© Copyright 2016 Hewlett Packard Enterprise Development LP

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.


Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Intel®, Itanium®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the United States and other countries.

Microsoft® and Windows® are trademarks of the Microsoft group of companies.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java and Oracle are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.
Contents

Using the CLI ................................................................. 1
  CLI views .................................................................. 1
  Entering system view from user view .............................. 2
  Returning to the upper-level view from any view .......... 2
  Returning to user view ................................................... 2
  Accessing the CLI online help ........................................ 2
  Using the undo form of a command ............................. 3
  Entering a command ....................................................... 3
  Editing a command line .................................................. 3
  Entering a text or string type value for an argument ........ 4
  Abbreviating commands ............................................... 4
  Configuring and using command keyword aliases .......... 4
  Configuring and using command hotkeys ..................... 5
  Enabling redisplaying entered-but-not-submitted commands .................................................. 6
  Understanding command-line error messages ................. 6
  Using the command history function ............................ 7
  Controlling the CLI output .............................................. 8
  Pausing between screens of output .............................. 8
  Numbering each output line from a display command ...... 8
  Filtering the output from a display command ................. 9
  Saving the output from a display command to a file ...... 11
  Viewing and managing the output from a display command effectively .................................................. 12
  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 ......................................................... 18
  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 ... 20
    Configuring common AUX line settings ................. 21
  Logging in through Telnet .......................................... 22
    Configuring Telnet login on the device .............. 23
    Using the device to log in to a Telnet server ........ 23
  Logging in through SSH .............................................. 28
    Configuring SSH login on the device ............ 28
    Using the device to log in to an SSH server .......... 30
  Logging in through a pair of modems ................. 30
  Displaying and maintaining CLI login ................. 33
Accessing the device through SNMP ................................. 34
Controlling user access .................................................. 35
  FIPS compliance ......................................................... 35
  Controlling Telnet/SSH logins .................................... 35
    Configuration procedures ........................................ 35
    Configuration example ............................................ 35
  Controlling SNMP access ............................................ 36
    Configuration procedure ......................................... 36
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring FTP</td>
<td>68</td>
</tr>
<tr>
<td>Establishing an FTP connection</td>
<td>71</td>
</tr>
<tr>
<td>Managing directories on the FTP server</td>
<td>73</td>
</tr>
<tr>
<td>Working with files on the FTP server</td>
<td>73</td>
</tr>
<tr>
<td>Changing to another user account</td>
<td>74</td>
</tr>
<tr>
<td>Maintaining and troubleshooting the FTP connection</td>
<td>74</td>
</tr>
<tr>
<td>Terminating the FTP connection</td>
<td>75</td>
</tr>
<tr>
<td>Displaying command help information</td>
<td>75</td>
</tr>
<tr>
<td>FTP client configuration example</td>
<td>75</td>
</tr>
<tr>
<td>Configuring RBAC</td>
<td>43</td>
</tr>
<tr>
<td>Overview</td>
<td>43</td>
</tr>
<tr>
<td>Permission assignment</td>
<td>43</td>
</tr>
<tr>
<td>Assigning user roles</td>
<td>45</td>
</tr>
<tr>
<td>FIPS compliance</td>
<td>46</td>
</tr>
<tr>
<td>Configuration task list</td>
<td>46</td>
</tr>
<tr>
<td>Creating user roles</td>
<td>46</td>
</tr>
<tr>
<td>Configuring user role rules</td>
<td>46</td>
</tr>
<tr>
<td>Configuration restrictions and guidelines</td>
<td>47</td>
</tr>
<tr>
<td>Configuration procedure</td>
<td>47</td>
</tr>
<tr>
<td>Configuring feature groups</td>
<td>48</td>
</tr>
<tr>
<td>Configuring resource access policies</td>
<td>48</td>
</tr>
<tr>
<td>Configuring the interface policy of a user role</td>
<td>48</td>
</tr>
<tr>
<td>Configuring the VLAN policy of a user role</td>
<td>49</td>
</tr>
<tr>
<td>Configuring the VPN instance policy of a user role</td>
<td>49</td>
</tr>
<tr>
<td>Assigning user roles</td>
<td>50</td>
</tr>
<tr>
<td>Enabling the default user role feature</td>
<td>50</td>
</tr>
<tr>
<td>Assigning user roles to remote AAA authentication users</td>
<td>50</td>
</tr>
<tr>
<td>Assigning user roles to local AAA authentication users</td>
<td>50</td>
</tr>
<tr>
<td>Assigning user roles to non-AAA authentication users on user lines</td>
<td>51</td>
</tr>
<tr>
<td>Configuring temporary user role authorization</td>
<td>52</td>
</tr>
<tr>
<td>Configuration guidelines</td>
<td>52</td>
</tr>
<tr>
<td>Configuring user role authentication</td>
<td>53</td>
</tr>
<tr>
<td>Obtaining temporary user role authorization</td>
<td>54</td>
</tr>
<tr>
<td>Displaying and maintaining RBAC settings</td>
<td>54</td>
</tr>
<tr>
<td>RBAC configuration examples</td>
<td>54</td>
</tr>
<tr>
<td>RBAC configuration example for local AAA authentication users</td>
<td>54</td>
</tr>
<tr>
<td>RBAC configuration example for RADIUS authentication users</td>
<td>54</td>
</tr>
<tr>
<td>RBAC temporary user role authorization configuration example (HWTAACS authentication)</td>
<td>56</td>
</tr>
<tr>
<td>RBAC temporary user role authorization configuration example (RADIUS authentication)</td>
<td>59</td>
</tr>
<tr>
<td>Troubleshooting RBAC</td>
<td>66</td>
</tr>
<tr>
<td>Local users have more access permissions than intended</td>
<td>66</td>
</tr>
<tr>
<td>Login attempts by RADIUS users always fail</td>
<td>66</td>
</tr>
<tr>
<td>Configuring FTP</td>
<td>68</td>
</tr>
<tr>
<td>FIPS compliance</td>
<td>68</td>
</tr>
<tr>
<td>Using the device as an FTP server</td>
<td>68</td>
</tr>
<tr>
<td>Configuring basic parameters</td>
<td>68</td>
</tr>
<tr>
<td>Configuring authentication and authorization</td>
<td>69</td>
</tr>
<tr>
<td>Manually releasing FTP connections</td>
<td>70</td>
</tr>
<tr>
<td>Displaying and maintaining the FTP server</td>
<td>70</td>
</tr>
<tr>
<td>FTP server configuration example</td>
<td>70</td>
</tr>
<tr>
<td>Using the device as an FTP client</td>
<td>71</td>
</tr>
<tr>
<td>Establishing an FTP connection</td>
<td>71</td>
</tr>
<tr>
<td>Managing directories on the FTP server</td>
<td>73</td>
</tr>
<tr>
<td>Working with files on the FTP server</td>
<td>73</td>
</tr>
<tr>
<td>Changing to another user account</td>
<td>74</td>
</tr>
<tr>
<td>Maintaining and troubleshooting the FTP connection</td>
<td>74</td>
</tr>
<tr>
<td>Terminating the FTP connection</td>
<td>75</td>
</tr>
<tr>
<td>Displaying command help information</td>
<td>75</td>
</tr>
<tr>
<td>Displaying and maintaining FTP client</td>
<td>75</td>
</tr>
<tr>
<td>FTP client configuration example</td>
<td>75</td>
</tr>
</tbody>
</table>
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

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 and some functions, such as the daylight saving time, banners, and hotkeys.
• Enter different function views. For example, you can perform the following tasks:
  o Enter interface view to configure interface parameters.
  o Enter VLAN view to add ports to the VLAN.
  o 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**

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>

**Returning to the upper-level view from any view**

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Return to the upper-level view from any view.</td>
<td>quit</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Return directly to user view.</td>
<td>return</td>
</tr>
</tbody>
</table>

**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 keywords and arguments at the position.

  o 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

<table>
<thead>
<tr>
<th>Keys</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common keys</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Keys and Function

<table>
<thead>
<tr>
<th>Keys</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>characters.</td>
<td>Unless the buffer is full, all common characters that you enter before pressing Enter are saved in the edit buffer.</td>
</tr>
<tr>
<td>Backspace</td>
<td>Deletes the character to the left of the cursor and moves the cursor back one character.</td>
</tr>
<tr>
<td>Left arrow key (←)</td>
<td>Moves the cursor one character to the left.</td>
</tr>
<tr>
<td>Right arrow key (→)</td>
<td>Moves the cursor one character to the right.</td>
</tr>
<tr>
<td>Up arrow key (↑)</td>
<td>Displays the previous command in the command history buffer.</td>
</tr>
<tr>
<td>Down arrow key (↓)</td>
<td>Displays the next command in the command history buffer.</td>
</tr>
<tr>
<td>Tab</td>
<td>If you press Tab after entering part of a keyword, the system automatically completes the keyword.</td>
</tr>
<tr>
<td></td>
<td>• If a unique match is found, the system displays the complete keyword.</td>
</tr>
<tr>
<td></td>
<td>• If there is more than one match, press Tab multiple times to pick the keyword you want to enter.</td>
</tr>
<tr>
<td></td>
<td>• If there is no match, the system does not modify what you entered but displays it again in the next line.</td>
</tr>
</tbody>
</table>

