type of storage medium as the default storage medium.
- If the USB disk is used to store the startup configuration files, do not remove the USB disk during the startup process. If you remove the USB disk on a device, one of the following consequences occurs:
 - In a single-chassis IRF fabric, the device will start up with the factory defaults.
 - In a multichassis IRF fabric, the device will leave the IRF fabric at startup and run the factory defaults.

Enabling configuration encryption

Configuration encryption enables the device to encrypt a startup configuration file automatically when it saves the running configuration. All HP devices running Comware V7 software use the same private key or public key to encrypt configuration files.

NOTE:

Only HP devices running Comware V7 software can decrypt the encrypted configuration files.

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

Restrictions and guidelines

On an IRF fabric, use the **display irf** command to verify that the IRF topology is correct before you save the running configuration. When a member device leaves because of an IRF split, the member device's settings are still retained in the running configuration and the next-startup configuration file. However, saving the running configuration will remove the member device's settings from the next-startup configuration file.

If you have saved the running configuration to the next-startup configuration file after an IRF split, use the following method to restore the settings of the member device:

1. Fix the split problem.
2. Reboot the IRF fabric after the member device rejoins the fabric.
3. Execute the **display current-configuration** command to make sure that the member device's settings are still retained in the running configuration.
4. Save the running configuration to the next-startup configuration file.

Using different methods to save 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 for saving 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, use either of the following command in any view:

Task	Command	Remarks
Save the running configuration to a configuration file without specifying the file as a next-startup configuration file.	save <i>file-url</i> [all slot <i>slot-number</i>]	N/A

Task	Command	Remarks
Save the running configuration to a configuration file and specify the file as a next-startup configuration file.	save [safely] [backup main] [force]	This command saves the configuration to a file on the default storage medium. For reliable configuration saving, HP recommends that you specify the safely keyword. If you specify only the safely keyword, the command saves the configuration to the main startup configuration file. If the force keyword is specified, the command saves the configuration to the existing next-startup configuration file. If the force keyword is not specified, the command allows you to specify a new next-startup configuration file.

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

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

Configuration task list

Tasks at a glance
(Required.) Configuring configuration archive parameters
(Required.) Perform either task: • Enabling automatic configuration archiving • Manually archiving the running configuration
(Required.) Rolling back configuration

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, all of the following events occur:

- The old configuration archives are regarded as common configuration files.
- The configuration archive counter is reset.
- The **display archive configuration** command no longer displays the old configuration archives.
- 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 to make room for the new archive.

Configuration guidelines

In an IRF fabric, the configuration archive function saves the running configuration only on the master device. To ensure that 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

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

To enable automatic configuration archiving:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable automatic configuration archiving and set the archiving interval.	archive configuration interval <i>minutes</i>	By default, this function is disabled. To display 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. Then, you can use the archive for configuration recovery if 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

Rolling back configuration

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 command lines in the configuration file are 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. This is 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 use the **save [safely] [backup | main] [force]** command to save the running configuration to a .cfg configuration file. The .cfg configuration file can be specified as both the main and backup next-startup configuration files.

Alternatively, you can use the **startup saved-configuration cfgfile [backup | main]** command to specify a .cfg configuration file as the main or backup next-startup configuration file. Make sure the specified configuration file is valid and saved to the root directory of each member device's default storage medium.

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

Task	Command	Remarks
Specify the next-startup configuration file.	startup saved-configuration <i>cfgfile</i> [backup main]	By default, no next-startup configuration file is specified. Use the display startup command and the display saved-configuration command in any view to verify the configuration. If you specify neither the backup keyword nor the main keyword, 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.

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

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

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

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>dest-addr [dest-filename]</i>	This command is not supported in FIPS mode.

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

To restore the main next-startup configuration file from a TFTP server, the device performs the following operations:

- Downloads a configuration file from a TFTP server to the root directory of each member's default storage medium.
- Specifies the file as the main next-startup configuration file.

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

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

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

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

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.

Delete the next-startup configuration file if one of the following events occurs:

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

If both the main and backup next-startup configuration files are deleted, the device uses factory defaults at the next startup.

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. Using only one of the commands removes the specified file attribute instead of deleting the file.

For example, if the **reset saved-configuration backup** command is executed, the backup next-startup configuration file setting is set to NULL. However, the file is still used as the main file. To delete the file, you must also execute the **reset saved-configuration main** command.

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 [module-name] interface [interface-type [interface-number]]]
Display the configuration differences between the current startup configuration file and the next-startup configuration file.	display current-configuration diff
Display the factory defaults.	display default-configuration

Task	Command
Display the configuration differences between two configuration files.	• display diff configfile <i>file-name-s</i> { configfile <i>file-name-d</i> current-configuration startup-configuration } • display diff current-configuration { configfile <i>file-name-d</i> startup-configuration } • display diff startup-configuration { configfile <i>file-name-d</i> current-configuration }
Display the contents of the configuration file for the next system startup.	display saved-configuration
Display the names of the configuration files for this startup and the next startup.	display startup
Display the valid configuration in the current view.	display this

Upgrading software

Overview

Software upgrade enables you to add new features and fix bugs. This chapter describes types of software and procedures to upgrade software from the CLI without using ISSU. For a comparison of all software upgrade methods, see "[Upgrade methods](#)."

Software types

The following software types are available:

- **Boot ROM image**—A .bin file that contains a basic segment and an extended segment. The basic segment is the minimum code that bootstraps the system. The extended segment enables hardware initialization and provides system management menus. You can use these menus to load software and the startup configuration file or manage files when the device cannot start up correctly. For easy software compatibility management, the Boot ROM image is contained in the Boot image file. The Boot ROM image is upgraded automatically when the Boot image is upgraded.
- **Comware image**—Includes the following image subcategories:
 - **Boot image**—A .bin file that contains the Boot ROM image and 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. To have advanced features, you must purchase feature images.
 - **Feature image**—A .bin file that contains advanced software features. Users purchase feature images as needed.
 - **Patch image**—A .bin file irregularly released for fixing bugs without rebooting the device. A patch image 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 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 decompresses the file automatically, loads the .bin boot and system images, and sets them as startup software images.

Software file naming conventions

Software image file names use the *chassis-comware version-image type-release* format, for example, 5700-CMW710-SYSTEM-R2311.bin and 5700-CMW710-BOOT-R2311.bin. This document uses **boot.bin** and **system.bin** as boot and system image file names.

Comware image redundancy and loading procedure

You can specify two lists of startup Comware software images: one main (primary) and one backup.

The boot and system images in a startup software image list must be the same version.

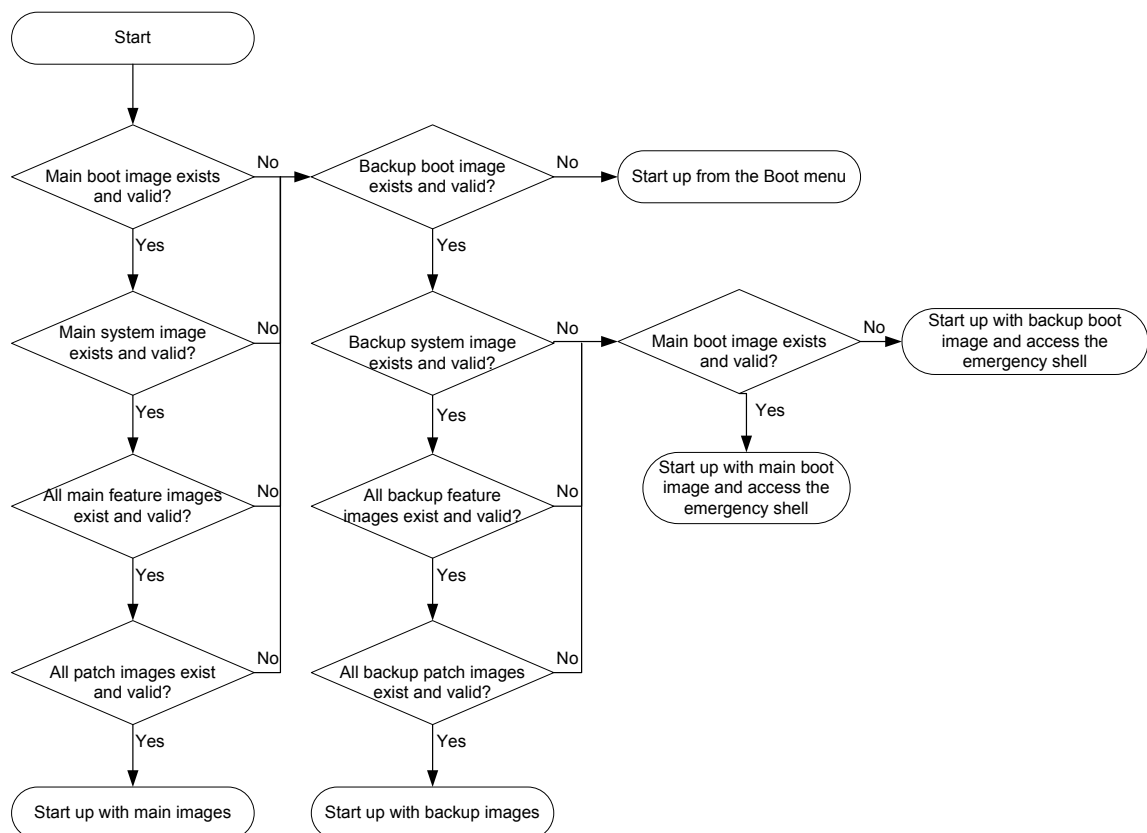
The system always attempts to start up with the main images. If any main images do not exist or are invalid, the system tries the backup images. [Figure 32](#) shows the entire Comware image loading procedure.

In this procedure, both the main and backup image lists have feature and patch images. If an image list does not have either feature images or patch images, the system starts up with the main boot and system images after they pass verification.

If both the main and backup boot images do not exist or are invalid, connect to the console port, and power cycle the device to load a boot image from the Boot menu. For more information about downloading and loading a boot image, see the release notes for the software version.

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 32 Comware image loading procedure

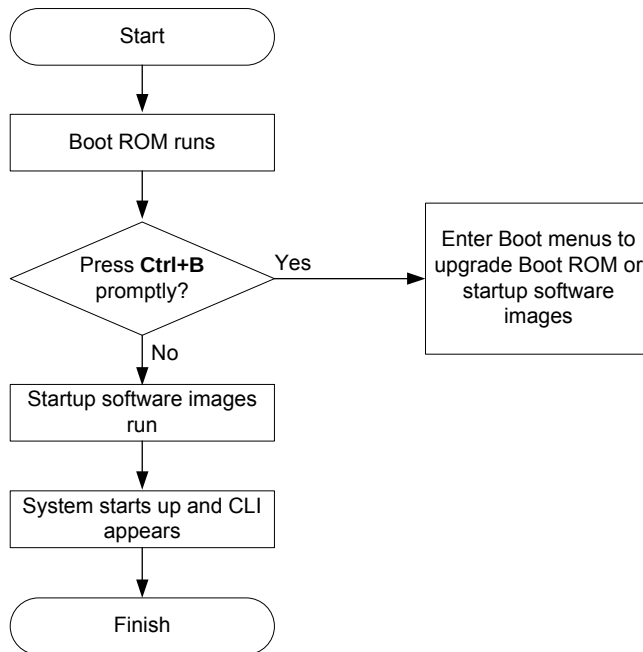


System startup process

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 33](#).

In an IRF system, this process applies to the parent fabric.

Figure 33 System startup process



Upgrade methods

Upgrading method	Software types	Remarks
Upgrading from the CLI:		
Upgrading software without using ISSU	• Boot ROM image • Comware images (excluding patches)	This method is disruptive. You must reboot the entire device to complete the upgrade.
Upgrading software through a warm reboot	Comware images	You can perform a warm reboot only on standalone devices. Compared to upgrading software through a reboot, warm reboot reduces the service downtime.
Performing an ISSU	Comware images	The ISSU method enables a software upgrade without service interruption. Use this method for an IRF fabric. For more information about ISSU, see " Performing an ISSU ."
Installing hotfixes	Comware images	Hotfixes repair software defects without requiring a reboot. Hotfixes do not add new features to system software images. For more information about installing hotfixes, see " Performing an ISSU ."

Upgrading method	Software types	Remarks
Upgrading from the Boot menu	• Boot ROM image • Comware software images	Use this method when the device cannot start up correctly. ! IMPORTANT: Upgrade an IRF fabric from the CLI rather than the Boot menu. The Boot menu method increases the service downtime, because it requires that you upgrade the member devices one by one.

This chapter only covers upgrading software from the CLI without using ISSU.

Upgrade procedure summary

To upgrade software from the CLI without using ISSU:

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 upgrades the Boot ROM automatically when it upgrades 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. Reboot the entire IRF fabric.
5. Verify the upgrade.

Upgrade restrictions and guidelines

The switch can start up from the built-in flash memory or a removable USB disk. HP recommends that you store the startup images in the built-in flash memory. If you store the startup images on a USB disk, do not remove the USB disk before the the startup is complete.

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 and startup software image.

3. Use the **dir** command to verify that all IRF member devices have sufficient storage space for the upgrade images. If the storage space is not sufficient, delete unused files by using the **delete** command. For more information, see "[Managing the file system](#)."
4. Configure FTP or TFTP settings.
5. Use FTP or TFTP to download the upgrade image file to the root directory of a storage medium on any one of the member devices.

For more information about FTP and TFTP, see "[Configuring FTP](#)" and "[Configuring TFTP](#)."

Preloading the Boot ROM image to Boot ROM

Step	Command	Remarks
1. Load the upgrade Boot ROM image to the 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

You can specify the startup image file for IRF member devices in bulk, or one by one.

Specifying the startup image file for all devices in bulk

Perform this task in user view.

Step	Command	Remarks
1. Specify the main or backup startup images for all devices.	• Use an .ipe file for upgrade: boot-loader file <i>ipe-filename</i> all { backup main } • Use .bin files for upgrade: boot-loader file boot <i>boot-package</i> system <i>system-package</i> [feature <i>feature-package</i>&<1-30>] all { backup main }	N/A
2. Save the running configuration.	save	This step ensures that any configuration you have made can survive a reboot.
3. Reboot the IRF system.	reboot	At startup, each IRF member device reads the preloaded Boot ROM image to RAM, and loads the startup images.
4. (Optional.) Verify the software image settings.	display boot-loader [<i>slot-number</i>]	Verify that the current software images are the same as the startup software images.

Specifying the startup image file for devices one by one

Step	Command	Remarks
1. Specify the main or backup startup images for the master device.	- Use an .ipe file for upgrade: boot-loader file <i>ipe-filename</i> slot <i>slot-number</i> { backup main } - Use .bin files for upgrade: boot-loader file boot <i>boot-package</i> system <i>system-package</i> [feature <i>feature-package</i>&<1-30>] slot <i>slot-number</i> { backup main }	N/A
2. Specify the main startup images for each subordinate device.	- Use an .ipe file for upgrade: boot-loader file <i>ipe-filename</i> slot <i>slot-number</i> { backup main } - Use .bin files for upgrade: boot-loader file boot <i>boot-package</i> system <i>system-package</i> [feature <i>feature-package</i>&<1-30>] slot <i>slot-number</i> { backup main } - Use the image list that the master device started up with for upgrade: boot-loader update { all slot <i>slot-number</i> }	Skip this step if you have only one device. If you use the image list that the master device started up with, make sure you understand the following requirements and upgrade results: - If an ISSU upgrade has been performed, use the install commit command to update the main startup images on the master device before software synchronization. The command ensures startup image consistency among IRF member devices. - If the master device started up with the main startup image list, its main startup images are synchronized to the subordinate devices. This synchronization occurs regardless of whether any change has occurred to this image list. - If the master device started up with the backup startup list, its backup startup images are synchronized to the subordinate devices. This synchronization occurs regardless of whether any change has occurred to this image list. - Startup image synchronization will fail if any software image being synchronized is corrupted or is not available.
3. Save the running configuration.	save	This step ensures that 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, and loads the startup 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.

Upgrading software by performing a warm reboot

You can perform a warm reboot only when the device is operating as a standalone device.

You can perform a warm reboot in the following situations:

- Upgrade Comware images without upgrading the Boot ROM. The warm-reboot method directly loads and executes Comware software images in the memory instead of booting the Comware images from the Boot ROM. Compared to upgrading software through the **boot-loader** command, warm reboot reduces the service downtime.
- Upgrade only a specific image, for example, upgrade only the system image. When you upgrade feature images through warm reboot, you only need to specify upgrade images for features you are upgrading. The warm-reboot method replaces the old images for the specific features instead of overwriting the entire software list as does the **boot-loader** command.

The system checks for software version incompatibility during the warm reboot. If any incompatibility exists, software upgrade fails.

Perform this task in user view.

Step	Command	Remarks
1. Save the running configuration.	save	This step ensures that any configuration you have made can survive a reboot.
2. Specify main startup images for the device and perform a warm reboot.	• Use an .ipe file for upgrade: warm-reboot [file ipe ipe-filename] • Use .bin files for upgrade: warm-reboot [file { boot boot-package system system-package feature feature-package&<1-30> }]	Upgrade files must be saved in the root directory of the storage medium. If the storage medium is partitioned, save the files to the root directory of the first partition. If you do not specify upgrade files, the switch reboots without upgrading software.
3. (Optional.) Verify the software image settings.	display boot-loader [slot slot-number]	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]

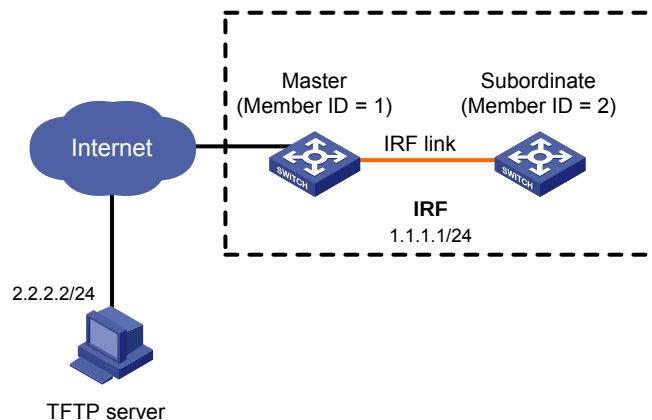
Non-ISSU software upgrade examples

Example of software upgrade through a reboot

Network requirements

Use the file **startup-a2105.ipe** to upgrade software images for the IRF fabric in [Figure 34](#).

Figure 34 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 the flash on the master device.

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

Back up the image file to **startup-a2105-backup.ipe**. Skip this step if the flash 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 device to complete the upgrade.

```
<Sysname> reboot
```

Verifying the configuration

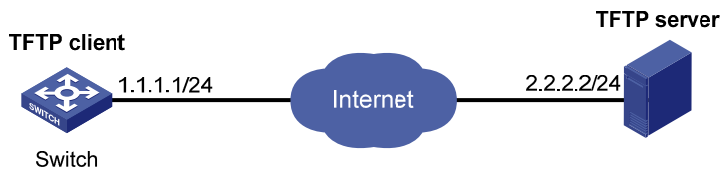
```
# Verify that the device is running the correct software.  
<Sysname> display version
```

Example of software upgrade through a warm reboot

Network requirements

Use the file **feature.bin** to upgrade the feature image file for the device.

Figure 35 Network diagram



Configuration procedure

```
# Configure IP addresses and routes. Make sure the device and the TFTP server can ping each other.  
(Details not shown.)
```

```
# Configure TFTP settings on both the device and the TFTP server. (Details not shown.)
```

```
# Use TFTP to download the image file feature.bin from the TFTP server to the root directory of the flash  
memory.
```

```
<Sysname> tftp 2.2.2.2 get feature.bin
```

```
# Specify feature.bin as a main startup image file and perform a warm reboot.
```

```
<Sysname> warm-reboot file feature flash:/feature.bin
```

This operation will delete the rollback point information for the previous upgrade and maybe get unsaved configuration lost. Continue? [Y/N]:Y

Upgrade summary according to following table:

```
flash:/feature.bin
```

Running Version	New Version
Alpha 7122	Alpha 7123

Slot	Upgrade Way
1	Warm Reboot

Upgrading software images to compatible versions. Continue? [Y/N]:y

Verifying the configuration

```
# Verify that the device is running the correct software.  
<Sysname> display version
```

Performing an ISSU

ISSU overview

The In-Service Software Upgrade (ISSU) feature upgrades software with a minimum amount of downtime.

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

- **Separation of service features from basic functions**—Device software is segmented into boot, system, and feature images. The images can be upgraded individually.
- **Independence between service features**—Features run independently. One feature can be added or upgraded without affecting the operation of the system or other features.
- **Support for hotfix**—Patch images are available to fix system bugs without a system reboot.
- **Hardware redundancy**—In an IRF fabric, one member device can be upgraded while other member devices are providing services.

For more information about images, see "[Upgrading software](#)."

ISSU methods

ISSU supports the following upgrade types:

- **Compatible upgrade**—The running software version is compatible with the upgrade software version. This upgrade type supports the ISSU methods in [Table 12](#).
- **Incompatible upgrade**—The running software version is incompatible with the upgrade software version. The two versions cannot run concurrently.

This upgrade type supports only one upgrade method (also called incompatible upgrade). This method requires a cold reboot. It is service disruptive if hardware redundancy is not available.

Table 12 ISSU methods for compatible upgrade

ISSU method	Description
Incremental upgrade: • Service Upgrade • File Upgrade	Upgrades only segments that contain differences between the new and old software versions. • Service upgrade—Upgrades service features. The upgrade does not affect the operation of features that are not being upgraded. • File upgrade—Upgrades hidden system program files. The system can provide services during the upgrade.
ISSU Reboot	Reboots CPUs to complete software upgrade. During the reboot, the data plane can still forward traffic. This method saves all data (running, configuration, and hardware) and status to memory before rebooting CPUs. For services that require regular communication with their peers, this method uses protocol agents to maintain their connectivity and status. After the reboot, all data is restored to CPU.

ISSU method	Description
Reboot	 CAUTION: The Reboot method is service disruptive if the device stands alone. HP recommends that you schedule the downtime carefully to minimize the upgrade impact on the services. This method reboots both the control and data planes to complete the software upgrade.

ISSU commands

ISSU provides the **install** and **issu** command sets. After you identify the ISSU method, use [Table 13](#) to choose the command set you want to use.