### Entering a text or string type value for an argument

A text type argument value can contain printable characters except 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable the command keyword alias function.</td>
<td>command-alias enable</td>
</tr>
<tr>
<td>3.</td>
<td>Configure a command keyword alias.</td>
<td>command-alias mapping cmdkey alias</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Display command keyword alias information.</td>
<td>display command-alias</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2. | 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

<table>
<thead>
<tr>
<th>Hotkey</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl+A</td>
<td>Moves the cursor to the beginning of a line.</td>
</tr>
<tr>
<td>Ctrl+B</td>
<td>Moves the cursor one character to the left.</td>
</tr>
<tr>
<td>Ctrl+C</td>
<td>Stops the current command.</td>
</tr>
<tr>
<td>Ctrl+D</td>
<td>Deletes the character at the cursor.</td>
</tr>
<tr>
<td>Ctrl+E</td>
<td>Moves the cursor to the end of a line.</td>
</tr>
<tr>
<td>Ctrl+F</td>
<td>Moves the cursor one character to the right.</td>
</tr>
<tr>
<td>Ctrl+H</td>
<td>Deletes the character to the left of the cursor.</td>
</tr>
<tr>
<td>Ctrl+K</td>
<td>Aborts the connection request.</td>
</tr>
<tr>
<td>Ctrl+R</td>
<td>Redisplays the current line.</td>
</tr>
<tr>
<td>Ctrl+V</td>
<td>Pastes text from the clipboard.</td>
</tr>
<tr>
<td>Ctrl+W</td>
<td>Deletes the word to the left of the cursor.</td>
</tr>
<tr>
<td>Ctrl+X</td>
<td>Deletes all characters to the left of the cursor.</td>
</tr>
<tr>
<td>Ctrl+Y</td>
<td>Deletes all characters from the cursor to the end of the line.</td>
</tr>
<tr>
<td>Ctrl+Z</td>
<td>Returns to user view.</td>
</tr>
<tr>
<td>Ctrl+]</td>
<td>Terminates the current connection.</td>
</tr>
<tr>
<td>Esc+B</td>
<td>Moves the cursor back one word.</td>
</tr>
<tr>
<td>Esc+D</td>
<td>Deletes all characters from the cursor to the end of the word.</td>
</tr>
<tr>
<td>Esc+F</td>
<td>Moves the cursor forward one word.</td>
</tr>
</tbody>
</table>

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 redisplays your input after finishing the output. You can then continue entering the command line.

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

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

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

<table>
<thead>
<tr>
<th>Error message</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>% Unrecognized command found at ‘^’ position.</td>
<td>The keyword in the marked position is invalid.</td>
</tr>
<tr>
<td>% Incomplete command found at ‘^’ position.</td>
<td>One or more required keywords or arguments are missing.</td>
</tr>
<tr>
<td>% Ambiguous command found at ‘^’ position.</td>
<td>The entered character sequence matches more than one command.</td>
</tr>
<tr>
<td>% Too many parameters.</td>
<td>The entered character sequence contains excessive keywords or arguments.</td>
</tr>
<tr>
<td>% Wrong parameter found at ‘^’ position.</td>
<td>The argument in the marked position is invalid.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Item</th>
<th>Command history buffer for a user line</th>
<th>Command history buffer for all user lines</th>
</tr>
</thead>
<tbody>
<tr>
<td>What kind of commands are saved in the buffer?</td>
<td>Commands successfully executed by the current user of the user line.</td>
<td>Commands successfully executed by all login users.</td>
</tr>
<tr>
<td>Cleared when the user logs out?</td>
<td>Yes.</td>
<td>No.</td>
</tr>
<tr>
<td>How to view buffered commands?</td>
<td>Use the display history-command command.</td>
<td>Use the display history-command all command.</td>
</tr>
<tr>
<td>How to recall buffered commands?</td>
<td>1. Navigate to the command in the buffer: o In Windows 200x or Windows XP HyperTerminal or Telnet, use the up or down arrow key (↑ or ↓). o In Windows 9x HyperTerminal, use Ctrl+P and Ctrl+N. 2. Press Enter.</td>
<td>You cannot call buffered commands.</td>
</tr>
<tr>
<td>How to set the buffer size?</td>
<td>Use the <strong>history-command max-size size-value</strong> command in user line view to set the buffer size. By default, the buffer can store up to 10 commands.</td>
<td>You cannot set the buffer size. By default, the buffer can store up to 1024 commands.</td>
</tr>
<tr>
<td>How to disable the buffer?</td>
<td>Setting the buffer size to 0 disables the buffer.</td>
<td>You cannot disable the buffer.</td>
</tr>
</tbody>
</table>

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

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

Disabling pausing between screens of output

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable pausing between screens of output</td>
<td>screen-length</td>
<td>By default, a session uses the screen-length screen-length command settings in user line view. This command is a one-time command and takes effect only for the current session.</td>
</tr>
<tr>
<td>for the current session.</td>
<td>disable</td>
<td></td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number each output line from a display command.</td>
<td>display command</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Characters</th>
<th>Meaning</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>^</td>
<td>Matches the beginning of a line.</td>
<td>&quot;^u&quot; matches all lines beginning with &quot;u&quot;. A line beginning with &quot;Au&quot; is not matched.</td>
</tr>
<tr>
<td>$</td>
<td>Matches the end of a line.</td>
<td>&quot;u$&quot; matches all lines ending with &quot;u&quot;. A line ending with &quot;uA&quot; is not matched.</td>
</tr>
<tr>
<td>. (period)</td>
<td>Matches any single character.</td>
<td>&quot;.s&quot; matches &quot;as&quot; and &quot;bs&quot;.</td>
</tr>
<tr>
<td>*</td>
<td>Matches the preceding character or string zero, one, or multiple times.</td>
<td>&quot;zo*&quot; matches &quot;z&quot; and &quot;zoo&quot;, and &quot;(zo)*&quot; matches &quot;zo&quot; and &quot;zozo&quot;.</td>
</tr>
<tr>
<td>+</td>
<td>Matches the preceding character or string one or multiple times.</td>
<td>&quot;zo+&quot; matches &quot;zo&quot; and &quot;zoo&quot;, but not &quot;z&quot;.</td>
</tr>
<tr>
<td></td>
<td>Matches the preceding or succeeding string.</td>
<td>&quot;deflnt&quot; matches a string containing &quot;def&quot; or &quot;int&quot;.</td>
</tr>
<tr>
<td>( )</td>
<td>Matches the string in the parentheses, usually used together with the plus sign (+) or asterisk sign (*).</td>
<td>&quot;(123A)&quot; matches &quot;123A&quot;. &quot;408(12)+&quot; matches &quot;40812&quot; and &quot;408121212&quot;, but not &quot;408&quot;.</td>
</tr>
<tr>
<td>\N</td>
<td>Matches the preceding strings in parentheses, with the Nth string repeated once.</td>
<td>&quot;(string)\1&quot; matches a string containing &quot;stringstring&quot;. &quot;(string1)(string2)\2&quot; matches a string containing &quot;string1string2string1string2&quot;. &quot;(string1)(string2)\1\2&quot; matches a string</td>
</tr>
<tr>
<td>Characters</td>
<td>Meaning</td>
<td>Examples</td>
</tr>
<tr>
<td>------------</td>
<td>---------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| [ ] | Matches a single character in the brackets. | "[16A]" matches a string containing 1, 6, or A; 
"[1-36A]" matches a string containing 1, 2, 3, 6, or A (- is a hyphen). 
To match the character ",", put it immediately after ",", for example, [jabc]. There is no such limit on ",". |
| [^] | Matches a single character that is not in the brackets. | "[^16A]" 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). |
| {n} | Matches the preceding character n times. The number n must be a nonnegative integer. | "o{2}" matches "food", but not "Bob". |
| {n,} | Matches the preceding character n times or more. The number n must be a nonnegative integer. | "o{2,}" matches "fooooood", but not "Bob". |
| {n,m} | Matches the preceding character n to m times or more. The numbers n and m must be nonnegative integers and n cannot be greater than m. | "o{1,3}" matches "fod", "food", and "fooooood", 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 contains the pattern but does not start or end with the pattern. | "er\b" matches "never", but not "verb" or "erase". 
"iber" matches "erase", but not "verb" or "never". |
| \B | Matches a word that starts with the pattern following \b or ends with the pattern preceding \b. | "er\B" matches "verb", but not "never" or "erase". |
| \w | Same as [A-Za-z0-9_], matches a digit, letter, or underscore. | "\w" matches "vian" 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 | exclude Direct for the display ip routing-table command to filter out direct routes and display only the non-direct routes.
<Sysname> display ip routing-table | exclude Direct

Destinations : 12       Routes : 12

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
2.2.2.0/24          RIP    10   2            1.1.2.2         Vlan 2

# 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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save the output from a display command to a separate file.</td>
<td>display command &gt; filename</td>
</tr>
</tbody>
</table>
Append the output from a display command to the end of a file.