Table 13 Command set comparison

Item	issu commands	install commands
Upgrade types	- Compatible. - Incompatible.	Compatible.
Patch install/uninstall	Not supported.	Supported.
Upgrade mode	Chassis by chassis.	Chassis by chassis.
Impact on the system	Large.	Small.
Technical skill requirements	Low. HP recommends that you use this command set.	High. Administrators must have extensive system knowledge and understand the impact of each upgrade task on the network.

Verifying the device operating status

Use the **display device** command to verify that all member devices are operating correctly.

Preparing the upgrade images

1. Use the **dir** command to verify that all member devices has sufficient storage space for the upgrade images. If the storage space is not sufficient, delete unused files by using the **delete** command. For more information, see "[Managing the file system](#)."
2. Use FTP or TFTP to transfer upgrade image files to the root directory of any storage medium in the IRF fabric.

Identifying the ISSU method

1. Execute the **display version comp-matrix file** command for the upgrade image version.
2. Check the **Version compatibility list** field.
 - If the running software version is in the list, a compatible upgrade is required.

- If the running software version is not in the list, an incompatible upgrade is required.
3. Identify the ISSU method:
 - If a compatible upgrade is required, check the **Upgrade Way** field to identify the ISSU method. For more information about ISSU methods, see [Table 12](#).
 - If an incompatible upgrade is required, check the end of command output for the **Incompatible upgrade** string.

Verifying feature status

For service continuity during ISSU, configure the following feature settings:

Feature	Setting requirements
Ethernet link aggregation	Use the long LACP timeout interval (the lacp period short command is not configured) on all member ports in dynamic aggregation groups.
IRF	Configure IRF bridge MAC persistence as follows: • Compatible upgrade—Configure the irf mac-address persistent timer or irf mac-address persistent always command. • Incompatible upgrade—Configure the irf mac-address persistent always command if the bridge MAC address is the MAC address of the device for which you want to execute the issu load command.

For an **ISSU Reboot** upgrade on a single-member IRF fabric, also verify that the following features are disabled:

Feature	Remarks
Spanning tree feature	If the spanning tree feature is enabled, service discontinuity might occur during the upgrade because the feature advertises the network topology change.
Dynamic Ethernet link aggregation	During an ISSU reboot, only static aggregation is supported, and dynamic aggregate interfaces might not be able to provide services.
CFD	If CFD is enabled, the CFD CC function will be disabled during an ISSU reboot, which results in traffic abnormality.
DLDLP	If DLDLP is enabled, the peer device might consider a link a unidirectional link and shut down the port because it cannot receive probe packets.
Loop detection	If loop detection is enabled, the peer device might enable looped ports because of false loop removal detection.

Determining the upgrade procedure

1. Use [Table 13](#) to choose an upgrade command set, depending on the ISSU method.
2. Identify the hardware redundancy condition.
 ISSU can maintain service continuity only when the IRF fabric has multiple members and uses the ring topology.

! IMPORTANT:

If hardware redundancy is not available, service discontinuity is not avoidable. Make sure you understand the impact of the upgrade on the network.

3. Choose the correct procedure from the procedures described in "Performing an ISSU by using `issu` commands" or "Performing an ISSU by using `install` commands."

Understanding ISSU guidelines

During an ISSU, use the following guidelines:

- In a multiuser environment, make sure no other administrators access the device while you are performing the ISSU.
- Do not perform any of the following tasks during an ISSU:
 - Reboot, add, or remove member devices.
 - Execute commands that are not related to the ISSU.
 - Modify, delete, or rename image files.
- You cannot use both **`install`** and **`issu`** commands for an ISSU. However, you can use **`display issu`** commands with both command sets.

After an ISSU, you must log in to the device again before you can configure the device.

Logging in to the device through the console port

Log in to the device through the console port after you finish all the preparation tasks and understand all the ISSU guidelines. If you use Telnet or SSH, you might be disconnected from the device before the ISSU is completed.

Saving the running configuration

Use the **`save`** command to save the running configuration.

Performing an ISSU by using `issu` commands

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

Upgrading a multichassis IRF fabric

On a multichassis IRF fabric, always start ISSU with a subordinate member.

Performing a compatible upgrade

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

Step	Command	Remarks
2. (Optional.) Set the automatic rollback timer.	issu rollback-timer <i>minutes</i>	By default, the automatic rollback timer is set to 45 minutes. This timer starts 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 images.
3. Return to user view.	quit	N/A
4. Load the upgrade images as main startup software images on subordinate members.	- Use .bin files: issu load file { boot filename system filename feature filename <1-30> } * slot slot-number - Use an .ipe file: issu load file ipe ipe-filename slot slot-number <1-9>	Specify the member ID of a subordinate member for the <i>slot-number</i> argument.
5. Perform a master/subordinate switchover.	issu run switchover	N/A
6. (Optional.) Accept the upgrade and delete the automatic rollback timer.	issu accept	N/A
7. Upgrade the remaining members to complete the ISSU.	issu commit chassis <i>chassis-number</i>	 IMPORTANT: After executing the command for one member, you must wait for the member to restart and join the IRF fabric before you execute the command for another member. Repeat the issu commit command to upgrade the remaining members one by one, including the original master. To manually roll back to the original software images during this ISSU process, use the issu rollback command. For more information about rollback, see <i>Fundamentals Command Reference</i>.

Performing an incompatible upgrade

Perform this task in user view.

Step	Command	Remarks
1. Load the upgrade images as main startup software images on subordinate members.	- Use .bin files: issu load file { boot filename system filename feature filename <1-30> } * slot slot-number <1-9> - Use an .ipe file: issu load file ipe ipe-filename slot slot-number <1-9>	Specify the member ID of a subordinate member for the <i>slot-number</i> argument. In a ring-topology IRF fabric, HP recommends that you specify half of the subordinate members for this command to reduce service interruption. Make sure the specified subordinate members are physically connected.
2. Perform a master/subordinate switchover to complete the ISSU process.	issu run switchover	To roll back to the original software images during this ISSU process, use the issu rollback command. This ISSU process does not support automatic rollback. For more information about rollback, see <i>Fundamentals Command Reference</i>.
3. Verify that the ISSU is finished.	display issu state	If the ISSU state field displays Init , the ISSU is finished.

Upgrading a single-chassis IRF fabric

Performing a service upgrade or file upgrade

Perform this task in user view.

Step	Command	Remarks
1. Load the upgrade images as main startup software images.	- Use .bin files: issu load file { boot filename system filename feature filename <1-30> } * slot slot-number - Use an .ipe file: issu load file ipe ipe-filename slot slot-number	Specify the member ID of the device for the <i>slot-number</i> argument.
2. Complete the ISSU process.	issu commit slot slot-number	Specify the member ID of the device for the <i>slot-number</i> argument. To roll back to the original software images during this ISSU process, use the issu rollback command. This ISSU process does not support automatic rollback. For more information about rollback, see <i>Fundamentals Command Reference</i>.
3. Verify that the ISSU is finished.	display issu state	If the ISSU state field displays Init , the ISSU is finished.

Performing a reboot/ISSU reboot/incompatible upgrade

Step	Command	Remarks
1. Load the upgrade images as main startup software images.	- Use .bin files: issu load file { boot filename system filename feature filename <1-30> } * slot slot-number - Use an .ipe file: issu load file ipe ipe-filename slot slot-number	Specify the member ID of the device for the <i>slot-number</i> argument.
2. Verify that the ISSU is finished.	display issu state	If the ISSU state field displays Init , the ISSU is finished.

Performing an ISSU by using install commands

ISSU task list

Tasks at a glance	Remarks
(Optional.) Decompressing an .ipe file	To use install commands for upgrade, you must use .bin image files. If the upgrade file is an .ipe file, perform this task before you use install commands for upgrade.
(Required.) Perform one of the following tasks to update software: - Installing or upgrading software images - Installing or upgrading images except for patches - Installing patch images - Uninstalling feature or patch images - Uninstalling feature images - Uninstalling patch images	Perform an activate operation to install new images or upgrade existing images. Perform an inactivate operation to uninstall feature or patch images. An image is added to or removed from the current software image list when it is activated or deactivated.
(Optional.) Rolling back the running software images	Perform this task to roll back running software image status after activate or deactivate operations. A commit operation removes all rollback points. You can perform this task only before software changes are committed.
(Optional.) Aborting a software activate/deactivate operation	You can perform this task while an image is being activated or deactivated. This task is available only for service upgrade or file upgrade.
(Optional.) Committing software changes	This task updates the main startup image list with the changes. If service upgrade or file upgrade is performed, you must perform this task for the changes to take effect after a reboot.

Tasks at a glance	Remarks
(Optional.) Verifying software images	Perform this task to verify that the software changes are correct.
(Optional.) Removing inactive software images	Perform this task to remove images

Decompressing an .ipe file

Perform this task in user view.

Step	Command
1. (Optional.) Identify images that are included in the .ipe file.	display install ipe-info
2. Decompress the .ipe file.	install add <i>ipe-filename medium-name:</i>

Installing or upgrading software images

Use one of the following methods to perform this task:

- **Chassis by chassis**—Activate all the images on one member device, and then move to the next member device.
- **Image by image**—Activate one image on all member devices before activating another image.

When you install an image, you must begin with the master device.

When you upgrade an image, you must begin with a subordinate device.

Installing or upgrading images except for patches

Perform this task in user view.

Step	Command
1. (Optional.) Identify the ISSU method and possible impacts of the upgrade.	install activate { boot <i>filename</i> system <i>filename</i> feature <i>filename</i> &<1-30> } * slot <i>slot-number</i> test
2. Activate images.	install activate { boot <i>filename</i> system <i>filename</i> feature <i>filename</i> &<1-30> } * slot <i>slot-number</i>

Installing patch images

Perform this task in user view.

Task	Command
Activate patch images.	install activate patch <i>filename</i> { all slot <i>slot-number</i> }

Uninstalling feature or patch images

The uninstall operation only removes images from the current software image list. For the change to take effect after a reboot, you must perform a commit operation to remove the images from the main startup image list.

Uninstalled images are still stored on the storage medium. To permanently remove the images, execute the **install remove** command. For more information, see "[Removing inactive software images](#)."

Boot and system images cannot be uninstalled.

Uninstalling feature images

Perform this task in user view.

Task	Command
Deactivate feature images.	install deactivate feature <i>filename</i> &<1-30> slot <i>slot-number</i>

Uninstalling patch images

Perform this task in user view.

Task	Command
Deactivate patch images.	install deactivate patch { all <i>filename</i> slot <i>slot-number</i> }

Rolling back the running software images

For each service or file upgrade performed through activate or deactivate operation, the system creates a rollback point. The rollback points are retained until any of the following event occurs:

- An ISSU reboot or reboot upgrade is performed.
- The **install commit** command is executed.

After an ISSU reboot or reboot upgrade is performed, you can roll back the running software images only to the status before any activate or deactivate operations are performed.

After a commit operation is performed, you cannot perform a rollback.

For a rollback to take effect after a reboot, you must perform a commit operation to update the main startup software image list.

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

Step	Command	Remarks
1. (Optional.) Display available rollback points.	display install rollback	A maximum of 50 rollback points are available for service and file upgrades. The earliest rollback point is removed if this limit has been reached when a rollback point is created.
2. Roll back the software.	install rollback to { <i>point-id</i> original }	N/A

Aborting a software activate/deactivate operation

This task is available only for service upgrade or file upgrade performed through activate or deactivate operation. After the operation is aborted, the system runs with the software images that it was running with before the operation.

Step	Command
1. Press Ctrl+C while a software image is being activated or deactivated.	N/A
2. Abort a software activate/deactivate operation in user view.	install abort [<i>job-id</i>]

Committing software changes

If the ISSU method is service upgrade or file upgrade for an activate or deactivate operation, the main startup image list does not update with the changes. The software changes are lost at reboot. For the changes to take effect after a reboot, you must commit the changes.

Perform this task in user view.

Task	Command	Remarks
Commit the software changes.	install commit	This command commits all software changes.

Verifying software images

Perform this task to verify the following items:

- **Integrity**—Verify that the boot, system, and feature images are integral.
- **Consistency**—Verify that the same active images are running across the entire system.
- **Software commit status**—Verify that the active images are committed as needed.

If an image is not integral, consistent, or committed, use the **install activate**, **install deactivate**, and **install commit** commands as appropriate to resolve the issue.

Perform this task in user view.

Task	Command
Verify software images.	install verify

Removing inactive software images

Removing a software image deletes the image file permanently. You cannot use the **install rollback to** command after the operation.

Perform this task in user view.

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

Displaying and maintaining ISSU

The **display issu state** command applies only to an ISSU that uses the **issu** series commands. All the other **display** commands and all **reset** commands can be used during an ISSU, regardless of whether the **install** or **issu** commands are used.

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 log entries.	display install log [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-filename</i>
Display rollback point information.	display install rollback
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 log entries.	reset install log-history oldest <i>log-number</i>
Clear ISSU rollback points.	reset install rollback oldest <i>point-id</i>

Troubleshooting ISSU

Failure to execute the issu load/issu run switchover/issu commit/install activate/install deactivate command

Symptom

The following commands cannot be executed:

- **issu commands**—**issu load**, **issu run switchover**, and **issu commit**.
- **install commands**—**install activate** and **install deactivate**.

Solution

To resolve this issue:

1. Use the **display device** command to verify that all cards are not in **Fault** state.
2. Use the **display system internal ha service-group** command to verify that the **Action** field is **0** for each service.
3. If the problem persists, contact HP Support.

ISSU examples for using issu commands

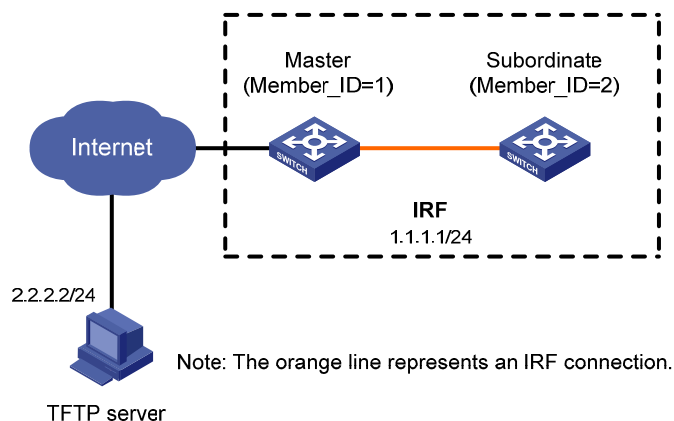
Software image upgrade to a compatible version

Upgrade requirements

As shown in Figure 36, the IRF fabric has two members.

Upgrade feature1 from R0201 to R0202. The two versions are compatible.

Figure 36 Network diagram



Upgrade procedure

Save the running configuration.

```
<Sysname> save
```

Download the image file that contains the feature1 image from the TFTP server.

```
<Sysname> tftp 2.2.2.2 get feature1-r0202.bin
```

% Total	% Received	% Xferd	Average Speed	Time	Time	Time	Current
			Dload Upload	Total	Spent	Left	Speed
100	256	100	256	0	0	764	0
--:--:--	--:--:--	--:--:--	--:--:--	--:--:--	--:--:--	--:--:--	810

Display active software images.

```
<Sysname> display install active
```

Active packages on slot 1:

flash:/boot-r0201.bin

flash:/system-r0201.bin

flash:/feature1-r0201.bin

Active packages on slot 2:

flash:/boot-r0201.bin

```
flash:/system-r0201.bin
flash:/feature1-r0201.bin
```

Identify the ISSU method to be used for the upgrade and view the possible impact of the upgrade.

```
<Sysname> display version comp-matrix file feature flash:/feature1-r0202.bin
Feature image: flash:/feature1-r0202.bin
```

```
Version:
V700R001B31D002
Version Compatibility List:
V700R001B31D001
V700R001B31D002
Version Dependency System List:
V700R001B31D001
V700R001B31D002
```

Slot	Upgrade Way
1	Service Upgrade
2	Service Upgrade

Influenced service according to following table on slot 1:

```
flash:/feature1-r0202.bin
feature1
```

Influenced service according to following table on slot 2:

```
flash:/feature1-r0202.bin
feature1
```

The output shows that an incremental upgrade is recommended. The feature1 module will be rebooted during the upgrade process.

Upgrade feature1 on the subordinate member.

```
<Sysname> issu load file feature flash:/feature1-r0202.bin slot 2
```

This operation will delete the rollback point information for the previous upgrade and maybe get unsaved configuration lost. Continue? [Y/N]:y

Upgrade summary according to following table:

Copying file flash:/feature1-r0202.bin to slot2#flash:/feature1-r0202.bin.....Done.

```
flash:/feature1-r0202.bin
```

Running Version	New Version
Alpha 0201	Alpha 0202

Slot	Upgrade Way
2	Service Upgrade

Upgrading software images to compatible versions. Continue? [Y/N]: y

Perform a master/subordinate switchover.

```
<Sysname> issu run switchover
```

Upgrade summary according to following table:

```
flash:/feature1-r0202.bin
```

Running Version	New Version
Alpha 0201	Alpha 0202

```

Slot                               Switchover Way
1                                 Active standby process switchover
Upgrading software images to compatible versions. Continue? [Y/N]: y
# Upgrade the feature on the original master.
<Sysname> issu commit slot 1
Upgrade summary according to following table:

flash:/feature1-r0202.bin
Running Version                    New Version
Alpha 0201                        Alpha 0202

Slot                               Upgrade Way
1                                 Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]: y
# Verify that both members are running the new image.
<Sysname> display install active
Active packages on slot 1:
flash:/boot-r0201.bin
flash:/system-r0201.bin
flash:/feature1-r0202.bin
Active packages on slot 2:
flash:/boot-r0201.bin
flash:/system-r0201.bin
flash:/feature1-r0202.bin

```

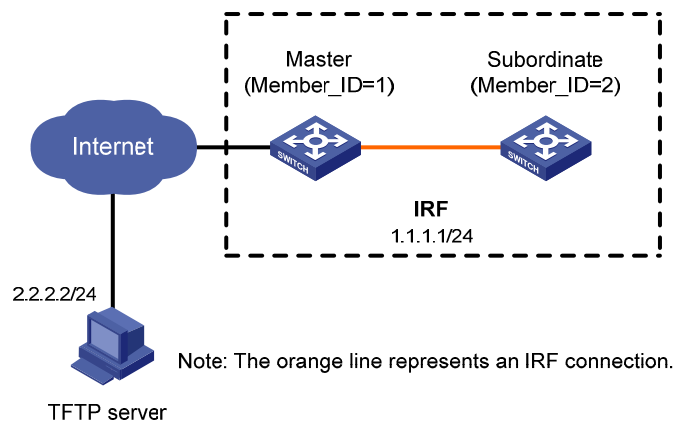
Software image upgrade to an incompatible version

Upgrade requirements

As shown in [Figure 37](#), the IRF fabric has two members.

Upgrade feature1 from R0201 to R0202. The two versions are incompatible.

Figure 37 Network diagram



Upgrade procedure

Save the running configuration.

<Sysname> save

Download the image file that contains the R0202 feature1 image from the TFTP server.

<Sysname> tftp 2.2.2.2 get feature1-r0202.bin

% Total		% Received		% Xferd		Average Speed		Time	Time	Time	Current
						Dload	Upload	Total	Spent	Left	Speed
100	256	100	256	0	0	764	0	--:--:--	--:--:--	--:--:--	810

Display active software images.

<Sysname> display install active

Active packages on slot 1:

flash:/boot-r0201.bin

flash:/system-r0201.bin

flash:/feature1-r0201.bin

Active packages on slot 2:

flash:/boot-r0201.bin

flash:/system-r0201.bin

flash:/feature1-r0201.bin

Identify the ISSU method to be used for the upgrade and view the possible impact of the upgrade.

<Sysname> display version comp-matrix file feature flash:/feature1-r0202.bin

Feature image: flash:/feature1-r0202.bin

Version:

V700R001B31D002

Version Compatibility List:

V700R001B31D002

Version Dependency System List:

V700R001B31D001

V700R001B31D002

Incompatible upgrade.

The output shows that the two versions are incompatible. The cards will be rebooted for the upgrade.

Upgrade feature1 on the subordinate member.

<Sysname> issu load file feature flash:/feature1-r0202.bin slot 2

This operation will delete the rollback point information for the previous upgrade and maybe get unsaved configuration lost. Continue? [Y/N]:y

Copying file flash:/feature1-r0202.bin to slot2#flash:/feature1-r0202.bin.....Done.

Upgrade summary according to following table:

flash:/feature1-r0202.bin

Running Version

New Version

Alpha 0201

Alpha 0202

Slot

Upgrade Way

2

Reboot

Upgrading software images to incompatible versions. Continue? [Y/N]: y

Upgrade feature1 on the original master.

<Sysname> issu run switchover

Upgrade summary according to following table:

```

flash:/feature1-r0202.bin
Running Version          New Version
Alpha 0201              Alpha 0202

Slot                    Upgrade Way
1                      Reboot
Upgrading software images to incompatible versions. Continue? [Y/N]: y
# Verify that both members are running the new image.
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0202.bin
Active packages on slot2:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0202.bin

```

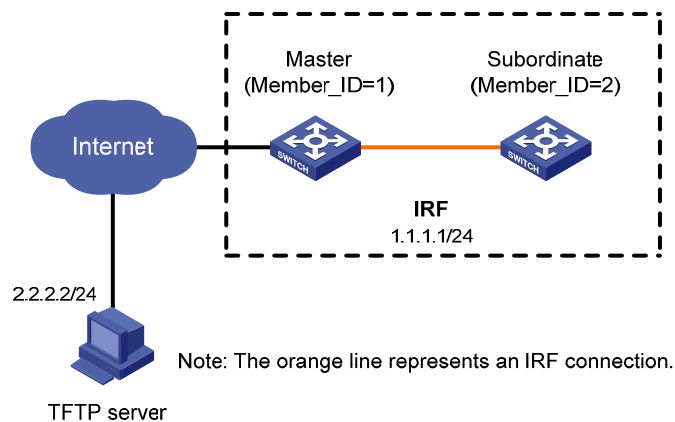
Software image rollback example

Rollback requirement

As shown in [Figure 38](#), the IRF fabric has two members.

Roll back feature1 from R0202 to R0201 after upgrading it from R0201 to R0202. The two versions are compatible.

Figure 38 Network diagram



Rollback procedure

Save the running configuration.

```
<Sysname> save
```

Download the image file that contains the R0202 feature1 image from the TFTP server.

```
<Sysname> tftp 2.2.2.2 get feature1-r0202.bin
```

% Total	% Received	% Xferd	Average Speed	Time	Time	Time	Current
			Dload Upload	Total	Spent	Left	Speed
100	256k	100	256k	0	0	764k	0

```

# Display active software images.
<Sysname> display install active
Active packages on slot 1:
    flash:/boot-r0201.bin
    flash:/system-r0201.bin
    flash:/feature1-r0201.bin
Active packages on slot 2:
    flash:/boot-r0201.bin
    flash:/system-r0201.bin
    flash:/feature1-r0201.bin

# Identify the ISSU method to be used for the upgrade and view the possible impact of the upgrade.
<Sysname> display version comp-matrix file feature flash:/feature1-r0202.bin
Feature image: flash:/feature1-r0202.bin
Version:
V700R001B31D002
Version Compatibility List:
V700R001B31D001
V700R001B31D002
Version Dependency System List:
V700R001B31D001
V700R001B31D002

Slot                Upgrade Way
1                   Service Upgrade
2                   Service Upgrade

Influenced service according to following table on slot 1:
    flash:/feature1-r0202.bin
        feature1
Influenced service according to following table on slot 2:
    flash:/feature1-r0202.bin
        feature1

The output shows that an incremental upgrade is recommended, and the feature1 module will be
rebooted during the upgrade process.

# Upgrade feature1 on the subordinate member.
<Sysname> issu load file feature flash:/feature1-r0202.bin slot 2
This operation will delete the rollback point information for the previous upgrade and
maybe get unsaved configuration lost. Continue? [Y/N]:y
Copying file flash:/feature1-r0202.bin to slot2#flash:/feature1-r0202.bin.....Done.
Upgrade summary according to following table:

flash:/feature1-r0202.bin
Running Version      New Version
Alpha 0201           Alpha 0202

Slot                Upgrade Way
2                   Service Upgrade

```

```

Upgrading software images to compatible versions. Continue? [Y/N]: y
# Perform a master/subordinate switchover.
<Sysname> issu run switchover
Upgrade summary according to following table:

flash:/feature1-r0202.bin
  Running Version      New Version
  Alpha 0201          Alpha 0202

  Slot                Switchover Way
  1                    Active standby process switchover
Upgrading software images to compatible versions. Continue? [Y/N]: y
# Display active software images.
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0201.bin
Active packages on slot 2:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0202.bin

# Roll back feature1 to R0201.
<Sysname> issu rollback
This command will quit the ISSU process and roll back to the previous version. Continue?
[Y/N]:Y

# Verify that both members are running the old image.
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0201.bin
Active packages on slot 2:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0201.bin

```

ISSU examples for using install commands

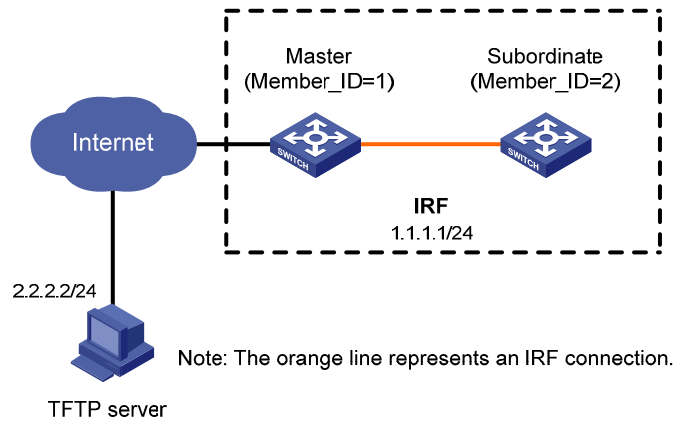
Software image upgrade example

Upgrade requirements

As shown in [Figure 39](#), the IRF fabric has two members.

Upgrade feature1 from R0201 to R0202. The two versions are compatible.

Figure 39 Network diagram



Upgrade procedure

Save the running configuration.

```
<Sysname> save
```

Download the .ipe file that contains the R0202 feature1 image from the TFTP server.

```
<Sysname> tftp 2.2.2.2 get feature1-r0202.ipe
```

% Total	% Received	% Xferd	Average Speed	Time	Time	Time	Current
			Dload Upload	Total	Spent	Left	Speed
100	256k	100	256k	0	0	764k	0
--:--:--	--:--:--	--:--:--	--:--:--	--:--:--	--:--:--	--:--:--	810k

Decompress the .ipe file.

```
<Sysname> install add flash:/feature1-r0202.ipe flash:
```

Display active software images.

```
<Sysname> display install active
```

Active packages on slot 1:

```
flash:/boot-r0201.bin
flash:/system-r0201.bin
flash:/feature1-r0201.bin
```

Active packages on slot 2:

```
flash:/boot-r0201.bin
flash:/system-r0201.bin
flash:/feature1-r0201.bin
```

Identify the ISSU methods for the upgrade and view the possible impact of the upgrade.

```
<Sysname> install activate feature flash:/feature1-r0202.bin slot 2 test
```

Copying file flash:/feature1-r0202.bin to slot2#flash:/feature1-r0202.bin.....Done.

Upgrade summary according to following table:

```
flash:/feature1-r0202.bin
```

Running Version	New Version
Alpha 0201	Alpha 0202

Slot	Upgrade Way
2	Service Upgrade

Influenced service according to following table on slot 2:

```
flash:/feature1-r0202.bin
feature1
<Sysname> install activate feature flash:/feature1-r0202.bin slot 1 test
Upgrade summary according to following table:
```

```
flash:/feature1-r0202.bin
Running Version      New Version
Alpha 0201          Alpha 0202

Slot                Upgrade Way
1                   Service Upgrade
```

```
Influenced service according to following table on slot 1:
flash:/feature1-r0202.bin
feature1
```

The output shows that both members require a service upgrade and the feature1 module will be rebooted during the upgrade process.

Activate the new feature1 image to upgrade feature1.

```
<Sysname> install activate feature flash:/feature1-r0202.bin slot 2
flash:/feature1-r0202.bin already exists on slot 2.
Overwrite it?[Y/N]:y
Copying file flash:/feature1-r0202.bin to slot2#flash:/feature1-r0202.bin.....Done.
Upgrade summary according to following table:
```

```
flash:/feature1-r0202.bin
Running Version      New Version
Alpha 0201          Alpha 0202

Slot                Upgrade Way
2                   Service Upgrade
```

```
Upgrading software images to compatible versions. Continue? [Y/N]: y
<Sysname> install activate feature flash:/feature1-r0202.bin slot 1
Upgrade summary according to following table:
```

```
flash:/feature1-r0202.bin
Running Version      New Version
Alpha 0201          Alpha 0202

Slot                Upgrade Way
1                   Service Upgrade
```

```
Upgrading software images to compatible versions. Continue? [Y/N]: y
```

Display active software images.

```
<Sysname> display install active
```

```
Active packages on slot 1:
```

```
flash:/boot-r0201.bin
flash:/system-r0201.bin
flash:/feature1-r0202.bin
```

```
Active packages on slot 2:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0202.bin
# Confirm the software change.
<Sysname> install commit
```

Software image rollback example

Rollback requirement

As shown in [Figure 39](#), the IRF fabric has two members. The feature1 feature has been upgraded from R0201 to R0202, but the software change has not been confirmed.

Roll back feature1 from R0202 to R0201.

Rollback procedure

```
# Display active software images.
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0202.bin
Active packages on slot2:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0202.bin
# Display available rollback points.
<Sysname> display install rollback
  Install rollback information 1 on slot 1:
    Updating from flash:/feature1-r0201.bin
      to flash:/feature1-r0202.bin.
  Install rollback information 2 on slot 2:
    Updating from flash:/feature1-r0201.bin
      to flash:/feature1-r0202.bin.
# Roll back feature1 to R0201.
<Sysname> install rollback to original
# Display active software images.
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0201.bin
Active packages on slot 2:
  flash:/boot-r0201.bin
  flash:/system-r0201.bin
  flash:/feature1-r0201.bin
# Confirm the software change.
```

```
<Sysname> install commit
```

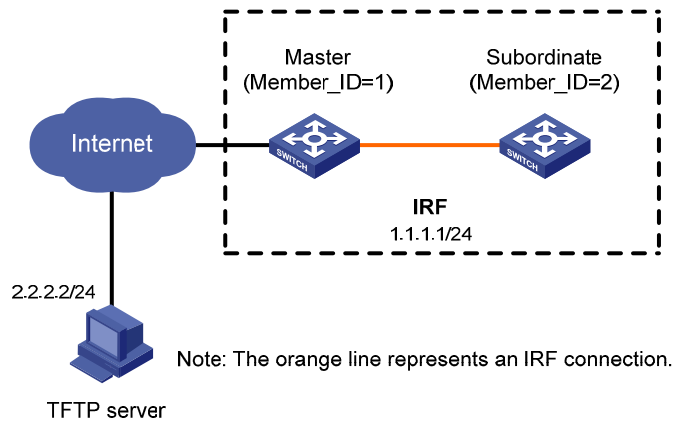
Software image patching example

Patching requirements

As shown in Figure 40, the IRF fabric has two members.

Patch the software images running on the members.

Figure 40 Network diagram



Patching procedure

Download the patch images **boot-patch.bin** and **system-patch.bin** from the TFTP server to the root directory of the flash memory on the master.

```
<Sysname> tftp 2.2.2.2 get boot-patch.bin
```

```
File will be transferred in binary mode
Downloading file from remote TFTP server, please wait...|
TFTP:      100752 bytes received in 11 second(s)
File downloaded successfully.
```

```
<Sysname> tftp 2.2.2.2 get system-patch.bin
```

```
File will be transferred in binary mode
Downloading file from remote TFTP server, please wait...|
TFTP:      100112 bytes received in 9 second(s)
File downloaded successfully.
```

Display active software images.

```
<Sysname> display install active
```

Active packages on slot 1:

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

Active packages on slot 2:

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

The output shows that the patch images are not active.

```

# Activate the patch images on the member devices.
<Sysname> install activate patch flash:/boot-patch.bin slot 1
<Sysname> install activate patch flash:/system-patch.bin slot 1
<Sysname> install activate patch flash:/boot-patch.bin slot 2
<Sysname> install activate patch flash:/system-patch.bin slot 2

# Display active software images.
<Sysname> display install active
Active packages on slot 1:
    flash:/boot.bin
    flash:/system.bin
    flash:/boot-patch.bin
    flash:/system-patch.bin
Active packages on slot 2:
    flash:/boot.bin
    flash:/system.bin
    flash:/boot-patch.bin
    flash:/system-patch.bin

# Confirm the software change.
<Sysname> install commit

# Display the main startup software images.
<Sysname> display install committed
Committed packages on slot 1:
    flash:/boot.bin
    flash:/system.bin
    flash:/boot-patch.bin
    flash:/system-patch.bin
Committed packages on slot 2:
    flash:/boot.bin
    flash:/system.bin
    flash:/boot-patch.bin
    flash:/system-patch.bin

```

The output shows that the patch images have been specified as the startup software images.

Using the emergency shell

At startup, the device tries to locate and load the Comware startup software images. These images can include a boot image, a system image, feature images, and patch images. If the following requirements are met, the device enters emergency shell mode:

- The boot image exists and can be used.
- The system image, a feature image, or a patch image is missing or corrupt.

After the device enters emergency shell mode, you can log in through the console port to obtain and load a system image to start the Comware system. After the Comware system is started, you can load feature images and patch images. This chapter describes how to obtain and load the system image in emergency shell mode. For information about loading feature and patch images, see "[Upgrading software](#)" and "[Performing an ISSU](#)."

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 in the parent folder.
Display the current path.	pwd	N/A
Copy a file.	copy <i>fileurl-source</i> <i>fileurl-dest</i>	N/A

Task	Command	Remarks
Move a file.	move <i>fileurl-source</i> <i>fileurl-dest</i>	The destination folder must have enough space for the file.
Display the contents of a file.	more <i>file-url</i>	N/A
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>storage-medium</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 this section.

The version of the system image must match that of the boot image. Before obtaining a system image, you must perform the following tasks:

- Check the version of the boot image by using the **display version** command.
- Check 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 perform the following tasks:

- Configure an IP address for the management Ethernet interface.
- Bring up the management Ethernet interface.
- If the servers reside on a different network, 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 interface.	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 interface.	ip gateway <i>ip-address</i>	By default, the management Ethernet interface has no IPv4 gateway configured.
5. Bring up the interface.	undo shutdown	By default, the management Ethernet interface is up.
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
3. Assign an IPv6 address to the interface.	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 interface.	ipv6 gateway <i>ipv6-address</i>	By default, the management Ethernet interface has no IPv6 gateway configured.
5. Bring up the interface.	undo shutdown	By default, the management Ethernet interface is up.
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 [-c <i>count</i> -s <i>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 [-c <i>count</i> -s <i>size</i>] * <i>ipv6-address</i>

Accessing the server

In emergency shell mode, the device can perform the following tasks:

- 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.

Before you use the device to access an FTP or TFTP server, you can log in to the server through Telnet or SSH to, for example, enable the FTP or TFTP server function and configure relevant parameters as required.

To access an FTP or TFTP server from the device, make sure the FTP or TFTP server is configured correctly. To configure the device as the FTP or TFTP server:

1. Log in to the server through Telnet or SSH.
2. Enable the FTP or TFTP server function.
3. Configure relevant parameters as required.

If you cannot log in to an SSH server from the device because the server has changed its public key, perform the following tasks:

4. Use the **reset ssh public-key** command to delete all locally saved server public keys.
5. Log in to the SSH server from the device again.

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

Task	Command
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>
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> }

To access a remote IPv6 server, execute the following commands as appropriate in user view:

Task	Command
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>
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> }

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. The device can reboot correctly with the modified image set.

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>
Display management Ethernet interface information.	display interface <i>m-eth0</i>
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

As shown in [Figure 41](#), the device has only the boot image (boot.bin). After startup, the device entered emergency shell mode. 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 41 Network diagram



Usage procedure

Display the version information.

```
<boot>display version
```

```
HP Comware Software, Version 7.1.045, ESS 2415
```

```
Copyright (c) 2010-2014 Hewlett-Packard Development Company, L.P.
```

```
HP FF 5700-32XGT-8XG-2QSFP+ Switch uptime is 0 weeks, 0 days, 0 hours, 20 minutes
```

```
Last reboot reason : USER reboot
```

```
Boot image: flash:/5700-cmw710-boot-e2415.bin
```

```
Boot image version: 7.1.045, ESS 2415
```

```
Compiled Sep 16 2014 13:44:42
```

Display the files and available space on the storage medium of the device.

```
<boot>dir
```

```
Directory of flash:
```

0	-rw-	104833	Jan 01 2011 05:46:24	startup.mdb
1	drw-	-	Jan 03 2011 03:33:27	versionInfo
2	-rw-	5341	Jan 01 2011 05:46:24	startup.cfg
3	-rw-	11109376	Jan 03 2011 03:26:14	5700-cmw710-boot-e2415.bin
4	-rw-	3707	Jan 01 2011 01:26:51	startup.cfg_bak
5	drw-	-	Jan 01 2011 00:00:24	seclog
6	drw-	-	Jan 01 2011 00:00:24	diagfile
7	drw-	-	Jan 01 2011 00:12:20	logfile
8	-rw-	203	Jan 01 2011 05:28:14	lauth.dat
9	-rw-	1646	Jan 01 2011 05:46:24	ifindex.dat

```
524288 KB total (147072 KB free)
```

The output shows that the boot image is present but the matching system image is not. The available space is 147072 KB, enough for saving the system image .

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
```

```
56 bytes from 1.2.1.1: seq=0 ttl=128 time=2.243 ms
```

```
56 bytes from 1.2.1.1: seq=1 ttl=128 time=0.717 ms
```

```
56 bytes from 1.2.1.1: seq=2 ttl=128 time=0.891 ms
```

```
56 bytes from 1.2.1.1: seq=3 ttl=128 time=0.745 ms
```

```
56 bytes from 1.2.1.1: seq=4 ttl=128 time=0.911 ms
```

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

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

```
round-trip min/avg/max = 0.717/1.101/2.243 ms
```

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

```
<boot> tftp 1.2.1.1 get system.bin flash:/5700-cmw710-system-e2415.bin
# Identify the compatibility between the system image and the boot image.
<boot> display install package flash:/5700-cmw710-system-e2415.bin
flash:/5700-cmw710-system-e2415.bin
[Package]
Vendor: HP
Product: 5700
Service name: system
Platform version: 7.1.045
Product version: ESS 2415
Supported board: mpu
[Component]
Component: system
Description: system package

# Load the system image to start the Comware system.
<boot> install load flash:/5700-cmw710-system-e2415.bin
Check package flash:/5700-cmw710-system-e2415.bin ...
Extracting package ...

Loading...
Line aux0 is available.

Press ENTER to get started.

After you press Enter, the following information appears:
<System>
<System>%Sep 23 18:29:59:777 2014 S58.59 SHELL/5/SHELL_LOGIN: TTY logged in from
aux0.
```

Managing the device

This chapter describes how to configure basic device parameters and manage the device.

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

Device management task list

Tasks at a glance
(Required.) Configuring the device name
(Required.) Configuring the system time
(Optional.) Enabling displaying the copyright statement
(Optional.) Configuring banners
(Required.) Setting the system operating mode
(Optional.) Rebooting the device
(Optional.) Scheduling a task
(Optional.) Disabling password recovery capability
(Optional.) Specifying the preferred airflow direction
(Optional.) Setting the port status detection timer
(Optional.) Configuring CPU usage monitoring
(Required.) Setting memory thresholds
(Required.) Configuring the temperature alarm thresholds
(Optional.) Disabling all USB interfaces
(Required.) Verifying and diagnosing transceiver modules
(Optional.) Restoring the factory-default settings and states

Configuring the device name

A device name (also called 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 sysname	The default device name is HP .

Configuring the system time

Specifying the system time source

The device can use one of the following system time sources:

- **None**—Local system time, which is manually configured at the CLI.
- **PTP**—PTP time source. When the device uses the PTP time source, you cannot change the system time manually. For more information about PTP, see *Network Management and Monitoring Configuration Guide*.
- **NTP**—NTP time source. When the device uses the NTP time source, you cannot change the system time manually. For more information about NTP, see *Network Management and Monitoring Configuration Guide*.

If you configure the **clock protocol none** command together with the **clock protocol ntp** or **clock protocol ptp** command, the device uses the NTP or PTP time source.

Power cycling an HP 5700 restores the default system time settings. Reconfigure the settings after the switch starts up.

To specify the system time source:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify the system time source.	clock protocol { none ntp ptp }	By default, the device uses the NTP time source. If you configure this command multiple times, the most recent configuration takes effect.

Setting the system time

When the system time source is the local 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. Set the system time correctly or use NTP to synchronize the device with a trusted time source before you run it on the network.

To set the system time:

Step	Command	Remarks
1. Set the UTC time.	clock datetime <i>time date</i>	By default, the UTC time is the factory-default time.
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.
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

When displaying the copyright statement is enabled, the device displays the copyright statement in the following situations:

- When a Telnet or SSH user logs in.
- After a console or modem dial-in user quits user view. This is because the device automatically tries to restart the console session.

The following is a sample copyright statement:

```
*****
* Copyright (c) 2010-2014 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. 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 is configured.
- **Incoming banner**—Appears for Modem users.
- **Shell banner**—Appears before a non-modem dial-in user accesses user view.

Banner input modes

You can configure a single-line banner or a multiline banner.

- **Single-line banner.**
A single-line banner must be input in the same line as the command. The start and end delimiters for the banner can be any printable character. However, they must be the same and must not be

included in the banner. The input text, including the command keywords and the delimiters, cannot exceed 510 characters. 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.%
```

- Multiline banner.

A multiline banner can be up to 2000 characters. To input a multiline banner, use one of the following methods:

- **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	Remarks
1. Enter system view.	system-view	N/A
2. Configure the legal banner.	header legal <i>text</i>	By default, the device does not have a banner.
3. Configure the MOTD banner.	header motd <i>text</i>	By default, the device does not have a banner.

Step	Command	Remarks
4. Configure the login banner.	header login <i>text</i>	By default, the device does not have a banner.
5. Configure the incoming banner.	header incoming <i>text</i>	By default, the device does not have a banner.
6. Configure the shell banner.	header shell <i>text</i>	By default, the device does not have a banner.

Setting the system operating mode

The device can operate in the following modes:

- **AdvancedBridge**—Advanced mode.
- **StandardBridge**—Standard mode.
- **ExpertBridge**—Expert mode.

In different operating modes, the device supports different features, and might have different specifications for the supported features. For example, the device supports FCoE over S-Channel only when it operates in ExpertBridge mode. For more information about FCoE over S-Channel, see *FCoE Command Reference*.

If the prompt "Not enough hardware resources available." appears after you set the system operating mode, perform the following tasks:

- Use the **display qos-acl resource** command to display ACL resource usage.
- Use the **undo acl** command to release ACL resources as required.
- Set the system operating mode again.

For more information about the **display qos-acl resource** and **undo acl** commands, see *ACL and QoS Command Reference*.

To set the system operating mode:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the system operating mode.	system-working-mode { AdvancedBridge StandardBridge ExpertBridge }	By default, the device operates in standard mode. Change to the operating mode takes effect after a reboot.

Rebooting the device

⚠ CAUTION:

- A device reboot might 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 the startup configuration file and startup software images are correctly specified. If a startup configuration file or software image problem exists, the device cannot start up correctly. For more information about the two **display** commands, see *Fundamentals Command Reference*.

The following device reboot methods are available:

- 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.
- Power off and then power on the device. This method might cause data loss, and is the least-preferred method.

Using the CLI, you can reboot the device from a remote host.

Configuration guidelines

When you schedule a reboot, follow these guidelines:

- The automatic reboot configuration takes effect on all member devices. It will be canceled if a master/subordinate switchover occurs.
- For data security purposes, the device does not reboot while it is performing file operations.

Rebooting devices immediately at the CLI

Execute the following command in user view:

Task	Command	Remarks
Reboot an IRF member device or all IRF member devices.	reboot [slot slot-number] [force]	Use this command in user view

Scheduling a device reboot

The device supports only one device reboot schedule. If you configure the **scheduler reboot at** or **scheduler reboot delay** command multiple times or configure both commands, the most recent configuration takes effect.

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 is automatically executed periodically.

Configuration guidelines

Follow these guidelines when you schedule a task:

- 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 either 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</i> <i>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 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.	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. Assign user roles to the schedule.	user-role <i>role-name</i>	By default, a schedule has the user role of the schedule creator. A command in a schedule can be executed if it is permitted by one or more user roles of the schedule.
8. Specify an execution time table for the one-time schedule.	- 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> &lt;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 system view.	quit	N/A
5. Create a schedule.	scheduler schedule <i>schedule-name</i>	By default, no schedule exists.
6. Assign user roles to the schedule.	user-role <i>role-name</i>	By default, a schedule has the user role of the schedule creator. A command in a schedule can be executed if it is permitted by one or more user roles of the schedule.
7. 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.

Step	Command	Remarks
8. Specify an execution time table for the periodic schedule.	- 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 [date]] 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

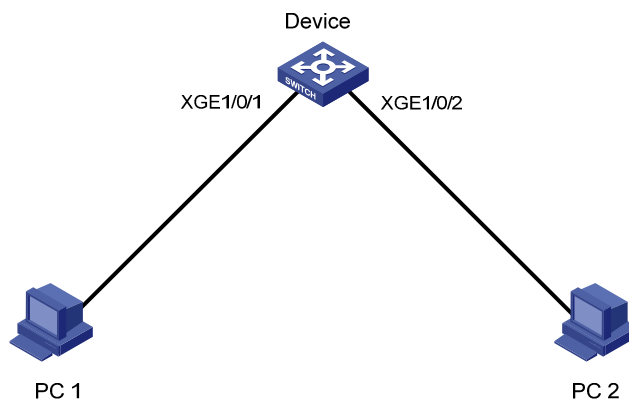
Network requirements

As shown in Figure 42, two interfaces of the device are connected to users.

To save energy, configure the device to perform the following operations:

- Enable interfaces Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 at 8:00 a.m. every Monday through Friday.
- Disable the interfaces at 18:00 every Monday through Friday.

Figure 42 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-gigabitethernet 1/0/1
```

```
[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-gigabitethernet
1/0/1
[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-gigabitethernet
1/0/2
[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-gigabitethernet
1/0/2
[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-gigabitethernet 1/0/1
shutdown

Job name: shutdown-Ten-GigabitEthernet1/0/2
system-view
interface ten-gigabitethernet 1/0/2
shutdown

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

```

```
interface ten-gigabitethernet 1/0/1
undo shutdown
```

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

```
system-view
interface ten-gigabitethernet 1/0/2
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

Logfile Size: 16054 Bytes.