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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>View and manage the output from a display command effectively.</td>
<td>`display command [ [ [ by-linenum ] [ begin</td>
</tr>
</tbody>
</table>

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

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

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 <HPE> 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.
<HPE>%Sep 24 09:48:54:109 2014 HPE SHELL/4/LOGIN: Console login from aux0
<HPE>
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>
<thead>
<tr>
<th>Table 7 CLI login method and user line matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>User line</td>
</tr>
<tr>
<td>AUX line</td>
</tr>
<tr>
<td>Virtual type terminal (VTY) line</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Authentication mode</th>
<th>Configuration tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Set the authentication mode to <strong>none</strong>.</td>
</tr>
</tbody>
</table>
| 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 *Security Configuration Guide*. |

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 feature 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:

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| 2. Enter AUX line view or class view. | • Enter AUX line view: line aux first-number [ last-number ]  
• 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. |
Step | Command | Remarks
--- | --- | ---
4. | Assign a user role. | 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2. | Enter AUX line view or class view. | • Enter AUX line view: line aux first-number [last-number]  
• 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} password | By default, no password is set. |
| 5. | Assign a user role. | user-role role-name | 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2. | Enter AUX line view or class view. | • Enter AUX line view: line aux first-number [last-number]  
• 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. |
Step | Command | Remarks
--- | --- | ---
3. | Enable scheme authentication. | 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter AUX line view or class view.</td>
<td>line aux first-number [last-number]</td>
</tr>
<tr>
<td>3.</td>
<td>Set the baud rate.</td>
<td>speed speed-value</td>
</tr>
<tr>
<td>4.</td>
<td>Specify the parity check mode.</td>
<td>parity { even</td>
</tr>
<tr>
<td>5.</td>
<td>Specify the number of stop bits.</td>
<td>stopbits { 1</td>
</tr>
</tbody>
</table>
Step | Command | Remarks
--- | --- | ---
6. Specify the number of data bits for each character. | `databits { 5 | 6 | 7 | 8 }` | The default is 8. Configure this command depending on 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 character` | By default, pressing Enter starts the terminal session.
8. Define a shortcut key for terminating tasks. | `escape-key { character | 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.
10. Specify the terminal display type. | `terminal type { ansi | vt100 }` | By default, the terminal display type is ANSI. The device supports ANSI and VT100 terminal display types. As a best practice, 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 screen-length` | 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 value` | By default, the buffer saves up to 10 history commands.
13. Set the CLI connection idle-timeout timer. | `idle-timeout minutes [ seconds ]` | By default, the CLI connection idle-timeout timer is 10 minutes. If no interaction occurs between the device and the user within the idle-timeout interval, the system automatically terminates the user connection on the user line. If you set the timeout timer to 0, the connection 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

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Configuring login authentication:</td>
<td></td>
</tr>
<tr>
<td>• Disabling authentication for Telnet login</td>
<td></td>
</tr>
<tr>
<td>• Configuring password authentication for Telnet login</td>
<td></td>
</tr>
<tr>
<td>• Configuring scheme authentication for Telnet login</td>
<td>Configure one authentication mode as required.</td>
</tr>
<tr>
<td>(Optional.) Setting the maximum number of concurrent Telnet users</td>
<td>N/A</td>
</tr>
<tr>
<td>(Optional.) Setting the DSCP value for outgoing Telnet packets</td>
<td>N/A</td>
</tr>
<tr>
<td>(Optional.) Configuring common VTY line settings</td>
<td>N/A</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enable Telnet server.</td>
<td>telnet server enable</td>
<td>By default, the Telnet server feature is disabled.</td>
</tr>
</tbody>
</table>
| 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. 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 role-name | 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) 2010-2016 Hewlett Packard Enterprise Development LP
*** Without the owner's prior written consent,
*** no decompiling or reverse-engineering shall be allowed.
```

---

### Configuring password authentication for Telnet login

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable Telnet server.</td>
<td>telnet server enable</td>
</tr>
<tr>
<td>3.</td>
<td>Enter VTY line view or class view.</td>
<td>line vty first-number [ last-number ]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>line class vty</td>
</tr>
<tr>
<td>4.</td>
<td>Enable password authentication.</td>
<td>authentication-mode password</td>
</tr>
<tr>
<td>5.</td>
<td>Set a password.</td>
<td>set authentication password { hash</td>
</tr>
<tr>
<td>6.</td>
<td>(Optional.) Assign a user role.</td>
<td>user-role role-name</td>
</tr>
</tbody>
</table>

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.
Configuring scheme authentication for Telnet login

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable Telnet server.</td>
<td>telnet server enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, the Telnet server feature is disabled.</td>
</tr>
<tr>
<td>3.</td>
<td>Enter VTY line view or</td>
<td>• Enter VTY line view: line vty first-number [ last-number ]</td>
</tr>
<tr>
<td></td>
<td>class view.</td>
<td>• Enter VTY line class view: line class vty</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A non-default setting in either view takes precedence over a default setting in the other view.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A non-default setting in user line view takes precedence over a non-default setting in user line class view.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>4.</td>
<td>Enable scheme authentication.</td>
<td>authentication-mode scheme</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, password authentication is enabled for VTY lines.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

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) 2010–2016 Hewlett Packard Enterprise Development LP
* Without the owner's prior written consent,
* no decompiling or reverse-engineering shall be allowed.

---

Login authentication

Username:admin
Password: 

Username:admin
Password: 

Setting the maximum number of concurrent Telnet users

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the maximum number of concurrent Telnet users.</td>
<td>aaa session-limit telnet max-sessions</td>
</tr>
</tbody>
</table>

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 Security Command Reference.

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set the DSCP value for outgoing Telnet packets.</td>
<td>For a Telnet server running IPv4: telnet server dscp dscp-value For a Telnet server running IPv6: telnet server ipv6 dscp dscp-value</td>
</tr>
</tbody>
</table>

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, the system automatically disconnects the Telnet session. Before you configure this feature 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:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter VTY line view or class view.</td>
<td>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.</td>
</tr>
<tr>
<td>3.</td>
<td>Enable the terminal service.</td>
<td>By default, terminal service is enabled.</td>
</tr>
<tr>
<td>4.</td>
<td>Specify the protocols for the user lines to support.</td>
<td>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 <strong>authentication-mode</strong> 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.</td>
</tr>
<tr>
<td>5.</td>
<td>Define a shortcut key for terminating tasks.</td>
<td>By default, pressing <code>Ctrl+C</code> terminates a task.</td>
</tr>
<tr>
<td>6.</td>
<td>Specify the terminal display type.</td>
<td>By default, the terminal display type is ANSI.</td>
</tr>
<tr>
<td>7.</td>
<td>Set the maximum number of lines to be displayed on a screen.</td>
<td>By default, up to 24 lines is displayed on a screen. A value of 0 disables the feature.</td>
</tr>
<tr>
<td>8.</td>
<td>Set the size of command history buffer.</td>
<td>By default, the buffer saves 10 history commands.</td>
</tr>
<tr>
<td>9.</td>
<td>Set the CLI connection idle-timeout timer.</td>
<td>By default, the CLI connection idle-timeout timer is 10 minutes. If no interaction occurs between the device and the user within the idle-timeout interval, the system automatically terminates the user connection on the user line. If you set the timeout timer to 0, the connection will not be aged out.</td>
</tr>
<tr>
<td>10.</td>
<td>Specify a command to be automatically executed when users log in to the user lines.</td>
<td>By default, no automatically executed command is specified.</td>
</tr>
</tbody>
</table>
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

![Diagram](image)

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>(Optional.) Specify the source IPv4 address or source interface for outgoing Telnet packets.</td>
<td>telnet client source { interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Exit to user view.</td>
<td>quit</td>
</tr>
</tbody>
</table>
| 4.   | Use the device to log in to a Telnet server. | • Log in to an IPv4 Telnet server: telnet remote-host [ service-port ] [ vpn-instance vpn-instance-name ] [ source { interface interface-type interface-number | ip ip-address } ] [ dscp dscp-value ]  
   • Log in to an IPv6 Telnet server: telnet ipv6 remote-host [ -i interface-type interface-number ] [ port-number ] [ vpn-instance vpn-instance-name ] [ dscp dscp-value ] | 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><strong>system-view</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Create local key pairs.</td>
<td>**public-key local create { dsa</td>
</tr>
<tr>
<td>3.</td>
<td>Enable SSH server.</td>
<td><strong>ssh server enable</strong></td>
</tr>
</tbody>
</table>
| 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. |
| 5.   | 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. |
| 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... |
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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log in to an IPv4 SSH server.</td>
<td>ssh2 server</td>
</tr>
<tr>
<td>Log in to an IPv6 SSH server.</td>
<td>ssh2 ipv6 server</td>
</tr>
</tbody>
</table>

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.
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 13 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**
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 <HPE> appears. If the authentication mode is password or scheme, you must enter the correct authentication information as prompted.

**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, enter **AT+ + +**. 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.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display online CLI user information.</td>
<td><code>display users [ all ]</code></td>
<td>N/A</td>
</tr>
<tr>
<td>Display user line information.</td>
<td>`display line [ num1</td>
<td>{ aux</td>
</tr>
<tr>
<td>Display the source address or interface for outgoing Telnet packets when the device acts as a Telnet client.</td>
<td><code>display telnet client</code></td>
<td>N/A</td>
</tr>
<tr>
<td>Release a user line.</td>
<td>`free line { num1</td>
<td>{ aux</td>
</tr>
<tr>
<td>Lock the current user line.</td>
<td><code>lock</code></td>
<td>By default, the system does not lock any user lines. This command is not supported in FIPS mode.</td>
</tr>
<tr>
<td>Send messages to user lines.</td>
<td>`send { all</td>
<td>num1</td>
</tr>
</tbody>
</table>
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 14 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Apply an ACL to filter Telnet logins. | - telnet server acl acl-number  
- telnet server ipv6 acl [ ipv6 ] acl-number | By default, no ACL is used to filter Telnet logins. |

To control SSH logins:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Apply an ACL to filter SSH logins. | - ssh server acl acl-number  
- ssh server ipv6 acl [ ipv6 ] acl-number | By default, no ACL is used to filter SSH logins.  
For more information about these two commands, see Security Command Reference. |

Configuration example

Network requirements

As shown in Figure 15, the device is a Telnet server.
Configure the device to permit only Telnet packets sourced from Host A and Host B.

Figure 15 Network diagram