```
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-gigabitethernet 1/0/1

[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-gigabitethernet 1/0/2.
[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-gigabitethernet 1/0/1
[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-gigabitethernet 1/0/2
[Sysname-Ten-GigabitEthernet1/0/2]shutdown

```

Disabling password recovery capability

Password recovery capability controls console user access to the device configuration and SDRAM from Boot ROM menus.

If password recovery capability is enabled, a console user can access the device configuration without authentication to configure new passwords.

If password recovery capability is disabled, console users must restore the factory-default configuration before they can configure new passwords. Restoring the factory-default configuration deletes the next-startup configuration files.

To prevent illegal users to access the startup configuration files, disable password recovery capability.

Availability of Boot ROM menu options varies by password recovery capability setting. For more information, see the release notes.

To disable password recovery capability:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Disable password recovery capability.	undo password-recovery enable	By default, password recovery capability is enabled.

Specifying the preferred airflow direction

The device supports the following airflow directions:

- From the port side to the power side.
- From the power side to the port side.

Select the correct fan tray model and set the preferred airflow direction to the airflow direction of the ventilation system in the equipment room. If a fan tray is not operating correctly or has a different airflow direction than the configured one, the system sends logs.

To specify the preferred airflow direction:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Specify 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 side to the port side.

Setting the port status detection timer

The device starts a port status detection timer when a port is shut down by a protocol. Once the detection timer expires, the device brings up the port so the port status reflects the port's 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.

Configuring CPU usage monitoring

You can enable CPU usage monitoring so the system periodically samples and saves CPU usage. To examine recent CPU usage, use the **display cpu-usage history** command.

You can also set CPU usage thresholds. When a CPU usage threshold is reached, the device sends a trap.

To configure CPU usage monitoring:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable CPU usage monitoring.	monitor cpu-usage enable [<i>slot slot-number</i> [cpu <i>cpu-number</i>]]	By default, CPU usage monitoring is enabled.

Step	Command	Remarks
3. Set the CPU usage sampling interval.	monitor cpu-usage interval <i>interval-value [slot slot-number</i> <i>[cpu cpu-number]]</i>	By default, the CPU usage sampling interval is 1 minute.
4. Set CPU usage thresholds.	monitor cpu-usage threshold <i>cpu-threshold [slot slot-number</i> <i>[cpu cpu-number]]</i>	By default, the CPU usage threshold is 99%.

Setting memory thresholds

To ensure correct operation and improve memory utilization, the system monitors the memory usage and the amount of free memory space in real time.

- If the memory usage threshold is exceeded, the system generates and sends a trap.
- If a free-memory threshold is exceeded, the system generates an alarm notification or an alarm-removed notification and sends it to affected service modules or processes.

The device supports the following free-memory thresholds:

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

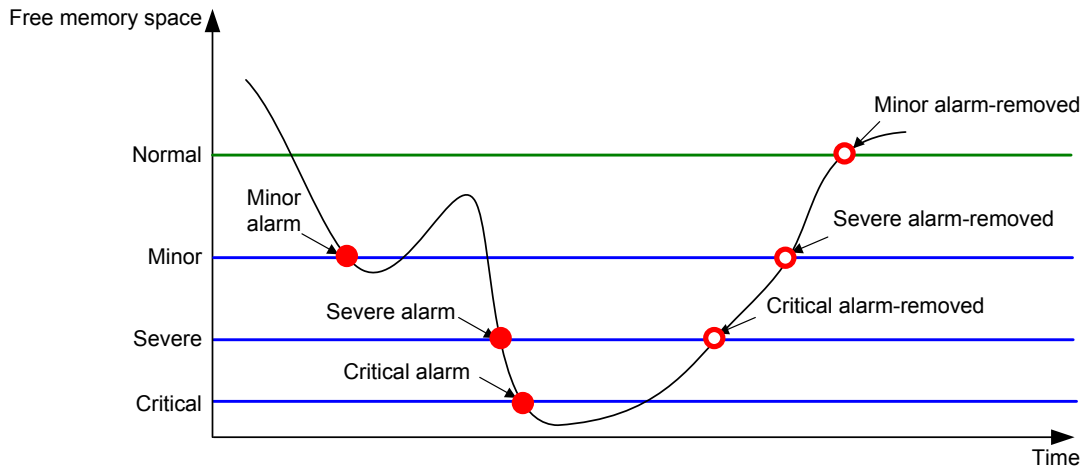
Table 14 and Figure 43 show how the device generates notifications based on the free-memory thresholds.

Table 14 Memory alarm notifications and memory alarm-removed notifications

Notification	Triggering condition	Remarks
Minor alarm notification	The amount of free memory space decreases 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 removed.
Severe alarm notification	The amount of free memory space decreases 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 removed.
Critical alarm notification	The amount of free memory space decreases 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 removed.
Critical alarm-removed notification	The amount of free memory space increases to or above the severe alarm threshold.	N/A

Notification	Triggering condition	Remarks
Severe alarm-removed notification	The amount of free memory space increases to or above the minor alarm threshold.	N/A
Minor alarm-removed notification	The amount of free memory space increases to or above the normal state threshold.	N/A

Figure 43 Memory alarm notification and alarm-removed notification



To set memory thresholds:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set free-memory thresholds.	memory-threshold [slot slot-number [cpu cpu-number]] minor minor-value severe severe-value critical critical-value normal normal-value	The defaults are as follows: • Minor alarm threshold—96 MB. • Severe alarm threshold—64 MB. • Critical alarm threshold—48 MB. • Normal state threshold—128 MB.
3. Set the memory usage threshold.	memory-threshold usage [slot slot-number [cpu cpu-number]] memory-threshold	By default, the memory usage threshold is 100%.

Configuring the temperature alarm thresholds

The device monitors its temperature through temperature sensors, based on the following thresholds:

- Low-temperature threshold.
- High-temperature warning threshold.
- High-temperature alarming threshold.

When the temperature drops below the low-temperature threshold or reaches the high-temperature warning threshold, the device performs the following tasks:

- Logs the event.
- Sends a log message.
- Sends a trap.

When the temperature reaches the high-temperature alarming threshold, the device performs the following tasks:

- Logs the event.
- Sends log messages repeatedly.
- Sets the LEDs on the device panel.

To configure the temperature alarm thresholds:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the temperature alarm thresholds.	temperature-limit slot slot-number hotspot sensor-number lowlimit warninglimit [alarmlimit]	To view the default settings, use the undo temperature-limit command to restore the defaults and then execute the display environment command. The high-temperature alarming threshold must be higher than the high-temperature warning threshold. The high-temperature warning threshold must be higher than the low-temperature threshold.

Disabling all 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. Before executing this command, use the umount command to unmount all USB partitions. For more information about this command, see <i>Fundamentals Command Reference</i> .

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 debugging or testing.

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

Task	Command	Remarks
Display the key parameters of transceiver modules.	display transceiver { interface [<i>interface-type interface-number</i>] }	N/A
Display the electrical label information of transceiver modules.	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 perform the following tasks:

- Check the alarms that exist on the transceiver module to identify the fault source.
- 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 commands in any view:

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

Restoring the factory-default settings and states

CAUTION:

This feature is disruptive. Use this feature only when you cannot troubleshoot the device by using other methods, or you want to use the device in a different scenario.

This feature performs the following tasks:

- Deletes all configuration files (.cfg files) in the root directories of the storage media.
- Deletes all log files (.log files in the folder /logfile).
- Clears all log information (in the log buffer), trap information, and debugging information.
- Restores the parameters for the Boot ROM options to the factory-default settings.
- Deletes all files on an installed hot-swappable storage medium, such as a USB disk.

Before this operation, remove all hot-swappable storage media from the device.

After this operation, only the items required for device operation are retained, including the .bin files, the MAC addresses, and the electronic label information.

To restore the factory-default settings and states, use the following command in user view:

Task	Command	Remarks
Restore the factory-default settings and states.	restore factory-default	This command takes effect after a device reboot.

Displaying and maintaining device management configuration

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

Task	Command
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 [slot slot-number [cpu cpu-number]]
Display CPU usage monitoring settings.	display cpu-usage configuration [slot slot-number [cpu cpu-number]]
Display historical CPU usage statistics in a chart.	display cpu-usage history [job job-id] [slot slot-number [cpu cpu-number]]
Display hardware information.	display device [flash usb] [slot slot-number [subslot subslot-number] verbose]
Display the electronic label information of the device.	display device manuinfo [slot slot-number]
Display the electronic label information of a fan.	display device manuinfo slot slot-number fan fan-id
Display the electronic label information of a power supply.	display device manuinfo slot slot-number power power-id
Display the operating statistics for multiple feature modules.	display diagnostic-information [hardware infrastructure l2 l3 service] [file-name]
Display device temperature statistics.	display environment [slot slot-number]
Display the operating states of fans.	display fan [slot slot-number [fan-id]]

Task	Command
Display memory usage statistics.	display memory [<i>slot slot-number</i> [cpu <i>cpu-number</i>]]
Display memory usage thresholds.	display memory-threshold [<i>slot slot-number</i> [cpu <i>cpu-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 system working mode information.	display system-working-mode
Display system version information.	display version
Display the startup software image upgrade history records of the master.	display version-update-record
Clear job execution log information.	reset scheduler logfile

Using Tcl

Comware V7 provides a built-in tool command language (Tcl) interpreter. From user view, you can use the **tclsh** command to enter Tcl configuration view to execute the following commands:

- Tcl 8.5 commands.
- Comware commands.

The Tcl configuration view is equivalent to the user view. You can use Comware commands in Tcl configuration view in the same way they are used in user view. For example, you can perform the following tasks:

- Use the **system-view** command to enter system view to configure features.
- Use the **quit** command to return to the upper-level view.

Tcl usage guidelines and restrictions

When you use Tcl, follow these guidelines and restrictions:

- You can apply Tcl environment variables to Comware commands.
- You can enter multiple Comware commands separated by semi-colons to execute the commands in the order they are entered.
- No online help information is provided for Tcl commands.
- You cannot press **Tab** to complete an abbreviated Tcl command.
- Successfully executed Tcl commands are not saved to command history buffers.
- In Tcl configuration view, if a Comware command conflicts with a Tcl command, the Tcl command will be executed. To execute the Comware command when a conflict occurs, execute the **cli** command.

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	Remarks
Return from Tcl configuration view to user view.	tclquit	You can achieve the same result by executing the quit command.

Executing Comware commands in Tcl configuration view

- The **cli** command is a Tcl command, so you cannot enter **?** to obtain online help or press **Tab** to complete an abbreviated command.
- You can use the **cli** command to execute all Comware commands in Tcl configuration view.
- To execute multiple Comware commands in one operation:
 - Specify multiple Comware commands for the **cli** command, quote them, and separate them by a space and a semicolon. For example, **cli "rip 1 ; network 10.1.1.1"**.
 - Specify one Comware command for each **cli** command and separate them by a space and a semicolon. For example, **cli rip 1 ; network 10.1.1.1**.

To execute Comware commands in Tcl configuration view:

Step	Command	Remarks
1. Enter Tcl configuration view	tdsh	N/A
2. Execute Comware commands.	cli <i>command</i>	This command cannot be used to execute Tcl commands.

Using Python

Comware V7 provides a built-in Python interpreter that supports the following items:

- Python 2.7 commands.
- Python 2.7 standard API.
- Comware V7 extended API. For more information about the Comware V7 extended API, see "[Comware V7 extended Python API](#)."
- Python scripts. You can use a Python script to configure the system.

Entering the Python shell

To use Python commands and APIs, you must enter the Python shell.

Task	Command
Enter the Python shell from user view.	python

Executing a Python script

Execute a Python script in user view.

Task	Command
Execute a Python script.	python <i>filename</i>

Python usage example

Network requirements

Use a Python script to perform the following tasks:

- Download configuration files **main.cfg** and **backup.cfg** to the device.
- Configure the files as the main and backup configuration files for the next startup.

Figure 44 Network diagram



Configuration procedure

```
# Use a text editor on the PC to edit Python script test.py as follows:  
#!/usr/bin/python  
import comware
```

```
comware.Transfer('tftp', '192.168.1.26', 'main.cfg', 'flash:/main.cfg')
comware.Transfer('tftp', '192.168.1.26', 'backup.cfg', 'flash:/backup.cfg')
comware.CLI('startup saved-configuration flash:/main.cfg main ;startup
saved-configuration flash:/backup.cfg backup')

# Use TFTP to download the script to the device.
<Sysname> tftp 192.168.1.26 get test.py

# Execute the script.
<Sysname> python flash:/test.py
<Sysname>startup saved-configuration flash:/main.cfg main
Please wait..... Done.
<Sysname>startup saved-configuration flash:/backup.cfg backup
Please wait..... Done.
```

Verifying the configuration

```
# Display startup configuration files.
<Sysname> display startup
Current startup saved-configuration file: flash:/startup.cfg
Next main startup saved-configuration file: flash:/main.cfg
Next backup startup saved-configuration file: flash:/backup.cfg
```

Comware V7 extended Python API

The Comware V7 extended Python API is compatible with the Python syntax.

Importing and using the Comware V7 extended Python API

To use the Comware V7 extended Python API, you must import the API to Python.

Use either of the following methods to import and use the Comware V7 extended Python API:

- Use **import comware** to import the entire API and use **comware.API** to execute an API.
For example, to use the extended API **Transfer** to download file **test.cfg** from TFTP server 192.168.1.26:

```
<Sysname> python
Python 2.7.3 (default, May 24 2014, 14:37:26)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.Transfer('tftp', '192.168.1.26', 'test.cfg', 'flash:/test.cfg', user='', password='')
<comware.Transfer object at 0xb7eab0e0>
```
- Use **from comware import API** to import an API and use **API** to execute the API.
For example, to use the extended API **Transfer** to download file **test.cfg** from TFTP server 192.168.1.26:

```
<Sysname> python
Python 2.7.3 (default, May 24 2014, 14:37:26)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> from comware import Transfer
>>> Transfer('tftp', '192.168.1.26', 'test.cfg', 'flash:/test.cfg', user='', password='')
<comware.Transfer object at 0xb7e5e0e0>
```

Comware V7 extended Python API functions

CLI class

CLI

Use **CLI** to execute Comware V7 CLI commands and create CLI objects.

Syntax

CLI(command='', do_print=True)

Parameters

command: Specifies the commands to be executed. To enter multiple commands, use a space and a semicolon (;) as the delimiter. To enter a command in a view other than user view, you must first enter the commands used to enter the view. For example, you must enter '**system-view ;local-user test class manage**' to execute the **local-user test class manage** command.

do_print: Specifies whether to output the execution result:

- **True**—Outputs the execution result. This value is the default.
- **False**—Does not output the execution result.

Returns

CLI objects

Examples

```
# Add a local user with the username test.
<Sysname> python
Python 2.7.3 (default, May 24 2014, 14:37:26)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.CLI('system-view ;local-user test class manage')
```

Sample output

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] local-user test class manage
New local user added.
<comware.CLI object at 0xb7f680a0>
```

get_output

Use **get_output** to get the output from executed commands.

Syntax

CLI.get_output()

Returns

Output from executed commands

Examples

```
# Add a local user and get the output from the command.
<Sysname> python
Python 2.7.3 (default, May 24 2014, 14:37:26)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> c = comware.CLI('system-view ;local-user test class manage', False)
>>> c.get_output()
```

Sample output

```
['<Sysname>system-view', 'System View: return to User View with Ctrl+Z.',
 '[Sysname]local-user test class manage']
```

Transfer class

Transfer

Use **Transfer** to download a file from a server.

Syntax

Transfer(protocol="", host="", source="", dest="", login_timeout=10, user="", password="")

Parameters

protocol: Specifies the protocol used to download a file:

- **ftp**—Uses FTP.
- **tftp**—Uses TFTP.
- **http**—Uses HTTP.

host: Specifies the IP address of the remote server.

source: Specifies the name of the file to be downloaded from the remote server.

dest: Specifies a name for the downloaded file.

login_timeout: Specifies the timeout for the operation, in seconds. The default is 10.

user: Specifies the username for logging in to the server.

password: Specifies the login password.

Returns

Transfer object

Examples

```
# Download file test.cfg from TFTP server 192.168.1.26.
```

```
<Sysname> python
```

```
Python 2.7.3 (default, May 24 2014, 14:37:26)
```

```
[GCC 4.4.1] on linux2
```

```
Type "help", "copyright", "credits" or "license" for more information.
```

```
>>> import comware
```

```
>>> comware.Transfer('tftp', '192.168.1.26', 'test.cfg', 'flash:/test.cfg', user='',  
password='')
```

Sample output

```
<comware.Transfer object at 0xb7f700e0>
```

get_error

Use **get_error** to get the error information from the download operation.

Syntax

Transfer.get_error()

Returns

If there is no error information, **None** is returned.

Examples

```
# Download file test.cfg from TFTP server 1.1.1.1 and get the error information from the operation.
```

```
<Sysname> python
```

```

Python 2.7.3 (default, May 24 2014, 14:37:26)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> c = comware.Transfer('tftp', '1.1.1.1', 'test.cfg', 'flash:/test.cfg', user='',
password='')
>>> c.get_error()

```

Sample output

```
'Timeout was reached'
```

API get_self_slot

get_self_slot

Use **get_self_slot** to get the member ID of the master device.

Syntax

```
get_self_slot()
```

Returns

A list object in the format `[-1,slot-number]`, where *slot-number* indicates the member ID of the master device.

Examples

```

# Get the member ID of the master device.
<Sysname> python
Python 2.7.3 (default, May 24 2014, 14:37:26)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.get_self_slot()

```

Sample output

```
[-1,1]
```

API get_standby_slot

get_standby_slot

Use **get_standby_slot** to get the member IDs of all subordinate devices.

Syntax

```
get_standby_slot()
```

Returns

A list object in one of the following formats:

- `[]`—The IRF fabric does not have a subordinate device.
- `[-1,slot-number]`—The IRF fabric has only one subordinate device.
- `[-1,slot-number1],[-1,slot-number2],...`—The IRF fabric has multiple subordinate devices. The *slot-number* arguments indicate the member IDs of the subordinate devices.

Examples

```
# Get the member IDs of all subordinate devices.
<Sysname> python
Python 2.7.3 (default, May 24 2014, 14:37:26)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import comware
>>> comware.get_standby_slot()
```

Sample output

```
[]
```

Using automatic configuration

Overview

With the automatic configuration feature, the device can automatically obtain a set of configuration settings when it starts up without a configuration file. This feature simplifies network configuration and maintenance.

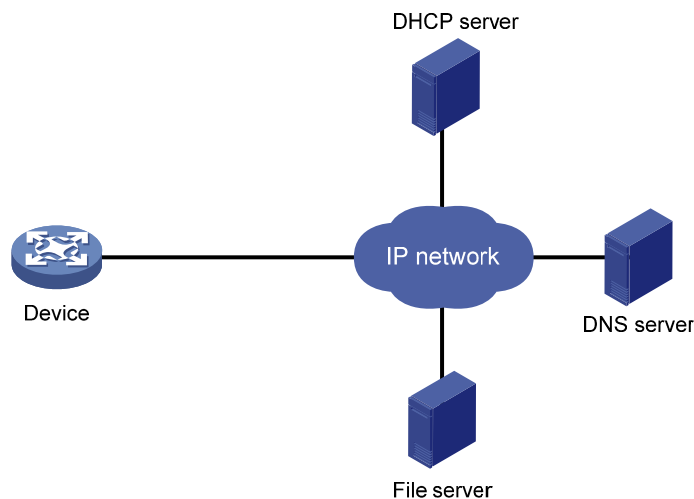
Automatic configuration applies to scenarios that have the following characteristics:

- A number of devices need to be configured.
- The devices to be configured are widely distributed.
- The configuration workload on individual devices is heavy.

As shown in [Figure 45](#), automatic configuration requires the following servers:

- DHCP server.
- File server (TFTP or HTTP server).
- (Optional.) DNS server.

Figure 45 Network diagram



Automatic configuration task list

Tasks at a glance

(Required.) [Configuring the file server](#)

(Required.) [Preparing the files for automatic configuration](#)

(Required.) [Configuring the DHCP server](#)

(Optional.) [Configuring the DNS server](#)

Tasks at a glance

(Optional.) [Configuring the gateway](#)

(Required.) [Selecting the interfaces used for automatic configuration](#)

(Required.) [Starting and completing automatic configuration](#)

Configuring the file server

For devices to obtain configuration information from a TFTP server, start TFTP service on the file server.

For devices to obtain configuration information from an HTTP server, start HTTP service on the file server.

Preparing the files for automatic configuration

The device can use a script file or configuration file for automatic configuration.

- For devices to use configuration files for automatic configuration, you must edit and save the configuration files to the file server as described in "[Configuration files](#)." If you do not configure the DHCP server to assign configuration file names, you must also create a host name file on the TFTP server.
- For devices to use script files for automatic configuration, you must edit and save the script files to the file server as described in "[Script files](#)."

Host name file

The host name file contains host name-IP address mappings and must be named **network.cfg**.

All mapping entries in the host name file must use the **ip host host-name ip-address** format. Each mapping entry must reside on a separate line. For example:

```
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
```

Configuration files

To prepare configuration files:

- For devices that require different configurations, perform the following tasks:
 - Determine the name for each device's configuration file.
The configuration file names must use the extension **.cfg**. For simple file name identification, use configuration file names that do not contain spaces.
 - Use the file names to save the configuration files for the devices to the file server.
- For devices that share all or some configurations, save the common configurations to a **.cfg** file on the file server.
- If a TFTP file server is used, you can save a default configuration file named **device.cfg** on the server. This file contains only common configurations that the devices use to start up. This file is assigned to a device only when the device does not have other configuration files to use.

During the automatic configuration process, a device first tries to obtain a configuration file dedicated for it. If no dedicated configuration file is found, the device tries to obtain the common configuration file. If

no common configuration file is found when a TFTP file server is used, the device obtains and uses the default configuration file.

Script files

Script files can be used for automatic software upgrade and automatic configuration. The device supports Python scripts (.py files) and Tcl scripts (.tcl files). For more information about Python and Tcl scripts, see "[Using Python](#)" and "[Using Tcl](#)."

To prepare script files:

- For devices that share all or some configurations, edit a script file that contains the common configurations.
- For the other devices, edit a separate script file for each of them.

Configuring the DHCP server

The DHCP server assigns the following items to devices that need to be automatically configured:

- IP addresses.
- Paths of the configuration files or scripts.

Configuration guidelines

When you configure the DHCP server, follow these guidelines:

- For devices for which you have prepared different configuration files, perform the following tasks for each of them on the DHCP server:
 - Create a DHCP address pool.
 - Configure a static address binding.
 - Specify a configuration file or script file.
- For devices for which you have prepared the same configuration file, perform the following tasks on the DHCP server:
 - Create a DHCP address pool for the devices.
 - Configure a static address binding for each of the devices in the address pool.
 - Specify the configuration file for the devices.
- If all devices on a subnet share the same configuration file or script file, perform the following tasks on the DHCP server:
 - Configure dynamic address allocation.
 - Specify the configuration file or script file for the devices.

The configuration file can contain only the common settings for the devices. You can provide a method for the device administrators to change the configurations after their devices start up.

Configuring the DHCP server when an HTTP file server is used

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable DHCP.	dhcp enable	By default, DHCP is disabled.
3. Create a DHCP address pool and enter its view.	dhcp server ip-pool <i>pool-name</i>	By default, no DHCP address pool is created.

Step	Command	Remarks
4. Configure the address pool.	(Method 1.) Specify the primary subnet for the address pool: network <i>network-address</i> [<i>mask-length</i> mask <i>mask</i>] (Method 2.) Configure a static binding: static-bind ip-address <i>ip-address</i> [<i>mask-length</i> mask <i>mask</i>] { client-identifier <i>client-identifier</i> hardware-address <i>hardware-address</i> [ethernet token-ring] }	Use either or both methods. By default, no primary subnet or static binding is configured. You can add multiple static bindings. One IP address can be bound to only one client. To change the binding for a DHCP client, you must delete the binding and reconfigure a binding.
5. Specify the URL of the configuration file or script file.	bootfile-name <i>url</i>	By default, no configuration file URL is specified.

Configuring the DHCP server when a TFTP file server is used

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable DHCP.	dhcp enable	By default, DHCP is disabled.
3. Create a DHCP address pool and enter its view.	dhcp server ip-pool <i>pool-name</i>	By default, no DHCP address pool is created.
4. Configure the address pool.	(Method 1.) Specify the primary subnet for the address pool: network <i>network-address</i> [<i>mask-length</i> mask <i>mask</i>] (Method 2.) Configure a static binding: static-bind ip-address <i>ip-address</i> [<i>mask-length</i> mask <i>mask</i>] { client-identifier <i>client-identifier</i> hardware-address <i>hardware-address</i> [ethernet token-ring] }	Use either or both methods. By default, no primary subnet or static binding is configured. You can add multiple static bindings. One IP address can be bound to only one client. To change the binding for a DHCP client, you must delete the binding and reconfigure a binding.
5. Specify a TFTP server.	(Method 1.) Specify the IP address of the TFTP server: tftp-server ip-address <i>ip-address</i> (Method 2.) Specify the name of the TFTP server: tftp-server domain-name <i>domain-name</i>	Use either or both methods. By default, no TFTP server is specified. If you specify a TFTP server by its name, a DNS server is required on the network.
6. Specify the configuration file name.	bootfile-name <i>bootfile-name</i>	By default, no configuration file name is specified.

Configuring the DNS server

A DNS server is required in the following situations:

- The TFTP server does not have a host name file. However, devices need to perform the following tasks:
 - Use their IP addresses to obtain their host names.
 - Obtain configuration files named in the format of *host name.cfg* from the TFTP server.
- The DHCP server assigns the TFTP server domain name through the DHCP reply message. Devices must use the domain name to obtain the IP address of the TFTP server.

Configuring the gateway

If the devices to be automatically configured and the servers for automatic configuration reside in different network segments, you must perform the following tasks:

- Deploy a gateway and make sure the devices can communicate with the servers.
- Configure the DHCP relay agent feature on the gateway.
- Configure the UDP helper feature on the gateway.

When a device sends a request through a broadcast packet to the file server, the UDP helper changes the broadcast packet to a unicast packet and forwards the unicast packet to the file server. For more information about UDP helper, see *Layer 3—IP Services Configuration Guide*.

Selecting the interfaces used for automatic configuration

For fast automatic device configuration, connect only the management Ethernet interface on each device to the network.

Starting and completing automatic configuration

1. Power on the devices to be automatically configured.
 If a device does not find a next-start configuration file locally, it starts the automatic configuration process to obtain a configuration file. If one attempt fails, the device waits 30 seconds and then automatically starts the process again. To stop the process, press **Ctrl+D**.
 After obtaining a configuration file, the device automatically executes the configuration file.
2. Use the **save** command to save the running configuration.
 The device does not save the obtained configuration file locally. If you do not save the running configuration, the device must use the automatic configuration feature again after a reboot.
 For more information about the **save** command, see *Fundamentals Command Reference*.

Automatic configuration examples

Automatic configuration using TFTP server

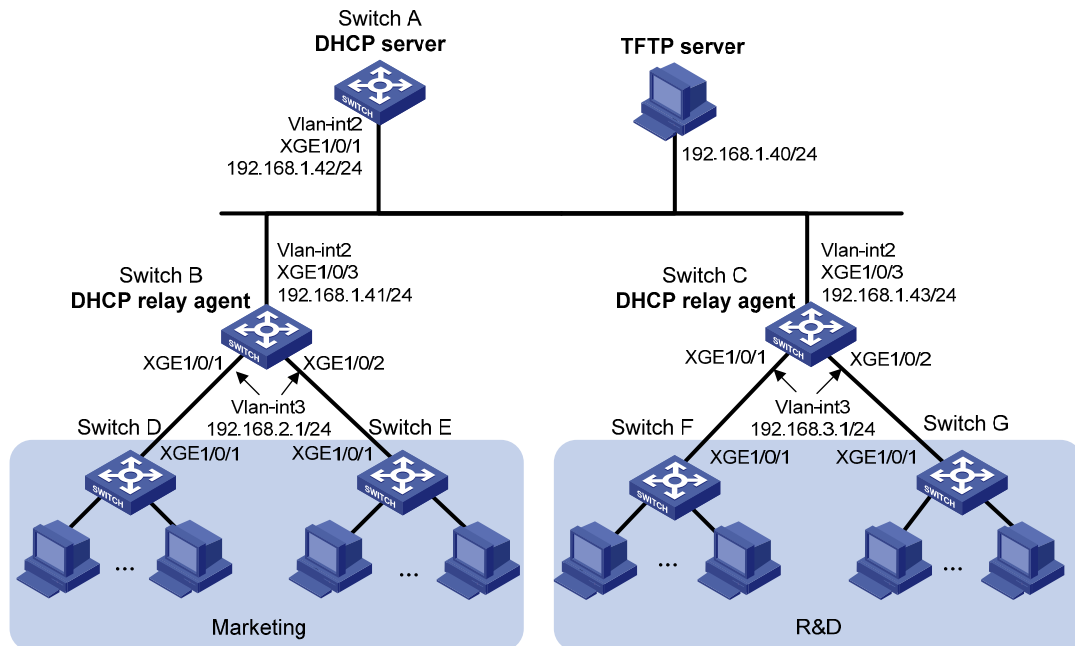
Network requirements

As shown in [Figure 46](#), two departments of a company are connected to the network through gateways (Switch B and Switch C). Access devices Switch D, Switch E, Switch F, and Switch G do not have a configuration file.

Configure the servers and gateways so the access devices can obtain a configuration file to complete the following configuration tasks:

- Enable administrators of access devices to Telnet to and manage their respective access devices.
- Require administrators to enter their respective usernames and passwords at login.

Figure 46 Network diagram



Configuration procedure

1. Configure the DHCP server:

Create a VLAN interface and assign an IP address to the interface.

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port Ten-GigabitEthernet 1/0/1
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.1.42 24
[SwitchA-Vlan-interface2] quit
```

Enable DHCP.

```
[SwitchA] dhcp enable
```

Enable the DHCP server on VLAN-interface 2.

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] dhcp select server
[SwitchA-Vlan-interface2] quit
```

Configure the address pool **market** to assign IP addresses on subnet 192.168.2.0/24 to clients in the Marketing department. Specify the TFTP server, gateway, and configuration file name for the clients.

```
[SwitchA] dhcp server ip-pool market
[SwitchA-dhcp-pool-market] network 192.168.2.0 24
[SwitchA-dhcp-pool-market] tftp-server ip-address 192.168.1.40
```

```

[SwitchA-dhcp-pool-market] gateway-list 192.168.2.1
[SwitchA-dhcp-pool-market] bootfile-name market.cfg
[SwitchA-dhcp-pool-market] quit
# Configure the address pool rd to assign IP addresses on subnet 192.168.3.0/24 to clients in
the R&D department. Specify the TFTP server, gateway, and configuration file name for the clients.
[SwitchA] dhcp server ip-pool rd
[SwitchA-dhcp-pool-rd] network 192.168.3.0 24
[SwitchA-dhcp-pool-rd] tftp-server ip-address 192.168.1.40
[SwitchA-dhcp-pool-rd] gateway-list 192.168.3.1
[SwitchA-dhcp-pool-rd] bootfile-name rd.cfg
[SwitchA-dhcp-pool-rd] quit
# Configure static routes to the DHCP relay agents.
[SwitchA] ip route-static 192.168.2.0 24 192.168.1.41
[SwitchA] ip route-static 192.168.3.0 24 192.168.1.43
[SwitchA] quit

```

2. Configure the gateway Switch B:

```

# Create VLAN interfaces and assign IP addresses to the interfaces.
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port Ten-GigabitEthernet 1/0/3
[SwitchB-vlan2] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 192.168.1.41 24
[SwitchB-Vlan-interface2] quit
[SwitchB] vlan 3
[SwitchB-vlan3] port Ten-GigabitEthernet 1/0/1
[SwitchB-vlan3] port Ten-GigabitEthernet 1/0/2
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ip address 192.168.2.1 24
[SwitchB-Vlan-interface3] quit
# Enable DHCP.
[SwitchB] dhcp enable
# Enable the DHCP relay agent on VLAN-interface 3.
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] dhcp select relay
# Specify the DHCP server address.
[SwitchB-Vlan-interface3] dhcp relay server-address 192.168.1.42

```

3. Configure the gateway Switch C:

```

# Create VLAN interfaces and assign IP addresses to the interfaces.
<SwitchC> system-view
[SwitchC] vlan 2
[SwitchC-vlan2] port Ten-GigabitEthernet 1/0/3
[SwitchC-vlan2] quit
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ip address 192.168.1.43 24

```

```

[SwitchC-Vlan-interface2] quit
[SwitchC] vlan 3
[SwitchC-vlan3] port Ten-GigabitEthernet 1/0/1
[SwitchC-vlan3] port Ten-GigabitEthernet 1/0/2
[SwitchC-vlan3] quit
[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] ip address 192.168.3.1 24
[SwitchC-Vlan-interface3] quit
# Enable DHCP.
[SwitchC] dhcp enable
# Enable the DHCP relay agent on VLAN-interface 3.
[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] dhcp select relay
# Specify the DHCP server address.
[SwitchC-Vlan-interface3] dhcp relay server-address 192.168.1.42

```

4. Configure the TFTP server:

On the TFTP server, edit the configuration file **market.cfg**.

```

#
 sysname Market
#
 telnet server enable
#
vlan 3
#
local-user market
 password simple market
 service-type telnet
 quit
#
interface Vlan-interface3
 ip address dhcp-alloc
 quit
#
interface Ten-GigabitEthernet1/0/1
 port access vlan 3
 quit
#
user-interface vty 0 4
 authentication-mode scheme
 user-role network-admin
#
return
# On the TFTP server, edit the configuration file rd.cfg.
#
 sysname RD
#
 telnet server enable

```

```
#
vlan 3
#
local-user rd
password simple rd
service-type telnet
quit
#
interface Vlan-interface3
ip address dhcp-alloc
quit
#
interface Ten-GigabitEthernet1/0/1
port access vlan 3
quit
#
user-interface vty 0 4
authentication-mode scheme
user-role network-admin
#
return
# Start TFTP service software, and specify the folder where the two configuration files reside as the
working directory. (Details not shown.)
# Verify that the TFTP server and DHCP relay agents can reach each other. (Details not shown.)
```

Verifying the configuration

1. Power on Switch D, Switch E, Switch F, and Switch G.
2. After the access devices start up, display assigned IP addresses on Switch A.

```
<SwitchA> display dhcp server ip-in-use
```

IP address	Client-identifier/ Hardware address	Lease expiration	Type
192.168.2.2	3030-3066-2e65-3233- 642e-3561-6633-2d56- 6c61-6e2d-696e-7465- 7266-6163-6533	May 6 05:21:25 2013	Auto(C)
192.168.2.3	3030-3066-2e65-3230- 302e-3232-3033-2d56- 6c61-6e2d-696e-7465- 7266-6163-6533	May 6 05:22:50 2013	Auto(C)
192.168.3.2	3030-6530-2e66-6330- 302e-3335-3131-2d56- 6c61-6e2d-696e-7465- 7266-6163-6531	May 6 05:23:15 2013	Auto(C)
192.168.3.3	3030-6530-2e66-6330- 302e-3335-3135-2d56- 6c61-6e2d-696e-7465- 7266-6163-6532	May 6 05:24:10 2013	Auto(C)

3. Telnet to 192.168.2.2 from Switch A.

```
<SwitchA> telnet 192.168.2.2
```

4. Enter the username **market** and password **market** as prompted. (Details not shown.)
You are logged in to Switch D or Switch E.

Automatic configuration using HTTP server and Tcl script

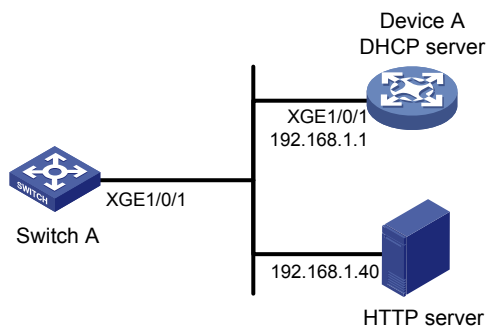
Network requirements

As shown in [Figure 47](#), Switch A does not have a configuration file.

Configure the servers so Switch A can obtain a Tcl script to complete the following configuration tasks:

- Enable the administrator to Telnet to Switch A to manage the device.
- Require the administrator to enter the correct username and password at login.

Figure 47 Network diagram



Configuration procedure

1. Configure the DHCP server:
Enable DHCP.

```
<DeviceA> system-view
[DeviceA] dhcp enable
```


Configure address pool 1 to assign IP addresses on subnet 192.168.1.0/24 to clients.

```
[DeviceA] dhcp server ip-pool 1
[DeviceA-dhcp-pool-1] network 192.168.1.0 24
```


Specify the URL of the script file for the clients.

```
[DeviceA-dhcp-pool-1] bootfile-name http://192.168.1.40/device.tcl
```
2. Configure the HTTP server:
Edit the configuration file **device.tcl** on the HTTP server.

```
return
system-view
telnet server enable
local-user user
password simple abcabc
service-type telnet
quit
user-interface vty 0 4
authentication-mode scheme
user-role network-admin
```

```
quit
```

```
interface Ten-GigabitEthernet 1/0/1
port link-mode route
ip address dhcp-alloc
return
```

```
# Start HTTP service software and enable HTTP service. (Details not shown.)
```

Verifying the configuration

1. Power on Switch A.
2. After Switch A starts up, display assigned IP addresses on Device A.
<DeviceA> display dhcp server ip-in-use

IP address	Client identifier/ Hardware address	Lease expiration	Type
192.168.1.2	0030-3030-632e-3239-3035-2e36-3736-622d-4574-6830-2f30-2f32	Dec 12 17:41:15 2013	Auto(C)
3. Telnet to 192.168.1.2 from Device A.
<DeviceA> telnet 192.168.1.2
4. Enter the username **user** and password **abcabc** as prompted. (Details not shown.)
You are logged in to Switch A.

Automatic configuration using HTTP server and Python script

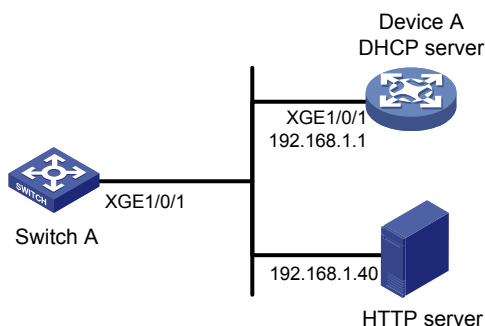
Network requirements

As shown in [Figure 48](#), Switch A does not have a configuration file.

Configure the servers so Switch A can obtain a Python script to complete the following configuration tasks:

- Enable the administrator to Telnet to Switch A to manage the device.
- Require the administrator to enter the correct username and password at login.

Figure 48 Network diagram



Configuration procedure

1. Configure the DHCP server:
Enable DHCP.

```

<DeviceA> system-view
[DeviceA] dhcp enable
# Configure address pool 1 to assign IP addresses on subnet 192.168.1.0/24 to clients.
[DeviceA] dhcp server ip-pool 1
[DeviceA-dhcp-pool-1] network 192.168.1.0 24
# Specify the URL of the script file for the clients.
[DeviceA-dhcp-pool-1] bootfile-name http://192.168.1.40/device.py
2. Configure the HTTP server:
# Edit the configuration file device.py on the HTTP server.
#!usr/bin/python

import comware
comware.CLI('system-view ;telnet server enable ;local-user user ;password simple
abcbabc ;service-type telnet ;quit ;user-interface vty 0 4 ;authentication-mode
scheme ;user-role network-admin ;quit ;interface Ten-GigabitEthernet 1/0/1 ;port
link-mode route ;ip address dhcp-alloc ;return')
# Start HTTP service software and enable HTTP service. (Details not shown.)

```

Verifying the configuration

1. Power on Switch A.
2. After Switch A starts up, display assigned IP addresses on Device A.

```

<DeviceA> display dhcp server ip-in-use

```

IP address	Client identifier/ Hardware address	Lease expiration	Type
192.168.1.2	0030-3030-632e-3239- 3035-2e36-3736-622d- 4574-6830-2f30-2f32	Dec 12 17:41:15 2013	Auto(C)
3. Telnet to 192.168.1.2 from Device A.

```

<DeviceA> telnet 192.168.1.2

```
4. Enter the username **user** and password **abcbabc** as prompted. (Details not shown.)
You are logged in to Switch A.

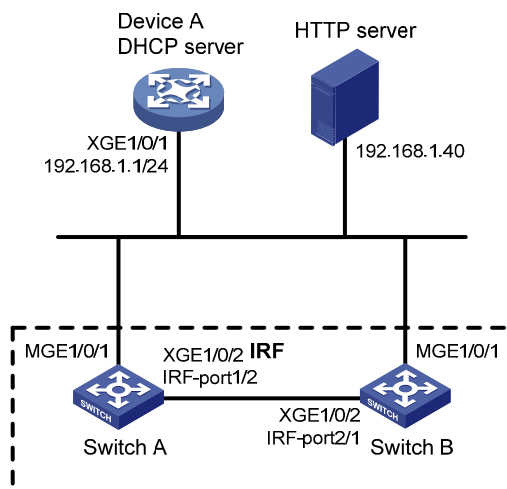
Automatic IRF setup

Network requirements

As shown in [Figure 49](#), Switch A and Switch B do not have a configuration file.

Configure the servers so the switches can obtain a Python script to complete their respective configuration and form an IRF fabric.

Figure 49 Network diagram



Configuration procedure

1. Assign IP addresses to the interfaces. Make sure the devices can reach each other. (Details not shown.)
2. Configure the following files on the HTTP server:

File	Content	Remarks
.cfg configuration file	Commands required for IRF setup.	You can create a configuration file by copying and modifying the configuration file of an existing IRF fabric.
sn.txt	Serial numbers of the member switches.	Each SN uniquely identifies a switch. These SNs will be used for assigning a unique IRF member ID to each member switch.
(Optional.) .ipe or .bin software image file	Software images.	If the member switches are running different software versions, you must prepare the software image file used for software upgrade.