```
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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the SNMP access right.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• (Method 1.) Create an SNMP community and specify ACLs for the community:</td>
<td>For more information about SNMP, see Network Management and Monitoring Configuration Guide.</td>
</tr>
<tr>
<td></td>
<td>o In VACM mode:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>snmp-agent community { read</td>
<td>write } [ simple</td>
</tr>
<tr>
<td></td>
<td>o In RBAC mode:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>snmp-agent community [ simple</td>
<td>cipher ]</td>
</tr>
<tr>
<td></td>
<td>community-name user-role role-name [ acl acl-number</td>
<td>acl ipv6 ipv6-acl-number ] *</td>
</tr>
<tr>
<td></td>
<td>• (Method 2.) Create an SNMPv1/v2c group and add a user to the group, specifying ACLs for the group and user:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. snmp-agent group { v1</td>
<td>v2c } group-name</td>
</tr>
</tbody>
</table>
To control SNMPv3 access, configure ACLs and perform the following tasks:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create an SNMPv3 group, specifying ACLs for the group.</td>
<td>snmp-agent group v3 group-name [ authentication</td>
</tr>
<tr>
<td>3.</td>
<td>Create an SNMPv3 user, specifying ACLs for the user.</td>
<td>snmp-agent usm-user v3 user-name group-name [ remote { ip-address</td>
</tr>
</tbody>
</table>

**Configuration example**

**Network requirements**

As shown in Figure 16, the device is running SNMP.

Configure the device to allow Host A and Host B to access the device through SNMP.
Figure 16 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 feature 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 feature 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Enter user line view or user line class view. | • Enter user line view: line { first-number1 [ last-number1 ] | { aux | vty } first-number2 [ last-number2 ] }  
• Enter user line class view: | 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 |
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>line class { aux</td>
<td>vty }</td>
</tr>
<tr>
<td>3.</td>
<td>authentication-mode scheme</td>
<td>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.</td>
</tr>
<tr>
<td>4.</td>
<td>command authorization</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Configuration example**

**Network requirements**

As shown in Figure 17, 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 17 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 user names 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 feature 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 feature 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:

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Enter user line view or user line class view.</td>
<td>• Enter user line view: line { first-number1 [ last-number1 ] } { aux</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Enable scheme authentication.</td>
<td>authentication-mode scheme</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>Enable command accounting.</td>
<td>command accounting</td>
</tr>
</tbody>
</table>

Configuration example

Network requirements

As shown in Figure 18, 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.
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, VLANs, and VPN instances.

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 static, in contrast to users, separating permissions from users enables simple 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, VLANs, and VPNs are accessible to the user role. (See "Resource access policies.")

To use a command related to a resource (an interface, VLAN, or VPN), 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.
- **VPN instance policy**—Controls access to VPNs.

Resource access policies do not control access to the interface, VLAN, or VPN options in the display commands. You can specify these options in the display commands if 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, VLANs, and VPNs). 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

<table>
<thead>
<tr>
<th>User role name</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>network-admin</td>
<td>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.</td>
</tr>
<tr>
<td>network-operator</td>
<td></td>
</tr>
<tr>
<td>level-n (n = 0 to 15)</td>
<td></td>
</tr>
<tr>
<td>level-0</td>
<td>Has access to diagnostic commands, including ping, quit, ssh2, super, system-view, telnet, and tracert. Level-0 access rights are configurable.</td>
</tr>
<tr>
<td>level-1</td>
<td>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.</td>
</tr>
<tr>
<td>level-2 to level-8, and level-10 to level-14</td>
<td>Have no access rights by default. Access rights are configurable.</td>
</tr>
<tr>
<td>level-9</td>
<td>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</td>
</tr>
<tr>
<td>User role name</td>
<td>Permissions</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>user account. Level-9 access rights are configurable.</td>
</tr>
<tr>
<td></td>
<td>o RBAC non-debugging commands.</td>
</tr>
<tr>
<td></td>
<td>o Local users.</td>
</tr>
<tr>
<td></td>
<td>o File management.</td>
</tr>
<tr>
<td></td>
<td>o Device management.</td>
</tr>
<tr>
<td></td>
<td>o The <strong>display history-command all</strong> command.</td>
</tr>
<tr>
<td></td>
<td>• <strong>level-15</strong>—Has the same rights as network-admin.</td>
</tr>
<tr>
<td>security-audit</td>
<td>Security log manager. The user role has the following access to security log files:</td>
</tr>
<tr>
<td></td>
<td>• Accesses to the commands for displaying and maintaining security log files (for example, the <code>dir</code>, <code>display security-logfile summary</code>, and <code>more</code> commands).</td>
</tr>
<tr>
<td></td>
<td>• Accesses to the commands for managing security log files and security log file system (for example, the <code>info-center security-logfile directory</code>, <code>mkdir</code>, and <code>security-logfile save</code> commands).</td>
</tr>
<tr>
<td></td>
<td>For more information about security log management, see <em>Network Management and Monitoring Configuration Guide</em>. For more information about file system management, see &quot;Managing the file system.&quot;</td>
</tr>
<tr>
<td></td>
<td><strong>IMPORTANT:</strong></td>
</tr>
<tr>
<td></td>
<td>Only the security-audit user role has access to security log files.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Creating user roles</td>
</tr>
<tr>
<td>(Required.) Configuring user role rules</td>
</tr>
<tr>
<td>(Optional.) Configuring feature groups</td>
</tr>
<tr>
<td>(Optional.) Configuring resource access policies</td>
</tr>
<tr>
<td>(Optional.) Assigning user roles</td>
</tr>
<tr>
<td>(Optional.) Configuring temporary user role authorization</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a user role and enter user role view.</td>
<td>role name role-name</td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Configure a description for the user role.</td>
<td>description text</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter user role view.</td>
<td>role name role-name</td>
</tr>
</tbody>
</table>
| 3.   | Configure a rule. | • Configure a command rule: `rule number { deny | permit } command command-string`
  • Configure a feature rule: `rule number { deny | permit } { execute | read | write } * feature [ feature-name ]`
  • Configure a feature group rule: `rule number { deny | permit } { execute | read | write } * feature-group feature-group-name` | 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 |
### 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Create a feature group and enter feature group view. | role feature-group name feature-group-name | 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 feature-name | 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, VLAN policy, and VPN instance policy. By default, these policies permit user roles to access any interface, VLAN, and VPN. You can configure the policies of a user-defined user role or a predefined level-n user role to limit its access to interfaces, VLANs, and VPNs. 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter user role view.</td>
<td>role name role-name</td>
</tr>
<tr>
<td>3.</td>
<td>Enter user role interface policy view.</td>
<td>interface policy deny</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Specify a list of interfaces accessible to the user role.</td>
<td><strong>permit interface interface-list</strong>&lt;br&gt;By default, no accessible interfaces are configured in user role interface policy view. Repeat this step to add more accessible interfaces.</td>
</tr>
</tbody>
</table>

**Configuring the VLAN policy of a user role**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><strong>system-view</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Enter user role view.</td>
<td><strong>role name role-name</strong></td>
</tr>
<tr>
<td>3.</td>
<td>Enter user role VLAN policy view.</td>
<td><strong>vlan policy deny</strong>&lt;br&gt;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 <strong>permit vlan</strong> command is not configured.</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Specify a list of VLANs accessible to the user role.</td>
<td><strong>permit vlan vlan-id-list</strong>&lt;br&gt;By default, no accessible VLANs are configured in user role VLAN policy view. Repeat this step to add more accessible VLANs.</td>
</tr>
</tbody>
</table>

**Configuring the VPN instance policy of a user role**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><strong>system-view</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Enter user role view.</td>
<td><strong>role name role-name</strong></td>
</tr>
<tr>
<td>3.</td>
<td>Enter user role VPN instance policy view.</td>
<td><strong>vpn-instance policy deny</strong>&lt;br&gt;By default, the VPN instance policy of the user role permits access to all VPNs. This command denies the access of the user role to all VPNs if the <strong>permit vpn-instance</strong> command is not configured.</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Specify a list of VPNs accessible to the user role.</td>
<td><strong>permit vpn-instance vpn-instance-name&amp;&lt;1-10&gt;</strong>&lt;br&gt;By default, no accessible VPNs are configured in user role VPN instance policy view. Repeat this step to add more accessible VPNs.</td>
</tr>
</tbody>
</table>
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 assigns the default user role to AAA-authenticated users if the authentication server (local or remote) does not assign any user roles to the users. These users are allowed to access the system with the default user role.