File	Content	Remarks
.py Python script file	Python commands and APIs that complete the following tasks: (Optional.) Verifies that the flash memory has sufficient space for the files to be downloaded. - Downloads the configuration file and sn.txt. (Optional.) Downloads the software image file and specifies it as the main startup image file. - Resolves sn.txt and assigns a unique IRF member ID to each SN. - Specifies the configuration file as the main next-startup configuration file. - Reboots the member switches.	For more information about Python script configuration, see " Using Python ."

3. Configure Device A as the DHCP server:

```
# Enable DHCP.
<DeviceA> system-view
[DeviceA] dhcp enable

# Configure address pool 1 to assign IP addresses on subnet 192.168.1.0/24 to clients.
[DeviceA] dhcp server ip-pool 1
[DeviceA-dhcp-pool-1] network 192.168.1.0 24

# Enable the DHCP server on Ten-GigabitEthernet 1/0/1.
[DeviceA] interface Ten-GigabitEthernet 1/0/1
[DeviceA-Ten-GigabitEthernet1/0/1] dhcp select server
[DeviceA-Ten-GigabitEthernet1/0/1] quit

# Specify the URL of the script file for the clients.
[DeviceA-dhcp-pool-1] bootfile-name http://192.168.1.40/device.py
[DeviceA-dhcp-pool-1] quit
```

4. Power on Switch A and Switch B.

Switch A and Switch B will obtain the Python script file from the DHCP server and execute the script. After completing the IRF configuration, Switch A and Switch B reboot.

5. After Switch A and Switch B start up again, use a cable to connect Switch A and Switch B through their IRF physical ports.

Switch A and Switch B will elect a master member. The subordinate member will reboot to join the IRF fabric.

Verifying the configuration

On Switch A, display IRF member devices. You can also use the **display irf** command on Switch B to display IRF member devices.

```
<Switch A> display irf
```

MemberID	Slot	Role	Priority	CPU-Mac	Description
1	1	Standby	1	00e0-fc0f-8c02	---
*+2	1	Master	30	00e0-fc0f-8c14	---

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

The Bridge MAC of the IRF is: 000c-1000-1111

Auto upgrade	: yes
Mac persistent	: always
Domain ID	: 0
Auto merge	: yes

The output shows that the switches have formed an IRF fabric.

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.
	Represents an access controller, a unified wired-WLAN module, or the switching engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load-balancing device.
	Represents a security card, such as a firewall, load-balancing, NetStream, SSL VPN, IPS, or ACG card.

Port numbering in examples

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

Index

A

AAA

- RBAC AAA authorization, 49
- RBAC default user role, 54
- RBAC local AAA authentication user configuration, 59
- RBAC non-AAA authorization, 49
- RBAC user role local AAA authentication, 55
- RBAC user role non-AAA authentication, 55
- RBAC user role remote AAA authentication, 54

abbreviating command, 4

aborting

- ISSU software activate/deactivate operation (install series commands), 124

accessing

- CLI online help, 2
- emergency shell server access, 140
- login management SNMP device access, 37
- RBAC VPN instance access policy, 48

accounting

- login management command accounting, 44, 45
- login management user access control, 38

ACL

- login management command authorization, 41, 42
- login management SNMP access control, 39, 40
- login management SSH login control, 38
- login management Telnet login control, 38, 39
- login management user access control, 38

activating

- ISSU activate operation (install series commands), 124

active

- FTP active (PORT) operating mode, 73

adjusting

- ARP/ND table capacity, 163
- routing table capacity, 163

airflow direction configuration, 157, 157

alias (command keyword), 5

API

- extended Python API, 168
- extended Python API functions, 168

archiving

- configuration archive, 99
- configuration archive parameters, 100
- configuration archiving (automatic), 100
- running configuration (manual), 101

argument (CLI string/text type), 4

ASCII transfer mode, 73

assigning

- CLI user line assignment, 17
- RBAC local AAA authentication user role, 55
- RBAC non-AAA authentication user role, 55
- RBAC permission assignment, 47
- RBAC remote AAA authentication user role, 54
- RBAC user role, 54
- RBAC user role assignment, 49

authenticating

- FTP basic server authentication, 74
- login management CLI console/AUX none authentication, 19
- login management CLI console/AUX password authentication, 20
- login management CLI console/AUX scheme authentication, 21
- login management CLI none authentication mode, 18
- login management CLI password authentication mode, 18
- login management CLI scheme authentication mode, 18
- login management Telnet login none authentication, 24
- login management Telnet login password authentication, 25
- login management Telnet login scheme authentication, 26
- RBAC local AAA authentication user configuration, 59
- RBAC RADIUS authentication user configuration, 61

- RBAC temporary user role authorization (HWTACACS authentication), 64
- RBAC temporary user role authorization (RADIUS authentication), 68
- RBAC user role authentication, 58
- RBAC user role local AAA authentication, 55
- RBAC user role remote AAA authentication, 54

authorizing

- FTP basic server authorization, 74
- login management command authorization, 41, 42
- login management user access control, 38
- RBAC temporary user role authorization, 56

auto

- automatic configuration archiving, 100
- configuration. See [automatic configuration](#)

automatic configuration

- DHCP server, 175
- DNS server, 176
- file preparation, 174
- file server configuration, 174
- gateway, 177
- HTTP server+Python script, 183
- HTTP server+ Tcl script, 182
- interface selection, 177
- IRF setup, 184
- server-based, 173, 177
- start, 177
- TFTP server, 177
- USB-based, 173

AUX

- console/AUX common user line settings, 21
- console/AUX none authentication, 19
- console/AUX password authentication, 20
- console/AUX scheme authentication, 21
- login management CLI local console/AUX port login, 19
- login management overview, 14

B

backing up

- main next-startup configuration file, 103
- software upgrade backup image set, 107

banner

- configuration, 147, 147, 148, 148
- incoming type, 147, 147

- legal type, 147, 147
- login type, 147, 147
- MOTD type, 147, 147
- multiple-line input mode, 147, 147
- shell type, 147, 147
- single-line input mode, 147, 147

binary transfer mode, 73

boot loader

- startup image file specification, 110
- startup image file specification (in bulk), 110
- startup image file specification (one by one), 111

Boot ROM

- Boot ROM image preload, 110
- software upgrade image type, 106, 106
- software upgrade methods, 108
- software upgrade preparation, 109
- software upgrade system startup, 107
- startup image file specification, 110, 112
- startup image file specification (in bulk), 110
- startup image file specification (one by one), 111

C

calculating

- file digest, 89

CF card partitioning, 92

changing

- file system current working directory, 89
- FTP user account, 79

checking

- emergency shell server connectivity, 140

CLI

- command abbreviation, 4
- command entry, 3
- command history function use, 7
- command hotkey use, 5
- command keyword alias configuration, 5
- command keyword alias use, 5
- command keyword hotkey configuration, 5
- command line editing, 4
- command redisplay, 6
- command-line error message, 7
- console port login procedure, 15
- console/AUX common user line settings, 21
- console/AUX none authentication, 19
- console/AUX password authentication, 20

- console/AUX scheme authentication, 21
- device reboot (immediate), 150, 150
- device reboot (scheduled), 150, 150
- display command output filtering, 9
- display command output line numbering, 9
- display command output management, 13
- display command output save to file, 12
- display command output viewing, 13
- displaying login, 35
- emergency shell file system management, 138
- emergency shell system software image retrieval, 139
- emergency shell use, 138, 142
- enter system view from user view, 2
- local console/AUX port login, 19
- login authentication modes, 18
- login management overview, 14
- login overview, 17
- maintaining login, 35
- online help access, 2
- output control, 8
- output control keys, 9
- return to upper-level view from any view, 2
- return to user view, 2
- running configuration save, 13
- software upgrade, 106
- string/text type argument value, 4
- undo command form, 3
- use, 1
- user lines, 17
- user roles, 18
- view hierarchy, 1

client

- FTP client configuration (centralized IRF device), 81
- IPv4 TFTP client configuration, 83
- IPv6 TFTP client configuration, 84

command

- 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, 5
- CLI command keyword alias use, 5

- CLI command line editing, 4
- CLI command redisplay, 6
- CLI string/text type argument value, 4
- CLI undo command form, 3
- ISSU command series, 116
- ISSU install series commands, 121
- ISSU performance by issu series commands, 118
- line interface. *Use* CLI
- login management command accounting, 44, 45
- login management command authorization, 41, 42
- Python, 166, 166
- Tcl, 164

committing

- ISSU software changes (install series commands), 124

completing

- software upgrade, 110
- software upgrade (in bulk), 110
- software upgrade (one by one), 111
- software upgrade with a warm reboot, 112

compressing

- file, 87, 88

Comware

- software upgrade Boot image type, 106
- software upgrade feature image, 106
- software upgrade image loading, 107
- software upgrade image redundancy, 107
- software upgrade image type, 106
- software upgrade patch image, 106
- software upgrade system image type, 106

configuration

- startup configuration loading, 95

configuration file

- configuration archive, 99
- configuration archive parameters, 100
- configuration archiving (automatic), 100
- configuration rollback, 99, 101
- content, 96
- device configuration types, 94
- displaying, 104
- encryption, 97
- file formats, 96
- FIPS compliance, 97
- format, 96
- main next-startup file backup, 103

- main next-startup file restore, 103
- management, 94
- next-startup configuration file, 102
- next-startup file delete, 104
- restrictions and guidelines, 97
- running configuration archiving (manual), 101
- running configuration save, 98, 98
- startup file selection, 96
- configuring
 - automatic configuration (DHCP server), 175
 - automatic configuration (DNS server), 176
 - automatic configuration (HTTP server+Python script), 183
 - automatic configuration (HTTP server+Tcl script), 182
 - automatic configuration (IRF setup), 184
 - automatic configuration (server-based), 177
 - automatic configuration (TFTP server), 177
 - command keyword alias, 5
 - command keyword hotkey, 5
 - configuration archive parameters, 100
 - configuration rollback, 99
 - device airflow direction, 157, 157
 - device as IPv4 TFTP client, 83
 - device as IPv6 TFTP client, 84
 - device banner, 147, 147, 148, 148
 - device CPU usage monitoring, 157, 157
 - device name, 145, 145
 - device temperature alarm threshold, 159, 159
 - emergency shell management Ethernet port, 139
 - FTP, 73
 - FTP basic server parameters, 74
 - FTP client (centralized IRF device), 81
 - FTP server (centralized IRF device), 75
 - FTP server authentication, 74
 - FTP server authorization, 74
 - login management CLI console/AUX common user line settings, 21
 - login management CLI console/AUX none authentication, 19
 - login management CLI console/AUX password authentication, 20
 - login management CLI console/AUX scheme authentication, 21

- login management CLI local console/AUX port login, 19
- login management command accounting, 44, 45
- login management command authorization, 41, 42
- login management common VTY line settings, 27
- login management SNMP access control, 40
- login management SSH login, 30
- login management SSH login on device, 30
- login management Telnet login, 23
- login management Telnet login on device, 24
- login management Telnet login password authentication, 25
- login management Telnet login scheme authentication, 26
- RBAC, 47, 50, 59
- RBAC feature group, 52
- RBAC for RADIUS authentication user, 61
- RBAC local AAA authentication user, 59
- RBAC resource access policies, 53
- RBAC temporary user role authorization, 56
- RBAC temporary user role authorization (HWTACACS authentication), 64
- RBAC temporary user role authorization (RADIUS authentication), 68
- RBAC user role authentication, 58
- RBAC user role interface policy, 53
- RBAC user role rules, 51
- RBAC user role VLAN policy, 53
- TFTP, 83
- console
 - login management CLI console/AUX common user line settings, 21
 - login management CLI console/AUX none authentication, 19
 - login management CLI console/AUX password authentication, 20
 - login management CLI console/AUX scheme authentication, 21
 - login management CLI local console/AUX port login, 19
 - login management console port login procedure, 15
 - login management overview, 14
- controlling
 - CLI output, 8
 - CLI output control keys, 9

- login management SNMP access, 39
- login management SSH logins, 38
- login management Telnet logins, 38, 39
- login management user access, 38
- RBAC configuration, 47, 50
- copying
 - file, 87
- copyright statement display, 147, 147
- CPU
 - device CPU usage monitoring, 157
 - ISSU command series, 116
 - ISSU methods, 115
- creating
 - file system directory, 90
 - RBAC user role, 50
- D**
- deactivating
 - ISSU deactivate operation (install series commands), 124
- decompressing
 - file, 87, 88
 - ISSU IPE file, 122
- deleting
 - file, 88
 - next-startup configuration file, 104
 - recycle bin file, 88
- detecting
 - device port status detection timer, 157, 157
- device
 - automatic configuration, 173
 - automatic configuration (DHCP server), 175
 - automatic configuration (DNS server), 176
 - automatic configuration (HTTP server+Python script), 183
 - automatic configuration (HTTP server+Tcl script), 182
 - automatic configuration (IRF setup), 184
 - automatic configuration (server-based), 177
 - automatic configuration (TFTP server), 177
 - automatic configuration file preparation, 174
 - automatic configuration start, 177
 - CLI command history function use, 7
 - CLI command redisplay, 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, 12
- CLI display command output viewing, 13
- CLI output control, 8, 9
- CLI running configuration save, 13
- CLI use, 1
- command help information display, 80
- configuration types, 94
- emergency shell management Ethernet port configuration, 139
- emergency shell reboot, 142
- emergency shell server access, 140
- emergency shell server connectivity check, 140
- emergency shell system software image load, 141
- emergency shell use, 138, 142
- enter system view from user view, 2
- file system management, 85
- file system storage media formatting, 91
- file system storage media management, 90
- file system storage media mount, 91
- file system storage media repair, 91
- file system storage media unmount, 91
- FTP basic server parameters configuration, 74
- FTP client, 77
- FTP client configuration (centralized IRF device), 81
- FTP client connection establishment, 77
- FTP configuration, 73
- FTP connection termination, 80
- FTP connection troubleshooting, 80
- FTP manual server connection release, 75
- FTP server, 73
- FTP server authentication, 74
- FTP server authorization, 74
- FTP server configuration (centralized IRF device), 75
- FTP server directory management, 78
- FTP server files, 78
- FTP user account change, 79
- IPv4 TFTP client configuration, 83
- IPv6 TFTP client configuration, 84
- ISSU install series commands, 132, 132
- login management modem login, 32
- login management SNMP device access, 37
- login management SSH login configuration on device, 30
- login management SSH server login, 32

- login management Telnet login device configuration, 24
- login management Telnet server login, 29
- management, 145
- return to upper-level view from any view, 2
- return to user view, 2
- running configuration, 94
- software upgrade, 106
- software upgrade system startup, 107
- startup configuration, 94
- startup configuration loading, 95
- storage media CF card partition, 92
- storage media USB disk partition, 92
- TFTP configuration, 83
- device management
 - airflow direction configuration, 157, 157
 - banner configuration, 147, 147, 148, 148
 - banner input modes, 147, 147
 - banner types, 147, 147
 - configuration, 145, 145
 - copyright statement display, 147, 147
 - CPU usage monitoring, 157, 157
 - device name configuration, 145, 145
 - device reboot, 150, 150
 - device reboot (immediate), 150, 150
 - device reboot (scheduled), 150, 150
 - displaying configuration, 162, 162
 - maintaining configuration, 162, 162
 - memory usage threshold, 158, 158
 - password recovery capability disable, 156, 156
 - port status detection timer, 157, 157
 - restoring factory-default settings and states, 161, 161
 - system operating mode, 149, 149
 - system time set, 146, 146
 - system time source set, 146, 146
 - table capacity adjust, 163
 - task scheduling, 151, 151, 153, 153
 - temperature alarm threshold, 159, 159
 - transceiver module
 - diagnosis, 161, 161, 161, 161
 - transceiver module verification, 161, 161, 161, 161
 - USB interface disable, 160, 160
- DHCP
 - automatic configuration, 173
 - automatic configuration (DHCP server), 175
 - automatic configuration (HTTP server+Python script), 183
 - automatic configuration (HTTP server+Tcl script), 182
 - automatic configuration (IRF setup), 184
 - automatic configuration (server-based), 177
 - automatic configuration (TFTP server), 177
 - automatic configuration start, 177
- diagnosing
 - device transceiver modules, 161, 161, 161, 161
- directory
 - file system current working directory change, 89
 - file system current working directory display, 89
 - file system directory creation, 90
 - file system directory information display, 89
 - file system directory management, 89
 - file system directory removal, 90
 - file system management, 85
 - FTP server directory management, 78
- disabling
 - CLI output screen pausing, 9
 - device password recovery capability, 156, 156
 - device USB interface, 160, 160
 - login management Telnet login authentication, 24
- displaying
 - CLI login, 35
 - command help information, 80
 - configuration files, 104
 - device copyright statement, 147, 147
 - device management configuration, 162, 162
 - emergency shell mode device information, 142
 - file system current working directory display, 89
 - file system directory information, 89
 - file system file information, 86
 - file system text file content, 87
 - FTP client, 81
 - FTP server, 75
 - ISSU, 125
 - RBAC settings, 59
 - software upgrade image settings, 112
- DNS
 - automatic configuration, 173
 - automatic configuration (DNS server), 176

automatic configuration start, 177

E

editing command line, 4

emergency shell

device information display, 142

device reboot, 142

file system management, 138

management Ethernet port configuration, 139

server access, 140

server connectivity check, 140

software upgrade (Comware), 107

system software image, 139

system software image load, 141

use, 138, 142

enabling

CLI command redisplay, 6

configuration archiving (automatic), 100

configuration encryption, 97

device copyright statement display, 147, 147

RBAC default user role, 54

encrypting

private key, 97

public key, 97

entering

CLI entered-but-not-submitted command

redisplay, 6

command, 3

string/text type argument value, 4

system view from user view, 2

error

CLI command line error message, 7

establishing

FTP client connection, 77

Ethernet

emergency shell management Ethernet port
configuration, 139

F

factory-default

restoring factory-default settings and states, 161

fast saving running configuration, 98, 98

file

calculating digest, 89

compression, 87, 88

configuration file content, 96

configuration file format, 96

configuration file formats, 96

configuration file management, 94

copying, 87

decompression, 87, 88

deleting from recycle bin, 88

deletion, 88

device configuration startup file selection, 96

FTP server files, 78

information display, 86

ISSU IPE file decompressing, 122

management, 86

moving, 87

name format, 85

next-startup configuration file, 102

renaming, 87

restoration, 88

software upgrade file naming, 106

system. See [file system](#)

text content display, 87

file system

current working directory change, 89

current working directory display, 89

directory creation, 90

directory information display, 89

directory management, 89

directory removal, 90

file compression, 87, 88

file copy, 87

file decompression, 87, 88

file deletion, 88

file digest calculation, 89

file information display, 86

file management, 86

file move, 87

file name formats, 85

file rename, 87

file restoration, 88

file/folder operation mode, 92

management, 85

recycle bin file delete, 88

storage media CF card partition, 92

storage media CF card partitioning restrictions, 92

storage media formatting, 91

storage media management, 90

- storage media mount, 91
- storage media mounting/unmounting restrictions, 91
- storage media naming rules, 85
- storage media repair, 91
- storage media unmount, 91
- storage media USB disk partition, 92, 92
- text file content display, 87

File Transfer Protocol. *Use* FTP

filtering

- CLI display command output, 9

FIPS compliance

- configuration file, 97
- RBAC, 50

format

- configuration file, 96, 96
- file name, 85
- file system storage media formatting, 91

FTP

- automatic configuration (file server), 174
- basic server parameters configuration, 74
- client configuration (centralized IRF device), 81
- client connection establishment, 77
- command help information display, 80
- configuration, 73
- connection maintenance, 80
- connection termination, 80
- device as client, 77
- device as server, 73
- displaying client, 81
- displaying server, 75
- emergency shell server access, 140
- emergency shell system software image retrieval, 139
- IPv4 TFTP client configuration, 83
- IPv6 TFTP client configuration, 84
- local server authentication, 74
- local server authorization, 74
- manual server connection release, 75
- remote server authentication, 74
- remote server authorization, 74
- server configuration (centralized IRF device), 75
- server directory management, 78
- server files, 78
- TFTP configuration, 83

- troubleshooting connection, 80
- user account change, 79

G

gateway

- automatic configuration, 177

group

- RBAC feature group configuration, 52

H

history

- CLI history function, 7

hotkey (command), 5

HTTP

- automatic configuration (HTTP server+Python script), 183
- automatic configuration (HTTP server+ Tcl script), 182
- automatic configuration (IRF setup), 184
- ISSU HTTP feature compatible upgrade (issu series commands), 126
- ISSU HTTP feature incompatible upgrade (issu series commands), 128
- ISSU HTTP feature rollback (install series commands), 135, 135
- ISSU HTTP feature rollback (issu series commands), 130
- ISSU HTTP feature upgrade (install series commands), 132, 132, 136, 136

HWTACACS

- login management command accounting, 44, 45
- RBAC temporary user role authorization, 64

I

identifying

- CLI user line, 17

image

- emergency shell system software image retrieval, 139
- ISSU inactive software image removal (install series commands), 124
- ISSU patch image (install series commands), 123
- ISSU software image (install series commands), 122
- ISSU software image upgrade (install series commands), 122
- software upgrade Boot ROM image type, 106
- software upgrade Comware Boot image type, 106