You can specify any user role existing in the system as the default user role.

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable the default user role feature.</td>
<td>role default-role enable [ role-name ]</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Create a local user and enter local user view.</td>
<td>N/A</td>
</tr>
<tr>
<td>3.</td>
<td>Authorize the user to have a user role.</td>
<td>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.</td>
</tr>
<tr>
<td>4.</td>
<td>(Optional.) Remove undesirable user roles.</td>
<td>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.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Enter user line view or use line class view.</td>
<td>For information about the priority order and application scope of the configurations in user line view and user line class view, see &quot;Logging into the CLI.&quot;</td>
</tr>
<tr>
<td>3.</td>
<td>Specify a user role on the user line.</td>
<td>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</td>
</tr>
</tbody>
</table>
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 **$enab\$\$ 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 **$enab\$\$ 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**

<table>
<thead>
<tr>
<th>Keywords</th>
<th>Authentication mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>Local password authentication only (local-only)</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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 Security Configuration Guide.  
  - Add the user account and password on the HWTACACS or RADIUS server. |
| local    | 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. |
| scheme   | 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>`super authentication-mode { local</td>
<td>scheme } *`</td>
</tr>
<tr>
<td>3.</td>
<td><code>super default role rolename</code></td>
<td>By default, the default target user role is network-admin.</td>
</tr>
</tbody>
</table>
### 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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain the temporary authorization to use a user role.</td>
<td><code>super [ rolename ]</code></td>
<td>If you do not specify the <code>rolename</code> 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 <code>super</code> command to obtain temporary user role authorization.</td>
</tr>
</tbody>
</table>

### Displaying and maintaining RBAC settings

Execute `display` commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display user role information.</td>
<td><code>display role [ name role-name ]</code></td>
</tr>
<tr>
<td>Display user role feature information.</td>
<td>`display role feature [ name feature-name</td>
</tr>
<tr>
<td>Display user role feature group information.</td>
<td><code>display role feature-group [ name feature-group-name ] [ verbose ]</code></td>
</tr>
</tbody>
</table>

### RBAC configuration examples

#### RBAC configuration example for local AAA authentication users

**Network requirements**

As shown in Figure 19, 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.
Figure 19 Network diagram

Configuration procedure

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

```bash
<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.

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

# Enable scheme authentication on the user lines for Telnet users.

```bash
[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.

```bash
[Switch] domain bbb
[Switch-isp-bbb] authentication login local
[Switch-isp-bbb] authorization login local
[Switch-isp-bbb] quit
```

# Create the user role role1.

```bash
[Switch] role name role1
```

# Configure rule 1 to permit the user role to access read commands of all features.

```bash
[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.

```bash
[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.

```bash
[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.

```bash
[Switch] local-user user1 class manage
New local user added.
```

# Set a plaintext password aabbcc for the user.

```bash
[Switch-luser-manage-user1] password simple aabbcc
```

# Set the service type to Telnet.

```bash
[Switch-luser-manage-user1] service-type telnet
```

# Assign role1 to the user.

```bash
[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`.

```shell
[Switch-user-manage-user1] undo authorization-attribute user-role network-operator
```

[Switch-user-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.

```shell
<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.

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

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

```shell
[Switch] display clock
09:31:56 UTC Tues 01/01/2013
```

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

```shell
<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 20, 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.
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.

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

---

**IMPORTANT:**

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

```bash
[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.

```bash
[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.

```bash
[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 21, 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 21 Network diagram**

1. **Configuration procedure**

   1. Configure the switch:

      ```bash
      # 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 hwtacac-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.
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 22 Configuring advanced TACACS+ settings

   ![Advanced TACACS+ Settings](image)

   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.
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.
   
   ```bash
   <Switch> telnet 192.168.1.70
   Trying 192.168.1.70 ...
   Press CTRL+K to abort
   Connected to 192.168.1.59 ...
   `*
   * Copyright (c) 2010-2015 Hewlett Packard Enterprise Development LP
   * 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 24, 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 24 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 25.

   Figure 25 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) 2010-2015 Hewlett Packard Enterprise Development LP *
      * 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
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 Hewlett Packard Enterprise 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 Hewlett Packard Enterprise 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 .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 26 FTP application scenario](image)

FIPS compliance

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable the FTP server.</td>
<td>ftp server enable</td>
</tr>
<tr>
<td>3.</td>
<td>(Optional.) Use an ACL to control access to the FTP</td>
<td>ftp server acl { acl-number</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>4. (Optional.) Associate an SSL server policy with the FTP server to ensure data security.</td>
<td><strong>ftp server ssl-server-policy policy-name</strong></td>
<td>By default, no SSL server policy is associated with the FTP server.</td>
</tr>
<tr>
<td>5. (Optional.) Set the FTP connection idle-timeout timer.</td>
<td><strong>ftp timeout minutes</strong></td>
<td>By default, the FTP connection idle-timeout timer is 30 minutes. If no data transfer occurs on an FTP connection within the idle-timeout interval, the FTP server closes the FTP connection to release resources.</td>
</tr>
</tbody>
</table>
| 6. (Optional.) Set the DSCP value for outgoing FTP packets. | • For an FTP server running IPv4: **ftp server dscp dscp-value**  
• For an FTP server running IPv6: **ftp server ipv6 dscp dscp-value** | By default, the DSCP value is 0. |
| 7. (Optional.) Set the maximum number of concurrent FTP users. | **aaa session-limit ftp max-sessions** | 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 Security Command Reference. |

### 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

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
</table>
| Manually release FTP connections. | • Release the FTP connection established using a specific user account: `free ftp user username`
| | • Release the FTP connection to a specific IP address: `free ftp user-ip [ipv6] client-address [port port-num]` |

Displaying and maintaining the FTP server

Execute `display` commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display FTP server configuration and status information.</td>
<td><code>display ftp-server</code></td>
</tr>
<tr>
<td>Display detailed information about online FTP users.</td>
<td><code>display ftp-user</code></td>
</tr>
</tbody>
</table>

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 27 Network diagram**

```
IRF (FTP server)
IP: 1.1.1.1/16
Master (Member_ID=1)
Subordinate (Member_ID=2)

FTP client
1.2.1.1/16

Note: The orange line represents an IRF connection.
```

**Configuration procedure**

1. Configure IP addresses as shown in Figure 27. 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:
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>(Optional.) Specify a source IP address for outgoing FTP packets.</td>
<td>ftp client source { interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Return to user view.</td>
<td>quit</td>
</tr>
<tr>
<td>4.</td>
<td>Log in to the FTP server.</td>
<td>• (Method 1.) Log in to the FTP server from user view: ftp ftp-server [ service-port ] [ vpn-instance vpn-instance-name ] [ dscp dscp-value ] [ source { interface interface-name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Method 2.) Log in to the FTP server from FTP client view:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. ftp</td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. open server-address [ service-port ]</td>
</tr>
</tbody>
</table>

To establish an IPv6 FTP connection:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>(Optional.) Specify the source IPv6 address for FTP packets sent by the FTP client.</td>
<td>ftp client ipv6 source { interface interface-type interface-number</td>
</tr>
<tr>
<td>3.</td>
<td>Return to user view.</td>
<td>quit</td>
</tr>
<tr>
<td>4.</td>
<td>Log in to the FTP server.</td>
<td>• (Method 1.) Log in to the FTP server from user view: ftp ipv6 ftp-server [ service-port ] [ vpn-instance vpn-instance-name ] [ dscp dscp-value ] [ source { interface interface-type interface-number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• (Method 2.) Log in to the FTP server from FTP client view:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a. ftp ipv6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>b. open server-address [ service-port ]</td>
</tr>
</tbody>
</table>
Managing directories on the FTP server

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
</table>
| Display directory and file information on the FTP server.           | • Display the detailed information of a directory or file on the FTP server: dir [ remotefile [ localfile ] ]  
|                                                                      | • Display the name of a directory or file on the FTP server: ls [ remotefile [ localfile ] ]                      |
| Change the working directory on the FTP server.                     | cd { directory | .. | / }                                                  |
| Return to the upper level directory on the FTP server.               | cdup                                                                    |
| Display the working directory that is being accessed.               | pwd                                                                    |
| Create a directory on the FTP server.                               | mkdir directory                                                         |
| Remove the specified working directory on the remote FTP server.     | rmdir directory                                                         |