- software upgrade Comware image loading, 107
- software upgrade Comware image redundancy, 107
- software upgrade Comware image type, 106
- software upgrade Comware system image type, 106
- startup image file specification, 110, 112
- startup image file specification (in bulk), 110
- startup image file specification (one by one), 111
- Import
 - extended Python API, 168
- incoming banner type, 147, 147
- In-Service Software Upgrade. *Use* ISSU
- install series commands
 - ISSU feature uninstall, 123
 - ISSU patch image uninstall, 123
 - ISSU software configuration rollback, 123
 - ISSU software image installation, 122
 - ISSU software image upgrade, 122
- installing, 122, *See also* install series commands
 - ISSU software images (install series commands), 122
- interface, 14, *See also* line
- IP
 - FTP configuration, 73
 - TFTP configuration, 83
- IPE file (ISSU), 122
- IPv4
 - emergency shell management Ethernet port configuration, 139
 - emergency shell server access, 140
 - emergency shell server connectivity check, 140
 - FTP client connection establishment, 77
 - TFTP client configuration, 83
- IPv6
 - emergency shell management Ethernet port configuration, 139
 - emergency shell server access, 140
 - emergency shell server connectivity check, 140
 - FTP client connection establishment, 77
 - TFTP client configuration, 84
- IRF
 - automatic configuration (IRF setup), 184
 - Boot ROM image preload, 110
 - emergency shell device reboot, 142
 - emergency shell use, 138, 142
 - FTP client configuration (centralized IRF device), 81
 - FTP server configuration (centralized IRF device), 75
 - ISSU, 115
 - ISSU (install series commands), 121
 - ISSU for multichassis IRF fabric, 118
 - ISSU for single-chassis IRF fabric, 120
 - ISSU HTTP feature compatible upgrade (issu series commands), 126
 - ISSU HTTP feature incompatible upgrade (issu series commands), 128
 - ISSU HTTP feature rollback (install series commands), 135, 135
 - ISSU HTTP feature rollback (issu series commands), 130
 - ISSU HTTP feature upgrade (install series commands), 132, 132, 136, 136
 - ISSU install series commands, 132, 132
 - ISSU issu series commands, 126
 - ISSU methods, 115
 - ISSU overview, 115
 - ISSU performance by issu series commands, 118
 - ISSU software image verification (install series commands), 124
 - non-ISSU software upgrade method, 113
 - software upgrade completion, 110
 - software upgrade completion (in bulk), 110
 - software upgrade completion (one by one), 111
 - software upgrade completion with a warm reboot, 112
 - software upgrade startup image file specification, 110, 112
 - software upgrade startup image file specification (in bulk), 110
 - software upgrade startup image file specification (one by one), 111
- ISSU
 - Boot ROM image preload, 110
 - command series, 116
 - displaying, 125
 - emergency shell use, 138, 142
 - feature uninstall (install series commands), 123
 - HTTP feature compatible upgrade (issu series commands), 126
 - HTTP feature incompatible upgrade (issu series commands), 128

- HTTP feature rollback (install series commands), [135](#), [135](#)
- HTTP feature rollback (issu series commands), [130](#)
- HTTP feature upgrade (install series commands), [132](#), [132](#), [136](#), [136](#)
- inactive software image removal (install series commands), [124](#)
- install series commands, [121](#), [132](#), [132](#)
- IPE file decompression (install series commands), [122](#)
- issu series commands, [118](#), [126](#)
- maintaining, [125](#)
- methods, [115](#)
- multichassis IRF fabric, [118](#)
- non-ISSU software upgrade, [113](#)
- overview, [115](#)
- patch image uninstall (install series commands), [123](#)
- single-chassis IRF fabric, [120](#)
- software activate/deactivate (install series commands), [124](#)
- software configuration rollback (install series commands), [123](#)
- software image (install series commands), [122](#)
- software image upgrade (install series commands), [122](#)
- software image verification (install series commands), [124](#)
- software upgrade Comware image method, [108](#)
- software upgrade non-ISSU method, [108](#)
- software upgrade procedure, [109](#)
- troubleshooting, [125](#)
- troubleshooting failure to execute, [125](#)

K

- key
 - command hotkey, [5](#)
- keyword alias configuration, [5](#)

L

- LAN
 - device management, [145](#)
- legal banner type, [147](#), [147](#)
- line
 - CLI user line assignment, [17](#)

- login management CLI console/AUX common user line settings, [21](#)
- login management CLI user line, [17](#)
- login management CLI user line identification, [17](#)
- login management VTY common line settings, [27](#)

loading

- emergency shell system software image, [141](#)

local

- RBAC local AAA authentication user configuration, [59](#)
- RBAC user role local AAA authentication, [55](#)

logging in

- login management CLI console/AUX common user line settings, [21](#)
- login management CLI console/AUX none authentication, [19](#)
- login management CLI console/AUX password authentication, [20](#)
- login management CLI console/AUX scheme authentication, [21](#)
- login management CLI local console/AUX port login, [19](#)
- login management CLI login, [17](#)
- login management CLI login authentication modes, [18](#)
- login management CLI user lines, [17](#)
- login management CLI user roles, [18](#)
- login management console port login, [15](#)
- login management modem login, [32](#)
- login management SSH login, [30](#)
- login management SSH login configuration on device, [30](#)
- login management SSH server login, [32](#)
- login management Telnet login, [23](#)
- login management Telnet login device configuration, [24](#)
- login management Telnet login max number concurrent users, [27](#)
- login management Telnet login none authentication, [24](#)
- login management Telnet login password authentication, [25](#)
- login management Telnet login scheme authentication, [26](#)
- login management Telnet server login, [29](#)
- login management VTY common line settings, [27](#)

login

- device banner login type, [147](#), [147](#)
- login management
 - CLI access, [17](#)
 - CLI console/AUX common user line settings, [21](#)
 - CLI console/AUX none authentication, [19](#)
 - CLI console/AUX password authentication, [20](#)
 - CLI console/AUX scheme authentication, [21](#)
 - CLI local console/AUX port login, [19](#)
 - CLI login authentication modes, [18](#)
 - CLI user line assignment, [17](#)
 - CLI user line identification, [17](#)
 - CLI user roles, [18](#)
 - console port access, [15](#)
 - displaying CLI login, [35](#)
 - DSCP value for outgoing Telnet packet, [27](#)
 - maintaining CLI login, [35](#)
 - modem login, [32](#)
 - overview, [14](#)
 - SNMP access control, [40](#)
 - SNMP device access, [37](#)
 - SSH login, [30](#)
 - SSH login control, [38](#)
 - SSH login on device, [30](#)
 - SSH server login, [32](#)
 - Telnet login, [23](#)
 - Telnet login control, [38](#), [39](#)
 - Telnet login device configuration, [24](#)
 - Telnet login max number concurrent users, [27](#)
 - Telnet login none authentication, [24](#)
 - Telnet login password authentication, [25](#)
 - Telnet login scheme authentication, [26](#)
 - Telnet server login, [29](#)
 - user access control, [38](#)
 - user lines, [17](#)
 - VTY common line settings, [27](#)

M

- main
 - software upgrade image set, [107](#)
- main next-startup configuration file, [103](#), [103](#)
- maintaining
 - CLI login, [35](#)
 - device management configuration, [162](#), [162](#)
 - FTP connection, [80](#)
 - ISSU, [125](#)

- software upgrade image settings, [112](#)
- management Ethernet port configuration, [139](#)
- managing
 - CLI display command output, [13](#)
 - configuration files, [94](#)
 - device. See [device management](#)
 - emergency shell file system, [138](#)
 - file system, [85](#)
 - file system directories, [89](#)
 - file system files, [86](#)
 - file system storage media, [90](#)
 - FTP server directories, [78](#)
- manual
 - FTP server connection release, [75](#)
- MDC
 - login management overview, [14](#)
- memory
 - device memory usage threshold, [158](#), [158](#)
- message
 - CLI command line error message, [7](#)
- message-of-the-day (MOTD) banner type, [147](#), [147](#)
- MIB
 - login management SNMP device access, [37](#)
- mode
 - device system operating mode, [149](#), [149](#)
 - file system file/folder alert operation mode, [92](#)
 - file system file/folder quiet operation mode, [92](#)
 - FTP active (PORT) operating mode, [73](#)
 - FTP ASCII transfer mode, [73](#)
 - FTP binary transfer mode, [73](#)
 - FTP passive (PASV) operating mode, [73](#)
 - login management none CLI authentication, [18](#)
 - login management password CLI authentication, [18](#)
 - login management scheme CLI authentication, [18](#)
 - table capacity mode, [163](#)
- modem
 - login, [32](#)
 - login management overview, [14](#)
- module
 - device transceiver module
 - diagnosis, [161](#), [161](#), [161](#), [161](#)
 - device transceiver module
 - verification, [161](#), [161](#), [161](#), [161](#)
- monitoring
 - device CPU usage, [157](#)

mounting
file system storage media, 91

moving
file, 87

MPU
emergency shell device reboot, 142
emergency shell use, 138, 142
ISSU, 115
ISSU (install series commands), 121
ISSU (issu series commands), 118
ISSU methods, 115
ISSU overview, 115

multiple-line banner input mode, 147, 147

N

naming
device name configuration, 145, 145
file name formats, 85
file rename, 87
software upgrade files, 106
storage media naming rules, 85

network
automatic configuration (DHCP server), 175
automatic configuration (DNS server), 176
automatic configuration (HTTP server+Python script), 183
automatic configuration (HTTP server+Tcl script), 182
automatic configuration (IRF setup), 184
automatic configuration (TFTP server), 177
automatic configuration file preparation, 174
automatic configuration gateway, 177
automatic configuration start, 177
command help information display, 80
device airflow direction configuration, 157, 157
device as FTP client, 77
device as FTP server, 73
device banner configuration, 147, 147
device banner input modes, 147, 147
device banner types, 147, 147
device copyright statement display, 147, 147
device CPU usage monitoring, 157, 157
device factory-default settings and states, 161
device management task
scheduling, 151, 151, 153, 153
device memory usage threshold, 158, 158

device name configuration, 145, 145
device password recovery capability
disable, 156, 156
device port status detection timer, 157, 157
device reboot, 150, 150
device reboot (immediate), 150, 150
device reboot (scheduled), 150, 150
device system operating mode, 149, 149
device system time set, 146, 146
device system time source set, 146, 146
device temperature alarm threshold, 159, 159
device transceiver module
diagnosis, 161, 161, 161, 161
device transceiver module
verification, 161, 161, 161, 161
device USB interface disable, 160, 160
emergency shell device reboot, 142
emergency shell management Ethernet port
configuration, 139
emergency shell server access, 140
emergency shell system software image load, 141
file system directory management, 89
file system file management, 86
file system storage media management, 90
FTP basic server parameters configuration, 74
FTP client configuration (centralized IRF device), 81
FTP client connection establishment, 77
FTP connection termination, 80
FTP connection troubleshooting, 80
FTP manual server connection release, 75
FTP server authentication, 74
FTP server authorization, 74
FTP server configuration (centralized IRF device), 75
FTP server directory management, 78
FTP server files, 78
FTP user account change, 79
IPv4 TFTP client configuration, 83
IPv6 TFTP client configuration, 84
ISSU command series, 116
ISSU feature (install series commands), 123
ISSU for multichassis IRF fabric, 118
ISSU for single-chassis IRF fabric, 120
ISSU inactive software image removal (install series
commands), 124
ISSU IPE file decompressing (install series
commands), 122

- ISSU patch image (install series commands), 123
- ISSU software activate/deactivate (install series commands), 124
- ISSU software changes commit (install series commands), 124
- ISSU software configuration rollback (install series commands), 123
- ISSU software image (install series commands), 122
- ISSU software image upgrade (install series commands), 122
- ISSU software image verification (install series commands), 124
- login management command
 - accounting, 44, 45
 - authorization, 41, 42
 - SNMP access control, 39, 40
 - SSH login control, 38
 - Telnet login control, 38, 39
 - RBAC default user role, 54
 - RBAC feature group configuration, 52
 - RBAC local AAA authentication user configuration, 59
 - RBAC permission assignment, 47
 - RBAC RADIUS authentication user configuration, 61
 - RBAC resource access policies, 53
 - RBAC temporary user role authorization, 56, 58
 - RBAC temporary user role authorization (HWTACACS authentication), 64
 - RBAC temporary user role authorization (RADIUS authentication), 68
 - RBAC user role assignment, 49, 54
 - RBAC user role authentication, 58
 - RBAC user role creation, 50
 - RBAC user role interface policy, 53
 - RBAC user role local AAA authentication, 55
 - RBAC user role non-AAA authentication, 55
 - RBAC user role remote AAA authentication, 54
 - RBAC user role rule configuration, 51
 - RBAC user role VLAN policy, 53
 - table capacity adjust, 163
- network management
 - automatic configuration, 173
 - automatic configuration (server-based), 177
 - CLI use, 1
 - configuration file management, 94
 - device management, 145, 145, 145
 - emergency shell use, 138, 142
 - extended Python API, 168
 - extended Python API functions, 168
 - extended Python API import, 168
 - extended Python API use, 168
 - file system management, 85
 - FTP configuration, 73
 - ISSU, 115
 - ISSU (install series commands), 121
 - ISSU HTTP feature compatible upgrade (issu series commands), 126
 - ISSU HTTP feature incompatible upgrade (issu series commands), 128
 - ISSU HTTP feature rollback (install series commands), 135, 135
 - ISSU HTTP feature rollback (issu series commands), 130
 - ISSU HTTP feature upgrade (install series commands), 132, 132, 136, 136
 - ISSU install series commands, 132, 132
 - ISSU issu series commands, 126
 - ISSU methods, 115
 - ISSU overview, 115
 - ISSU performance by issu series commands, 118
 - login management SNMP device access, 37
 - login management user access control, 38
 - non-ISSU software upgrade, 113
 - Python use, 166, 166
 - RBAC configuration, 47, 50, 59
 - software upgrade, 106
 - software upgrade with a warm reboot, 114
 - Tcl use, 164
 - TFTP configuration, 83
- next-startup configuration file, 104
- NMS
 - login management SNMP device access, 37
 - non-AAA authentication (RBAC), 55
 - non-AAA authorization (RBAC), 49
 - non-default MDC login management, 14
 - none
 - login management CLI authentication mode, 18

- login management CLI console/AUX none authentication, 19
- login management Telnet login none authentication, 24
- numbering
 - CLI display command output lines, 9
- O**
- obtaining
 - emergency shell system software image, 139
 - RBAC temporary user role authorization, 58
- online
 - CLI online help access, 2
- outputting
 - CLI display command output filtering, 9
 - CLI display command output management, 13
 - CLI display command output view, 13
 - CLI display comment output to file, 12
 - CLI output control, 8
 - CLI output control keys, 9
 - CLI output line numbering, 9
- P**
- parameter
 - configuration archive parameters, 100
 - device management, 145, 145
 - FTP basic server parameters configuration, 74
- partitioning
 - storage media CF card partition, 92
 - storage media USB disk, 92
- passive
 - FTP passive (PASV) operating mode, 73
- password
 - device password recovery capability disable, 156, 156
 - login management CLI authentication mode, 18
 - login management CLI console/AUX password authentication, 20
 - login management Telnet login password authentication, 25
 - login management Telnet login scheme authentication, 26
- patch
 - ISSU patch image, 123
 - software upgrade Comware patch image, 106
- pausing between CLI output screens, 8

- performing
 - ISSU, 115
 - ISSU (install series commands), 121
 - ISSU by issu series commands, 118
 - ISSU for multichassis IRF fabric, 118
 - ISSU for single-chassis IRF fabric, 120
 - ISSU HTTP feature compatible upgrade (issu series commands), 126
 - ISSU HTTP feature incompatible upgrade (issu series commands), 128
 - ISSU HTTP feature rollback (install series commands), 135, 135
 - ISSU HTTP feature rollback (issu series commands), 130
 - ISSU HTTP feature upgrade (install series commands), 132, 132, 136, 136
 - ISSU install series commands, 132, 132
 - ISSU issu series commands, 126
- permitting
 - RBAC permission assignment, 47
 - RBAC user role assignment, 49
- policy
 - RBAC interface access policy, 48
 - RBAC resource access policies, 53
 - RBAC user role assignment, 54
 - RBAC user role interface policy, 53
 - RBAC user role local AAA authentication, 55
 - RBAC user role non-AAA authentication, 55
 - RBAC user role remote AAA authentication, 54
 - RBAC user role VLAN policy, 53
 - RBAC VLAN access policy, 48
 - RBAC VPN instance access policy, 48
- port
 - device status detection timer, 157, 157
 - emergency shell management Ethernet port configuration, 139
- preloading
 - Boot ROM image, 110
- preparing
 - software upgrade (non-ISSU), 109
- procedure
 - abbreviating CLI command, 4
 - aborting ISSU software activate/deactivate (install series commands), 124
 - accessing CLI online help, 2
 - accessing server with emergency shell, 140

- adjusting table capacities, 163
- archiving running configuration (manual), 101
- assigning RBAC local AAA authentication user role, 55
- assigning RBAC non-AAA authentication user role, 55
- assigning RBAC remote AAA authentication user role, 54
- assigning RBAC user role, 54
- backing up main next-startup configuration file, 103
- calculating file digest, 89
- changing current working directory, 89
- changing FTP user accounts, 79
- checking emergency shell server connectivity with emergency shell, 140
- committing ISSU software changes (install series commands), 124
- completing software upgrade, 110
- completing software upgrade (in bulk), 110
- completing software upgrade (one by one), 111
- completing software upgrade with a warm reboot, 112
- compressing file, 87, 88
- configuring automatic configuration (DHCP server), 175
- configuring automatic configuration (DNS server), 176
- configuring automatic configuration gateway, 177
- configuring CLI command hotkey, 5
- configuring CLI command keyword alias, 5
- configuring configuration archive parameters, 100
- configuring configuration rollback, 99
- configuring device airflow direction, 157, 157
- configuring device as IPv4 TFTP client, 83
- configuring device as IPv6 TFTP client, 84
- configuring device banner, 147, 147, 148, 148
- configuring device CPU usage monitoring, 157
- configuring device name, 145, 145
- configuring device temperature alarm threshold, 159, 159
- configuring emergency shell management Ethernet port, 139
- configuring FTP basic server parameters, 74

- configuring FTP client (centralized IRF device), 81
- configuring FTP server (centralized IRF device), 75
- configuring FTP server local authentication, 74
- configuring FTP server local authorization, 74
- configuring FTP server remote authentication, 74
- configuring FTP server remote authorization, 74
- configuring login management CLI console/AUX common user line settings, 21
- configuring login management CLI console/AUX password authentication, 20
- configuring login management CLI console/AUX scheme authentication, 21
- configuring login management CLI local console/AUX port login, 19
- configuring login management command accounting, 44, 45
- configuring login management command authorization, 41, 42
- configuring login management SNMP access control, 40
- configuring login management SSH login, 30
- configuring login management SSH login on device, 30
- configuring login management Telnet login, 23
- configuring login management Telnet login on device, 24
- configuring login management Telnet login password authentication, 25
- configuring login management Telnet login scheme authentication, 26
- configuring login management VTY common line settings, 27
- configuring RBAC, 50, 59
- configuring RBAC feature group, 52
- configuring RBAC for RADIUS authentication user, 61
- configuring RBAC local AAA authentication user, 59
- configuring RBAC resource access policies, 53
- configuring RBAC temporary user role authorization, 56
- configuring RBAC temporary user role authorization (HWTACACS authentication), 64
- configuring RBAC temporary user role authorization (RADIUS authentication), 68
- configuring RBAC user role authentication, 58
- configuring RBAC user role interface policy, 53

- configuring RBAC user role rules, 51
- configuring RBAC user role VLAN policy, 53
- controlling CLI output, 8, 9
- controlling login management SNMP access, 39
- controlling login management SSH logins, 38
- controlling login management Telnet logins, 38, 39
- copying file, 87
- creating directory, 90
- creating RBAC user role, 50
- decompressing file, 87, 88
- decompressing ISSU IPE file (install series commands), 122
- deleting file, 88
- deleting file from recycle bin, 88
- deleting next-startup configuration file, 104
- diagnosing device transceiver module, 161, 161, 161, 161
- disabling device USB interface, 160, 160
- disabling CLI console/AUX authentication, 19
- disabling CLI output screen pausing, 9
- disabling device password recovery capability, 156, 156
- disabling login management Telnet login authentication, 24
- displaying CLI login, 35
- displaying command help information, 80
- displaying configuration files, 104
- displaying current working directory, 89
- displaying device management configuration, 162, 162
- displaying directory information, 89
- displaying emergency shell mode device information, 142
- displaying file information, 86
- displaying FTP client, 81
- displaying FTP server, 75
- displaying ISSU, 125
- displaying RBAC settings, 59
- displaying software upgrade image settings, 112
- displaying text file content, 87
- editing CLI command line, 4
- enabling CLI redisplay of entered-but-not-submitted command, 6

- enabling configuration archiving (automatic), 100
- enabling configuration encryption, 97
- enabling device copyright statement display, 147, 147
- enabling RBAC default user role, 54
- entering CLI command, 3
- entering CLI string/text type argument value, 4
- entering Python shell, 166
- entering system view from user view, 2
- entering Tcl configuration view, 164
- establishing FTP client connection, 77
- executing Comware commands in Tcl configuration view, 165
- executing Python script, 166
- filtering CLI display command output, 9
- formatting file system storage media, 91
- installing ISSU software images (install series commands), 122
- loading emergency shell system software image, 141
- logging in through modems, 32
- logging in to SSH server (device login), 32
- logging in to Telnet server (device login), 29
- maintaining CLI login, 35
- maintaining device management configuration, 162, 162
- maintaining FTP connection, 80
- maintaining ISSU, 125
- maintaining software upgrade image settings, 112
- managing CLI display command output, 13
- managing file system (emergency shell), 138
- managing file system directories, 89
- managing file system files, 86
- managing file system storage media, 90
- managing FTP server directories, 78
- manually releasing FTP server connection, 75
- mounting file system storage media, 91
- moving file, 87
- numbering CLI display command output lines, 9
- obtaining emergency shell system software image, 139
- obtaining RBAC temporary user role authorization, 58
- partitioning CF card, 92
- partitioning USB disk, 92
- pausing between CLI output screens, 8

- performing ISSU, 115
- performing ISSU (install series commands), 121
- performing ISSU for multichassis IRF fabric, 118
- performing ISSU for single-chassis IRF fabric, 120
- performing ISSU HTTP feature compatible upgrade (issu series commands), 126
- performing ISSU HTTP feature incompatible upgrade (issu series commands), 128
- performing ISSU HTTP feature rollback (install series commands), 135, 135
- performing ISSU HTTP feature rollback (issu series commands), 130
- performing ISSU HTTP feature upgrade (install series commands), 132, 132, 136, 136
- performing ISSU install series commands, 132, 132
- performing ISSU issu series commands, 126
- preloading Boot ROM image, 110
- preparing automatic configuration files, 174
- preparing for software upgrade (non-ISSU), 109
- rebooting device, 150, 150
- rebooting device (immediate), 150, 150
- rebooting device (scheduled), 150, 150
- rebooting device with emergency shell, 142
- removing directory, 90
- removing ISSU inactive software image (install series commands), 124
- renaming file, 87
- repairing file system storage media, 91
- restoring factory-default settings and states, 161
- restoring file, 88
- restoring main next-startup configuration file, 103
- returning to Tcl user view, 164
- returning to upper-level view from any view, 2
- returning to user view, 2
- rolling back configuration, 101
- rolling back ISSU software configuration (install series commands), 123
- saving CLI display command output to file, 12
- saving CLI running configuration, 13
- saving running configuration, 98, 98
- scheduling device management task, 151, 151, 153, 153
- selecting automatic configuration interface, 177