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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display directory or file information on the FTP server.</td>
<td></td>
<td>N/A</td>
</tr>
</tbody>
</table>
|                                                                      | • Display detailed information about a directory or file on the FTP server: dir [ remotefile [ localfile ] ]  
|                                                                      | • Display the name of a directory or file on the FTP server: ls [ remotefile [ localfile ] ]                      |
| Delete the specified file on the FTP server permanently.             | delete remotefile | N/A     |
| Set the file transfer mode.                                          |         | The default file transfer mode is binary. |
|                                                                      | • Set the file transfer mode to ASCII: ascii  
|                                                                      | • Set the file transfer mode to binary: binary |
| Set the FTP operation mode to passive.                              | passive | The default mode is passive. |
### Task Command Remarks

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display or change the local working directory of the FTP client.</td>
<td>`lcd [ directory</td>
<td>/ ]`</td>
</tr>
<tr>
<td>Upload a file to the FTP server.</td>
<td><code>put localfile [ remotefile ]</code></td>
<td>N/A</td>
</tr>
<tr>
<td>Download a file from the FTP server.</td>
<td><code>get remotefile [ localfile ]</code></td>
<td>N/A</td>
</tr>
<tr>
<td>Add the content of a file on the FTP client to a file on the FTP server.</td>
<td><code>append localfile [ remotefile ]</code></td>
<td>N/A</td>
</tr>
<tr>
<td>Specify the retransmit marker.</td>
<td><code>restart marker</code></td>
<td>Use this command together with the <code>put</code>, <code>get</code>, or <code>append</code> command.</td>
</tr>
<tr>
<td>Update the local file.</td>
<td><code>newer remotefile</code></td>
<td>N/A</td>
</tr>
<tr>
<td>Get the missing part of a file.</td>
<td><code>reget remotefile [ localfile ]</code></td>
<td>N/A</td>
</tr>
<tr>
<td>Rename the file.</td>
<td><code>rename [ oldfilename [ newfilename ] ]</code></td>
<td>N/A</td>
</tr>
</tbody>
</table>

### 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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change to another user account.</td>
<td><code>user username [ password ]</code></td>
</tr>
</tbody>
</table>

### Maintaining and troubleshooting the FTP connection

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminate the connection to the FTP server without exiting FTP client view.</td>
<td>disconnect, close</td>
</tr>
<tr>
<td>Terminate the connection to the FTP server and return to user view.</td>
<td>bye, quit</td>
</tr>
</tbody>
</table>

Displaying command help information

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display command help information</td>
<td>help [ command-name ]</td>
</tr>
<tr>
<td></td>
<td>? [ command-name ]</td>
</tr>
</tbody>
</table>

Displaying and maintaining FTP client

Execute the display command in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display source IP address information on the FTP client</td>
<td>display ftp client source</td>
</tr>
</tbody>
</table>

FTP client configuration example

Network requirements

As shown in Figure 28, 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.
Configuration procedure

# Configure IP addresses as shown in Figure 28. 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 29 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>(Optional.) Use an ACL to control the client's access to TFTP servers.</td>
<td>tftp-server acl acl-number</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the source IP address for TFTP packets sent by the TFTP client.</td>
<td>tftp client source { interface interface-type interface-number</td>
</tr>
<tr>
<td>4.</td>
<td>Return to user view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Download or upload a file in an IPv4 network.</td>
<td>tftp tftp-server { get</td>
</tr>
</tbody>
</table>
## Configuring the device as an IPv6 TFTP client

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>(Optional.) Use an ACL to control the client's access to TFTP servers.</td>
<td>tftp-server ipv6 acl acl-number</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the source IPv6 address for TFTP packets sent by the TFTP client.</td>
<td>tftp client ipv6 source { interface interface-type interface-number</td>
</tr>
<tr>
<td>4.</td>
<td>Return to user view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Download or upload a file in an IPv6 network.</td>
<td>tftp ipv6 tftp-server [ -i interface-type interface-number ] { get</td>
</tr>
</tbody>
</table>
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 depends on whether the USB disk is partitioned:
- If the USB disk is not partitioned, its name is usba0:
- If the USB disk is partitioned, 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 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 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

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>file-name</td>
<td>Specifies a file in the current working directory.</td>
<td>a.cfg indicates a file named a.cfg in the current working directory.</td>
</tr>
<tr>
<td>[path]file-name</td>
<td>Specifies a file in a folder in the current working directory.</td>
<td>• test/a.cfg indicates a file named a.cfg in the test folder in the current working directory.</td>
</tr>
<tr>
<td></td>
<td>The path argument represents the path to the file.</td>
<td>• test/subtest/a.cfg indicates a file</td>
</tr>
<tr>
<td>Format</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>---------</td>
</tr>
<tr>
<td>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 (/).</td>
<td>named a.cfg in the subtest subfolder of the test folder in the current working directory.</td>
<td></td>
</tr>
<tr>
<td>drive:@[path]/file-name</td>
<td>Specifies a file in a storage medium on the device. The drive argument represents the storage medium name. Typically, the storage medium name is flash: or usba0:. If the device has only one storage medium, the drive argument is optional.</td>
<td>flash:/test/a.cfg indicates a file named a.cfg in the test folder in the root directory of the flash memory.</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display folder or file information.</td>
<td><code>dir [ /all ] [ file-url ] [ /all-filesystems ]</code></td>
</tr>
</tbody>
</table>

#### Displaying the contents of a text file

Perform this task in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the contents of a text file.</td>
<td><code>more file-url</code></td>
</tr>
</tbody>
</table>
## Renaming a file

Perform this task in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rename a file.</td>
<td><code>rename fileurl-source fileurl-dest</code></td>
</tr>
</tbody>
</table>

## Copying a file

Perform this task in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy a file.</td>
<td>• In non-FIPS mode: <code>copy fileurl-source fileurl-dest</code></td>
</tr>
</tbody>
</table>

## Moving a file

Perform this task in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move a file.</td>
<td><code>move fileurl-source fileurl-dest</code></td>
</tr>
</tbody>
</table>

## Compressing/decompressing a file

Perform the following tasks in user view:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compress a file.</td>
<td><code>gzip filename</code></td>
</tr>
<tr>
<td>Decompress a file.</td>
<td><code>gunzip filename</code></td>
</tr>
</tbody>
</table>

## Archiving/extracting files

Perform the following tasks in user view:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extract files.</td>
<td>`tar extract archive-file fileurl-dest [ verbose ] [ screen</td>
</tr>
<tr>
<td>Display the names of archived files.</td>
<td><code>tar list archive-file fileurl-dest</code></td>
</tr>
</tbody>
</table>
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:

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

**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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete files from the recycle bin.</td>
<td><code>reset recycle-bin</code> [ /force ]</td>
</tr>
</tbody>
</table>

Calculating the file digest

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

Perform this task in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calculate the digest of a file.</td>
<td>• Use the SHA-256 digest algorithm: <code>sha256sum file-url</code></td>
</tr>
<tr>
<td></td>
<td>• Use the MD5 digest algorithm: <code>md5sum file-url</code></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display directory or file information.</td>
<td><code>dir /all [file-url] /all-fileystems</code></td>
</tr>
</tbody>
</table>

Displaying the current working directory

Perform this task in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the current working directory.</td>
<td><code>pwd</code></td>
</tr>
</tbody>
</table>

Changing the current working directory

Perform this task in user view.

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

Creating a directory

Perform this task in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a directory.</td>
<td><code>mkdir directory</code></td>
</tr>
</tbody>
</table>

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.
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.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repair a storage medium.</td>
<td><code>fixdisk medium-name</code></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format a storage medium.</td>
<td><code>format medium-name</code></td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mount a storage medium.</td>
<td><code>mount medium-name</code></td>
<td>By default, a storage medium is automatically mounted and in mounted state when connected to the system.</td>
</tr>
<tr>
<td>Unmount a storage medium.</td>
<td><code>umount medium-name</code></td>
<td>By default, a storage medium is automatically mounted and in mounted state when connected to the system.</td>
</tr>
</tbody>
</table>

**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.

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

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2. Set the operation mode for files and folders.</td>
<td>`file prompt { alert</td>
<td>quiet }`</td>
</tr>
</tbody>
</table>
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 names of 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.