- setting device memory usage threshold, 158, 158
- setting device port status detection timer, 157, 157
- setting device system operating mode, 149, 149
- setting device system time, 146, 146
- setting DSCP value for outgoing Telnet packet, 27
- setting file/folder operation mode, 92
- setting login management Telnet login max number concurrent users, 27
- specifying device system time source, 146, 146
- specifying next-startup configuration file, 102
- specifying startup image file, 110, 112
- specifying startup image file (in bulk), 110
- specifying startup image file (one by one), 111
- terminating FTP connection, 80
- troubleshooting FTP connection, 80
- troubleshooting ISSU, 125
- troubleshooting ISSU failure to execute, 125
- troubleshooting RBAC local user access permissions, 71
- troubleshooting RBAC login attempts by RADIUS users fail, 71
- understanding CLI command-line error message, 7
- uninstalling ISSU feature (install series commands), 123
- uninstalling ISSU patch images (install series commands), 123
- unmounting file system storage media, 91
- upgrading ISSU software images (install series commands), 122
- upgrading software, 109
- upgrading software with a warm reboot, 114
- upgrading software with non-ISSU method, 113
- using CLI command history function, 7
- using CLI command hotkey, 5
- using CLI command keyword alias, 5
- using CLI undo command form, 3
- using emergency shell, 142
- using Python, 166
- verifying device transceiver module, 161, 161, 161, 161
- verifying ISSU software image (install series commands), 124
- viewing CLI display command output, 13
- working with FTP server files, 78

Python

- automatic configuration (HTTP server+Python script), 183
- automatic configuration (IRF setup), 184
- extended API, 168
- extended API functions, 168
- script, 166
- shell, 166
- use, 166, 166

R

RADIUS

- RBAC RADIUS authentication user configuration, 61
- RBAC temporary user role authorization, 68

RBAC

- AAA authorization, 49
- configuration, 47, 50, 59
- default user role, 54
- feature group configuration, 52
- FIPS compliance, 50
- local AAA authentication user configuration, 59
- non-AAA authorization, 49
- permission assignment, 47
- predefined user roles, 48
- RADIUS authentication user configuration, 61
- resource access policies, 48, 53
- rule configuration restrictions, 51
- settings display, 59
- temporary user role authorization, 58
- temporary user role authorization (HWTACACS authentication), 64
- temporary user role authorization (RADIUS authentication), 68
- temporary user role authorization configuration, 56
- troubleshoot, 71
- troubleshoot local user access permissions, 71
- troubleshoot login attempts by RADIUS users fail, 71
- user role assignment, 49, 54
- user role authentication, 58
- user role creation, 50
- user role interface policy, 53
- user role local AAA authentication, 55
- user role non-AAA authentication, 55
- user role remote AAA authentication, 54

- user role rule configuration, 51
- user role rules, 47
- user role VLAN policy, 53

rebooting

- device, 150, 150
- device (immediate), 150, 150
- device (scheduled), 150, 150
- emergency shell device reboot, 142

remote

- RBAC user role AAA authentication, 54

removing

- file system directory, 90
- ISSU inactive software image (install series commands), 124

renaming

- file, 87

repairing

- file system storage media, 91

resource

- RBAC resource access policies, 53

restoring

- factory-default settings and states, 161
- file, 88
- main next-startup configuration file, 103

restrictions

- partitioning storage media CF cards, 92
- partitioning storage media USB disks, 92
- RBAC rule configuration, 51
- Tcl, 164
- unmounting file system storage media, 91

returning

- to upper-level view from any view, 2
- to user view, 2

role

- RBAC default user role, 54
- RBAC predefined user roles, 48
- RBAC temporary user role authorization, 56, 58
- RBAC user role assignment, 49, 54
- RBAC user role authentication, 58
- RBAC user role creation, 50
- RBAC user role interface policy, 53
- RBAC user role local AAA authentication, 55
- RBAC user role non-AAA authentication, 55
- RBAC user role remote AAA authentication, 54
- RBAC user role rule configuration, 51

- RBAC user role VLAN policy, [53](#)
- role-based access control. Use [RBAC](#)
- rolling back
 - configuration, [99](#), [101](#)
 - ISSU HTTP feature rollback (install series commands), [135](#), [135](#)
 - ISSU HTTP feature rollback (issu series commands), [130](#)
 - ISSU software configuration (install series commands), [123](#)
- routing
 - FTP configuration, [73](#)
 - TFTP configuration, [83](#), [83](#)
- rule
 - file system storage media naming, [85](#)
 - RBAC command rule, [47](#)
 - RBAC feature execute rule, [47](#)
 - RBAC feature group rule, [47](#)
 - RBAC feature read rule, [47](#)
 - RBAC feature write rule, [47](#)
 - RBAC OID rule, [47](#)
 - RBAC user role rule configuration, [51](#)
 - RBAC Web menu rule, [47](#)
 - RBAC XML element rule, [47](#)
- running configuration
 - archiving, [99](#)
 - archiving (manual), [101](#)
 - CLI save, [13](#)
 - device, [94](#)
 - encryption, [97](#)
 - rollback, [99](#)
 - saving (fast mode), [98](#), [98](#)
 - saving (safe mode), [98](#), [98](#)

S

- safe saving running configuration, [98](#), [98](#)
- saving
 - CLI display command output to file, [12](#)
 - CLI running configuration, [13](#)
 - running configuration, [98](#), [98](#)
- scheduling
 - device management task, [151](#), [151](#), [153](#), [153](#)
 - device reboot (scheduled), [150](#), [150](#)
- scheme
 - login management CLI authentication mode, [18](#)

- login management CLI console/AUX common user line settings, [21](#)
- login management CLI console/AUX scheme authentication, [21](#)
- script
 - extended Python API, [168](#)
 - extended Python API functions, [168](#)
 - Python, [166](#), [166](#), [166](#)
- scripting
 - automatic configuration (HTTP server+Python script), [183](#)
 - automatic configuration (HTTP server+Tcl script), [182](#)
- security
 - configuration encryption, [97](#)
 - device USB interface disable, [160](#), [160](#)
 - login management command accounting, [44](#), [45](#)
 - login management command authorization, [41](#), [42](#)
 - login management SNMP access control, [39](#), [40](#)
 - login management SSH login control, [38](#)
 - login management Telnet login control, [38](#), [39](#)
 - login management user access control, [38](#)
 - RBAC configuration, [47](#), [50](#), [59](#)
 - RBAC default user role, [54](#)
 - RBAC feature group configuration, [52](#)
 - RBAC local AAA authentication user configuration, [59](#)
 - RBAC permission assignment, [47](#)
 - RBAC RADIUS authentication user configuration, [61](#)
 - RBAC resource access policies, [53](#)
 - RBAC temporary user role authorization, [56](#), [58](#)
 - RBAC temporary user role authorization (HWTACACS authentication), [64](#)
 - RBAC temporary user role authorization (RADIUS authentication), [68](#)
 - RBAC user role assignment, [49](#), [54](#)
 - RBAC user role authentication, [58](#)
 - RBAC user role creation, [50](#)
 - RBAC user role interface policy, [53](#)
 - RBAC user role local AAA authentication, [55](#)
 - RBAC user role non-AAA authentication, [55](#)
 - RBAC user role remote AAA authentication, [54](#)
 - RBAC user role rule configuration, [51](#)
 - RBAC user role VLAN policy, [53](#)
- selecting
 - automatic configuration interface, [177](#)

server

- automatic configuration (DHCP server), 175
- automatic configuration (DNS server), 176
- automatic configuration (file server), 174
- automatic configuration (HTTP server+Python script), 183
- automatic configuration (HTTP server+Tcl script), 182
- automatic configuration (IRF setup), 184
- automatic configuration (server-based), 177
- automatic configuration (TFTP server), 177
- automatic configuration file preparation, 174
- automatic configuration gateway, 177
- automatic configuration start, 177
- emergency shell server connectivity check, 140
- FTP server directory management, 78

setting

- device memory usage threshold, 158, 158
- device port status detection timer, 157, 157
- device system operating mode, 149, 149
- device system time, 146, 146
- DSCP value for outgoing Telnet packet, 27
- file/folder operation mode, 92
- login management Telnet login max number concurrent users, 27

shell

- Python, 166

shell banner type, 147, 147

single-line banner input mode, 147, 147

SNMP

- access control, 39, 40
- access management overview, 14
- device access, 37

SNMPv1

- login management SNMP device access, 37

SNMPv2

- login management SNMP device access, 37

SNMPv3

- login management SNMP device access, 37

software

- emergency shell system software image load, 141
- emergency shell system software image retrieval, 139
- emergency shell use, 138, 142

upgrade. See [software upgrade](#)

software upgrade

- Boot ROM image preload, 110
- Boot ROM image type, 106
- CLI method, 106
- completion, 110
- completion (in bulk), 110
- completion (one by one), 111
- completion with a warm reboot, 112
- Comware Boot image type, 106
- Comware feature image, 106
- Comware image loading, 107
- Comware image redundancy, 107
- Comware image type, 106
- Comware patch image, 106
- Comware system image type, 106
- file naming, 106
- image settings display, 112
- image settings maintain, 112
- ISSU, 115
- ISSU (install series commands), 121
- ISSU HTTP feature compatible upgrade (issu series commands), 126
- ISSU HTTP feature incompatible upgrade (issu series commands), 128
- ISSU HTTP feature rollback (install series commands), 135, 135
- ISSU HTTP feature rollback (issu series commands), 130
- ISSU HTTP feature upgrade (install series commands), 132, 132, 136, 136
- ISSU inactive software image removal (install series commands), 124
- ISSU install series commands, 132, 132
- ISSU IPE file decompressing (install series commands), 122
- ISSU issu series commands, 126
- ISSU overview, 115
- ISSU performance by issu series commands, 118
- ISSU software configuration rollback (install series commands), 123
- ISSU software image (install series commands), 122
- ISSU software image upgrade (install series commands), 122
- methods, 108
- non-ISSU upgrade, 113

- non-ISSU upgrade preparation, 109
- overview, 106
- procedure, 109
- startup image file specification, 110, 112
- startup image file specification (in bulk), 110
- startup image file specification (one by one), 111
- system startup, 107
- upgrade with a warm reboot, 114
- specifying
 - device system time source, 146, 146
 - next-startup configuration file, 102
- SSH
 - login, 30
 - login configuration on device, 30
 - login control, 38
 - login management overview, 14
 - server login, 32
- starting
 - automatic configuration, 177
- starting up
 - Boot ROM image preload, 110
 - software upgrade procedure, 109
 - software upgrade system startup, 107
 - software upgrade with a warm reboot, 114
 - software upgrade with non-ISSU method, 113
 - startup image file specification, 110, 112
 - startup image file specification (in bulk), 110
 - startup image file specification (one by one), 111
- startup
 - configuration loading, 95
 - device configuration startup file selection, 96
 - device configuration), 94
 - next-startup configuration file, 102
- storage media
 - CF card partition, 92, 92
 - file system management, 85
 - file system storage media naming rules, 85
 - formatting, 91
 - management, 90
 - mounting, 91
 - repair, 91
 - unmounting, 91
 - USB disk partition, 92, 92
- string type argument value, 4
- system
 - software upgrade Comware feature image, 106
 - software upgrade Comware image loading, 107
 - software upgrade Comware image redundancy, 107
 - software upgrade Comware patch image, 106
 - software upgrade Comware system image type, 106
 - software upgrade startup process, 107
 - system administration
 - automatic configuration, 173
 - automatic configuration (DHCP server), 175
 - automatic configuration (DNS server), 176
 - automatic configuration (HTTP server+Python script), 183
 - automatic configuration (HTTP server+Tcl script), 182
 - automatic configuration (IRF setup), 184
 - automatic configuration (server-based), 177
 - automatic configuration (TFTP server), 177
 - automatic configuration file preparation, 174
 - automatic configuration gateway, 177
 - automatic configuration interface selection, 177
 - automatic configuration start, 177
 - 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, 5
 - CLI command keyword alias use, 5
 - CLI command line editing, 4
 - CLI command redisplay, 6
 - CLI command-line error message, 7
 - 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, 12
 - CLI display command output viewing, 13
 - CLI online help access, 2
 - CLI output control, 8, 9
 - CLI running configuration save, 13
 - CLI string/text type argument value, 4
 - CLI undo command form, 3
 - CLI use, 1
 - CLI view hierarchy, 1

- configuration archive parameters, 100
- configuration archiving (automatic), 100
- configuration file encryption, 97
- configuration file formats, 96
- configuration file main next-startup file backup, 103
- configuration file main next-startup file restore, 103
- configuration file management, 94
- configuration file next-startup file delete, 104
- configuration rollback, 99, 101
- device airflow direction configuration, 157, 157
- device banner
 - configuration, 147, 147, 148, 148
- device banner input modes, 147, 147
- device banner types, 147, 147
- device configuration startup file selection, 96
- device copyright statement display, 147, 147
- device CPU usage monitoring, 157, 157
- device factory-default settings and states, 161
- device management, 145, 145, 145
- device management task
 - scheduling, 151, 151, 153, 153
- device memory usage threshold, 158, 158
- device name configuration, 145, 145
- device password recovery capability
 - disable, 156, 156
- device port status detection timer, 157, 157
- device reboot, 150, 150
- device reboot (immediate), 150, 150
- device reboot (scheduled), 150, 150
- device system operating mode, 149, 149
- device system time set, 146, 146
- device system time source set, 146, 146
- device temperature alarm threshold, 159, 159
- device transceiver module
 - diagnosis, 161, 161, 161, 161
 - verification, 161, 161, 161, 161
- device USB interface disable, 160, 160
- emergency shell file system management, 138
- emergency shell server connectivity check, 140
- emergency shell system software image retrieval, 139
- emergency shell use, 138, 142
- enter system view from user view, 2

- executing Comware commands, 165
- extended Python API, 168
- extended Python API functions, 168
- extended Python API import, 168
- extended Python API use, 168
- file system directory management, 89
- file system file management, 86
- file system file name formats, 85
- file system management, 85
- file system storage media management, 90
- file system storage media naming rules, 85
- FTP configuration, 73
- ISSU command series, 116
- ISSU feature (install series commands), 123
- ISSU for multichassis IRF fabric, 118
- ISSU for single-chassis IRF fabric, 120
- ISSU HTTP feature compatible upgrade (issu series commands), 126
- ISSU HTTP feature incompatible upgrade (issu series commands), 128
- ISSU HTTP feature rollback (install series commands), 135, 135
- ISSU HTTP feature rollback (issu series commands), 130
- ISSU HTTP feature upgrade (install series commands), 132, 132, 136, 136
- ISSU inactive software image removal (install series commands), 124
- ISSU install series commands, 132, 132
- ISSU issu series commands, 126
- ISSU overview, 115
- ISSU patch image (install series commands), 123
- ISSU performance by issu series commands, 118
- ISSU software activate/deactivate (install series commands), 124
- ISSU software changes commit (install series commands), 124
- ISSU software configuration rollback (install series commands), 123
- ISSU software image verification (install series commands), 124
- login management CLI console/AUX common user line settings, 21
- login management CLI console/AUX none authentication, 19

- login management CLI console/AUX password authentication, 20
- login management CLI console/AUX scheme authentication, 21
- login management CLI local console/AUX port login, 19
- login management CLI login, 17
- login management CLI login authentication modes, 18
- login management CLI user lines, 17
- login management CLI user roles, 18
- login management command
 - accounting, 44, 45
 - authorization, 41, 42
- login management console port login procedure, 15
- login management modem login, 32
- login management overview, 14
- login management SNMP access control, 39, 40
- login management SSH login, 30
- login management SSH login configuration on device, 30
- login management SSH login control, 38
- login management SSH server login, 32
- login management Telnet login, 23
- login management Telnet login control, 38, 39
- login management Telnet login device configuration, 24
- login management Telnet login max number concurrent users, 27
- login management Telnet login none authentication, 24
- login management Telnet login password authentication, 25
- login management Telnet login scheme authentication, 26
- login management Telnet packet DSCP value, 27
- login management Telnet server login, 29
- login management user access control, 38
- login management VTY common line settings, 27
- next-startup configuration file specification, 102
- Python script execute, 166
- Python shell, 166

- Python use, 166, 166
- return to upper-level view from any view, 2
- return to user view, 2
- running configuration archiving (manual), 101
- running configuration save, 98
- software upgrade, 106
- software upgrade completion, 110
- software upgrade completion (in bulk), 110
- software upgrade completion (one by one), 111
- software upgrade completion with a warm reboot, 112
- table capacity adjust, 163
- Tcl configuration view, 164
- Tcl use, 164
- Tcl user view, 164
- TFTP configuration, 83

T

- task scheduling (device management), 151, 151, 153, 153

Tcl

- automatic configuration (HTTP server+Tcl script), 182
- configuration view, 164
- executing Comware commands, 165
- restrictions, 164
- use, 164
- user view, 164

TCP

- device as FTP client, 77
- device as FTP server, 73
- FTP client connection establishment, 77
- FTP configuration, 73
- IPv4 TFTP client configuration, 83
- IPv6 TFTP client configuration, 84
- TFTP configuration, 83

Telnet

- DSCP value for outgoing packet, 27
- login, 23
- login control, 38, 39
- login device configuration, 24
- login management overview, 14
- login max number concurrent users, 27
- login none authentication, 24
- login password authentication, 25
- login scheme authentication, 26

- server login, [29](#)
- VTY common line settings, [27](#)
- temperature
 - device temperature alarm threshold, [159](#), [159](#)
- terminating
 - FTP connection, [80](#)
- text file content display, [87](#)
- text type argument value, [4](#)
- TFTP, [83](#), *See also* [FTP](#)
 - automatic configuration, [173](#)
 - automatic configuration (file server), [174](#)
 - automatic configuration (server-based), [177](#)
 - automatic configuration (TFTP server), [177](#)
 - automatic configuration start, [177](#)
 - configuration, [83](#)
 - emergency shell server access, [140](#)
 - emergency shell system software image retrieval, [139](#)
 - IPv4 client configuration, [83](#)
 - IPv6 client configuration, [84](#)
 - main next-startup configuration file, [103](#), [103](#)
- threshold
 - device memory usage, [158](#), [158](#)
 - device temperature threshold alarm, [159](#), [159](#)
- time
 - device system time set, [146](#), [146](#)
 - device system time source set, [146](#), [146](#)
- timer
 - device port status detection, [157](#), [157](#)
- tool command language. *Use* [Tcl](#)
- transceiver
 - device module diagnosis, [161](#), [161](#), [161](#), [161](#)
 - device module verification, [161](#), [161](#), [161](#), [161](#)
- Trivial File Transfer Protocol. *Use* [TFTP](#)
- troubleshooting
 - FTP connection, [80](#)
 - ISSU, [125](#)
 - ISSU failure to execute, [125](#)
 - RBAC, [71](#)
 - RBAC local user access permissions, [71](#)
 - RBAC login attempts by RADIUS users fail, [71](#)

U

- undo command form, [3](#)
- uninstalling
- ISSU feature (install series commands), [123](#)
- ISSU patch images (install series commands), [123](#)
- unmounting
 - file system storage media, [91](#)
- upgrading
 - ISSU HTTP feature compatible upgrade (issu series commands), [126](#)
 - ISSU HTTP feature incompatible upgrade (issu series commands), [128](#)
 - ISSU HTTP feature upgrade (install series commands), [132](#), [132](#), [136](#), [136](#)
 - ISSU software images (install series commands), [122](#)
 - software. *See* [software upgrade](#)
- USB
 - device USB interface disable, [160](#), [160](#)
 - disk partitioning, [92](#)
- user
 - interface, [14](#), *See also* user line
 - interface login management VTY common line settings, [27](#)
- user access
 - RBAC configuration, [47](#), [50](#), [59](#)
 - RBAC feature group configuration, [52](#)
 - RBAC local AAA authentication user configuration, [59](#)
 - RBAC permission assignment, [47](#)
 - RBAC predefined user roles, [48](#)
 - RBAC RADIUS authentication user configuration, [61](#)
 - RBAC resource access policies, [53](#)
 - RBAC temporary user role authorization, [56](#), [58](#)
 - RBAC temporary user role authorization (HWTACACS authentication), [64](#)
 - RBAC temporary user role authorization (RADIUS authentication), [68](#)
 - RBAC user role assignment, [49](#), [54](#)
 - RBAC user role authentication, [58](#)
 - RBAC user role creation, [50](#)
 - RBAC user role interface policy, [53](#)
 - RBAC user role local AAA authentication, [55](#)
 - RBAC user role non-AAA authentication, [55](#)
 - RBAC user role remote AAA authentication, [54](#)
 - RBAC user role rule configuration, [51](#)
 - RBAC user role rules, [47](#)
 - RBAC user role VLAN policy, [53](#)
- user access control

- login control, [38](#)
- login management command
 - accounting, [44](#), [45](#)
 - login management command
 - authorization, [41](#), [42](#)
 - login management SNMP access control, [39](#), [40](#)
 - login management SSH login control, [38](#)
 - login management Telnet login control, [38](#), [39](#)

using

- automatic configuration, [173](#)
- CLI, [1](#)
- command history function, [7](#)
- command hotkey, [5](#)
- command keyword alias, [5](#)
- device as FTP client, [77](#)
- device as FTP server, [73](#)
- Extended Python API, [168](#), [168](#)
- Python, [166](#), [166](#)
- Tcl, [164](#)
- undo command form, [3](#)

V

verifying

- device transceiver modules, [161](#), [161](#), [161](#), [161](#)
- ISSU software image (install series commands), [124](#)

viewing

- CLI display command output, [13](#)

VLAN

- RBAC user role VLAN policy, [53](#)
- RBAC VLAN access policy, [48](#)

VPN

- RBAC VPN instance access policy, [48](#)

VTY line settings, [27](#)

W

working with

- FTP server files, [78](#)