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 30 shows the 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 menus 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 different command views, including system view, interface views, protocol views, and user line views.
- 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$6$Twd73mLrN8O2vvD5Srz1vgdpR4KoT1rQNE9pg33gU14Br2p1VguczLSVvyJLO2huV5Syx/LfD1f8ROLtV
ErJ/C3loq2rFtmNuyZf4STw==
    service-type ssh telnet terminal
    authorization-attribute user-role network-admin
    authorization-attribute user-role network-operator
#
interface Ten-GigabitEthernet1/0/1
    shutdown
    trill enable
#
```

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 HPE devices running Comware 7 software use the same private key or public key to encrypt configuration files.

**NOTE:**

Only HPE devices running Comware 7 software can decrypt the encrypted configuration files.

To enable configuration encryption:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable configuration encryption.</td>
<td>configuration encrypt { private-key</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save the running configuration to a configuration file without specifying the file as a next-startup configuration file.</td>
<td>`save file-url [all</td>
<td>slot slot-number]`</td>
</tr>
<tr>
<td>Save the running configuration to a configuration file and specify the file as a next-startup configuration file.</td>
<td>`save [safely] [backup</td>
<td>main] [force]`</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Configuring configuration archive parameters</td>
</tr>
<tr>
<td>(Required.) Perform either task:</td>
</tr>
<tr>
<td>• Enabling automatic configuration archiving</td>
</tr>
<tr>
<td>• Manually archiving the running configuration</td>
</tr>
<tr>
<td>(Required.) Rolling back configuration</td>
</tr>
</tbody>
</table>

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 make sure the system can archive the running configuration after a master/subordinate switchover, create the directory on all IRF members.

Configuration procedure

To configure configuration archive parameters:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view. system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the directory and file name prefix for archiving the running archive configuration location directory filename-prefix filename-prefix</td>
<td>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.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>archive configuration interval minutes</td>
<td>By default, this function is disabled. To display configuration archive names and their archiving time, use the display archive configuration command.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manually archive the running configuration.</td>
<td>archive configuration</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Roll the running configuration back to the configuration defined by a configuration file.</td>
<td><code>configuration replace file filename</code></td>
</tr>
</tbody>
</table>

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.

Configuring configuration commit delay

This feature allows you to perform the following operations:

1. Use the `configuration commit delay` command to set the allowed delay time for a manual commit to keep the settings configured after the command was executed.
2. Use the `configuration commit` command to commit the settings. If no manual commit is performed within the allowed delay time, the device rolls back the configuration to the settings before the `configuration commit delay` command was executed.

**NOTE:**
Once the rollback begins, the device outputs logs to notify the user of the rollback operation. The user cannot perform other operations before the rollback is finished.

As a best practice, set the allowed delay time in the following situations:

• The user configures the device remotely. The user might be disconnected from the device because of a setting. If the `configuration commit delay` command is configured and the setting is not committed, the user can reconnect to the device after the delay time expires.
• The user is not familiar with the device configuration. If any parameters are configured incorrectly, the rollback mechanism can remove the incorrect settings after the delay time expires.

To configure the configuration commit delay feature:

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the next-startup configuration file.</td>
<td>`startup saved-configuration cfgfile [ backup</td>
<td>main ]`</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. (Optional.) Verify that a next-startup configuration file has been specified in user view.</td>
<td>display startup</td>
<td>If no next-startup configuration file has been specified, the backup operation will fail.</td>
</tr>
<tr>
<td>2. Back up the next-startup configuration file to a TFTP server in user view.</td>
<td>backup startup-configuration to dest-addr [dest-filename]</td>
<td>This command is not supported in FIPS mode.</td>
</tr>
</tbody>
</table>

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:

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

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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete next-startup configuration files.</td>
<td>`reset saved-configuration [ backup</td>
<td>If neither <code>backup</code> nor <code>main</code> is specified, this command deletes</td>
</tr>
<tr>
<td></td>
<td>main ]`</td>
<td>the main next-startup configuration file.</td>
</tr>
</tbody>
</table>

**Displaying and maintaining configuration files**

Execute `display` commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about configuration rollback.</td>
<td><code>display archive configuration</code></td>
</tr>
<tr>
<td>Display the running configuration.</td>
<td>`display current-configuration [ configuration [ module-name ]</td>
</tr>
<tr>
<td>Display the configuration differences between the running configuration and the next-startup configuration file.</td>
<td><code>display current-configuration diff</code></td>
</tr>
<tr>
<td>Display the factory defaults.</td>
<td><code>display default-configuration</code></td>
</tr>
<tr>
<td>Display the configuration differences between two configuration files or between a configuration file and the running configuration.</td>
<td>• `display diff configfile file-name-s { configfile file-name-d</td>
</tr>
<tr>
<td></td>
<td>• `display diff current-configuration { configfile file-name-d</td>
</tr>
<tr>
<td></td>
<td>• `display diff startup-configuration { configfile file-name-d</td>
</tr>
<tr>
<td>Display the contents of the configuration file for the next system startup.</td>
<td><code>display saved-configuration</code></td>
</tr>
<tr>
<td>Display the names of the configuration files for this startup and the next startup.</td>
<td><code>display startup</code></td>
</tr>
<tr>
<td>Display the valid configuration in the current view.</td>
<td><code>display this</code></td>
</tr>
</tbody>
</table>
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-R2418P01.bin and 5700-CMW710-BOOT-R2418P01.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 31 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 are nonexistent or invalid, connect to the console port, and power cycle the device to load a boot image from the Boot ROM 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 31 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 32.
Figure 32 System startup process

Start

Boot ROM runs

Press Ctrl+B promptly?

Yes

Enter Boot menus to upgrade Boot ROM or startup software images

No

Startup software images run

System starts up and CLI appears

Finish

Upgrade methods

<table>
<thead>
<tr>
<th>Upgrading method</th>
<th>Software types</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrading from the CLI:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upgrading software without using ISSU</td>
<td>• Boot ROM image</td>
<td>This method is disruptive. You must reboot the entire device to complete the upgrade.</td>
</tr>
<tr>
<td></td>
<td>• Comware images (excluding patches)</td>
<td></td>
</tr>
<tr>
<td>Upgrading software through a warm reboot</td>
<td>Comware images</td>
<td>You can perform a warm reboot only on standalone devices. Compared to upgrading software through a reboot, warm reboot reduces the service downtime.</td>
</tr>
<tr>
<td>Performing an ISSU</td>
<td>Comware images</td>
<td>The ISSU method enables a software upgrade without service interruption. Use this method for an IRF fabric. For more information about ISSU, see &quot;ISSU overview.&quot;</td>
</tr>
<tr>
<td>Upgrading from the Boot ROM menu</td>
<td>• Boot ROM image</td>
<td>Use this method when the device cannot start up correctly.</td>
</tr>
<tr>
<td></td>
<td>• Comware software images</td>
<td></td>
</tr>
</tbody>
</table>

**IMPORTANT:**

Upgrade an IRF fabric from the CLI rather than the Boot ROM menu.
The Boot ROM 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.
Upgrading 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.

Upgrading restrictions and guidelines

The switch can start up from the built-in flash memory or the USB disk. As a best practice, store the startup images in the built-in flash memory. If you store the startup images on the USB disk, do not remove the USB disk during startup.

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 transfer the upgrade image file to the root directory of a storage medium on the IRF fabric.

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

Preloading the Boot ROM image to Boot ROM

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load the upgrade Boot ROM image to the Boot ROM.</td>
<td><code>bootrom update file file-url slot slot-number-list</code></td>
<td>Specify the downloaded software image file for the <code>file-url</code> argument. The new Boot ROM image takes effect at a reboot.</td>
</tr>
</tbody>
</table>
Specifying startup images and completing the upgrade

You can specify startup images for IRF member devices in bulk, or one by one.

**Specifying startup images for all devices in bulk**

Perform this task in user view.

To specify startup images and complete the upgrade:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| 1. Specify the main or backup startup images for all devices. | • Use an .ipe file for upgrade: 
 `<boot-loader file ipe-filename all { backup | main }>`  
 • Use .bin files for upgrade: 
 `<boot-loader file boot boot-package system system-package [ feature feature-package&<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 [ slot slot-number ]` | Verify that the current software images are the same as the startup software images. |

**Specifying startup images for devices one by one**

Perform this task in user view.

To specify startup images and complete the upgrade:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| 1. Specify the main or backup startup images for the master device. | • Use an .ipe file for upgrade: 
 `<boot-loader file ipe-filename slot slot-number { backup | main }>`  
 • Use .bin files for upgrade: 
 `<boot-loader file boot boot-package system system-package [ feature feature-package&<1-30> ] slot slot-number { backup | main }>`  | N/A |
| 2. Specify the main startup images for each | • Use an .ipe file for upgrade: 
 `<boot-loader file ipe-filename slot slot-number { backup | main }>`  | 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 |
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>subordinate device.</td>
<td>• Use .bin files for upgrade: `boot-loader file boot boot-package system system-package { feature feature-package&lt;&amp;1-30&gt; } slot slot-number { backup</td>
<td>main }<code>&lt;br&gt;• Use the image list that the master device started up with for upgrade: </code>boot-loader update { all</td>
</tr>
<tr>
<td>3.</td>
<td>save</td>
<td>This step ensures that any configuration you have made can survive a reboot.</td>
</tr>
<tr>
<td>4.</td>
<td>reboot</td>
<td>At startup, each device reads the preloaded Boot ROM image to RAM, and loads the startup images.</td>
</tr>
<tr>
<td>5.</td>
<td><code>display boot-loader [ slot slot-number ]</code></td>
<td>Verify that the current software images are the same as the startup software images.</td>
</tr>
</tbody>
</table>

### 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.
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:
     
     ```bash
     warm-reboot [ file ipe ipe-filename ]
     ```
   
   • Use .bin files for upgrade:
     
     ```bash
     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.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display current software images and startup software images.</td>
<td><strong>display boot-loader [ slot slot-number ]</strong></td>
</tr>
</tbody>
</table>

### 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 33**.

**Figure 33 Network diagram**

![Network Diagram](image_url)
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 34 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:

<table>
<thead>
<tr>
<th>Slot</th>
<th>Upgrade Way</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Warm Reboot</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Table 12 ISSU methods for compatible upgrade</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ISSU method</strong></td>
</tr>
<tr>
<td>Incremental upgrade:</td>
</tr>
<tr>
<td>Service Upgrade</td>
</tr>
<tr>
<td>File Upgrade</td>
</tr>
<tr>
<td>ISSU Reboot</td>
</tr>
<tr>
<td>Reboot</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Item</th>
<th>issu commands</th>
<th>install commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade types</td>
<td>• Compatible.</td>
<td>Compatible.</td>
</tr>
<tr>
<td></td>
<td>• Incompatible.</td>
<td></td>
</tr>
<tr>
<td>Patch install/uninstall</td>
<td>Not supported.</td>
<td>Supported.</td>
</tr>
<tr>
<td>Upgrade mode</td>
<td>Chassis by chassis.</td>
<td>Chassis by chassis.</td>
</tr>
<tr>
<td>Impact on the system</td>
<td>Large.</td>
<td>Small.</td>
</tr>
<tr>
<td>Technical skill</td>
<td>Low.</td>
<td>High.</td>
</tr>
<tr>
<td>requirements</td>
<td>As a best practice, use this command set.</td>
<td>Administrators must have extensive system knowledge and understand the impact of each upgrade task on the network.</td>
</tr>
</tbody>
</table>

Preparing for ISSU

To perform a successful ISSU, make sure all the preparation requirements are met.

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:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Setting requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>GR/NSR</td>
<td>Enable GR or NSR for protocols including LDP, RSVP, OSPF, ISIS, BGP, and FSPF.</td>
</tr>
<tr>
<td>BFD</td>
<td>Disable BFD for protocols including LDP, RSVP, OSPF, ISIS, RIP, BGP, VRRP, and NQA.</td>
</tr>
<tr>
<td>Ethernet link aggregation</td>
<td>Use the long LACP timeout interval (the <code>lACP period short</code> command is not configured) on all member ports in dynamic aggregation groups.</td>
</tr>
<tr>
<td>IRF</td>
<td>Configure IRF bridge MAC persistence as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Compatible upgrade</strong>—Configure the <code>irf mac-address persistent timer</code> or <code>irf mac-address persistent always</code> command.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Incompatible upgrade</strong>—Configure the <code>irf mac-address persistent always</code> command if the bridge MAC address is the MAC address of the device for which you want to execute the <code>issu load</code> command.</td>
</tr>
</tbody>
</table>

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

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>(Optional.) Set the automatic rollback timer.</td>
<td>issu rollback-timer minutes</td>
</tr>
<tr>
<td>3.</td>
<td>Return to user view.</td>
<td>quit</td>
</tr>
</tbody>
</table>
## Step-by-Step Instructions

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| 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&<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 `slot-number` 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 chassis-number` | **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 *Fundamentals Command Reference*. |

---

### Performing an incompatible upgrade

Perform this task in user view.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| 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 `slot-number` argument.  
    As a best practice on a ring-topology IRF fabric, 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 *Fundamentals Command Reference*. |
### Upgrading a single-chassis IRF fabric

#### Performing a service upgrade or file upgrade

Perform this task in user view.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| 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 `slot-number` argument. |
| 2. | Complete the ISSU process. | `issu commit slot slot-number`

Specify the member ID of the device for the `slot-number` 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 [Fundamentals Command Reference]. |
| 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| 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 `slot-number` 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

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional.) Decompressing an .ipe file</td>
<td>To use <code>install</code> commands for upgrade, you must use .bin image files. If the upgrade file is an .ipe file, perform this task before you use <code>install</code> commands for upgrade.</td>
</tr>
<tr>
<td>(Required.) Perform one of the following tasks to update software:</td>
<td></td>
</tr>
<tr>
<td>• Installing or upgrading software images</td>
<td>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.</td>
</tr>
<tr>
<td>o Installing or upgrading images except for patches</td>
<td></td>
</tr>
<tr>
<td>o Installing patch images</td>
<td></td>
</tr>
<tr>
<td>• Uninstalling feature or patch images</td>
<td></td>
</tr>
<tr>
<td>o Uninstalling feature images</td>
<td></td>
</tr>
<tr>
<td>o Uninstalling patch images</td>
<td></td>
</tr>
<tr>
<td>(Optional.) Rolling back the running software images</td>
<td>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.</td>
</tr>
<tr>
<td>(Optional.) Aborting a software activate/deactivate operation</td>
<td>You can perform this task while an image is being activated or deactivated. This task is available only for service upgrade or file upgrade.</td>
</tr>
<tr>
<td>(Optional.) Committing software changes</td>
<td>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.</td>
</tr>
<tr>
<td>(Optional.) Verifying software images</td>
<td>Perform this task to verify that the software changes are correct.</td>
</tr>
<tr>
<td>(Optional.) Removing inactive software images</td>
<td>Perform this task to remove images</td>
</tr>
</tbody>
</table>

Decompressing an .ipe file

Perform this task in user view.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. (Optional.) Identify images that are included in the .ipe file.</td>
<td><code>display install ipe-info</code></td>
</tr>
<tr>
<td>2. Decompress the .ipe file.</td>
<td><code>install add ipe-filename medium-name:</code></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. (Optional.) Identify the ISSU method and possible impacts of the upgrade.</td>
<td>`install activate { boot filename</td>
</tr>
<tr>
<td>2. Activate images.</td>
<td>`install activate { boot filename</td>
</tr>
</tbody>
</table>

Installing patch images

Perform this task in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate patch images.</td>
<td>`install activate patch filename { all</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deactivate feature images.</td>
<td><code>install deactivate feature filename&amp;&lt;1-30&gt; slot slot-number</code></td>
</tr>
</tbody>
</table>

Uninstalling patch images

Perform this task in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deactivate patch images.</td>
<td>`install deactivate patch { all</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>(Optional.) Display available rollback points.</td>
<td>display install rollback</td>
</tr>
<tr>
<td>2.</td>
<td>Roll back the software.</td>
<td>install rollback to { point-id</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Press Ctrl+C while a software image is being activated or deactivated.</td>
</tr>
<tr>
<td>2.</td>
<td>Abort a software activate/deactivate operation in user view.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commit the software changes.</td>
<td>install commit</td>
<td>This command commits all software changes.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify software images.</td>
<td><code>install verify</code></td>
</tr>
</tbody>
</table>

Removing inactive software images

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

Perform this task in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove inactive software images.</td>
<td>`install remove [ slot slot-number ] { filename</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display version compatibility information.</td>
<td><code>display version comp-matrix</code></td>
</tr>
<tr>
<td>Display ISSU status information.</td>
<td><code>display issu state</code></td>
</tr>
<tr>
<td>Display automatic rollback timer information.</td>
<td><code>display issu rollback-timer</code></td>
</tr>
<tr>
<td>Display active software images.</td>
<td><code>display install active [ slot slot-number ] [ verbose ]</code></td>
</tr>
<tr>
<td>Display inactive software images.</td>
<td><code>display install inactive [ slot slot-number ] [ verbose ]</code></td>
</tr>
<tr>
<td>Display main startup software images.</td>
<td><code>display install committed [ slot slot-number ] [ verbose ]</code></td>
</tr>
<tr>
<td>Display backup startup software images.</td>
<td><code>display install backup [ slot slot-number ] [ verbose ]</code></td>
</tr>
<tr>
<td>Display ongoing ISSU activate, deactivate, and rollback operations.</td>
<td><code>display install job</code></td>
</tr>
<tr>
<td>Display ISSU log entries.</td>
<td><code>display install log [ verbose ]</code></td>
</tr>
<tr>
<td>Display software image file information.</td>
<td>`display install package { filename</td>
</tr>
<tr>
<td>Display the software images included in an .ipe file.</td>
<td><code>display install ipe-info ipe-filename</code></td>
</tr>
<tr>
<td>Display rollback point information.</td>
<td><code>display install rollback</code></td>
</tr>
<tr>
<td>Display all software image files that include a specific component or file.</td>
<td>`display install which { component name</td>
</tr>
<tr>
<td>Clear ISSU log entries.</td>
<td><code>reset install log-history oldest log-number</code></td>
</tr>
<tr>
<td>Clear ISSU rollback points.</td>
<td><code>reset install rollback oldest point-id</code></td>
</tr>
</tbody>
</table>
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 Hewlett Packard Enterprise Support.

ISSU examples for using issu commands

Software image upgrade to a compatible version

Upgrade requirements

As shown in Figure 35, the IRF fabric has two members.
Upgrade feature1 from R0201 to R0202. The two versions are compatible.

Figure 35 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

118
Display active software images.

```markdown
<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.

```markdown
<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

<table>
<thead>
<tr>
<th>Slot</th>
<th>Upgrade Way</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Service Upgrade</td>
</tr>
<tr>
<td>2</td>
<td>Service Upgrade</td>
</tr>
</tbody>
</table>

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.

```markdown
<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:

<table>
<thead>
<tr>
<th>Slot</th>
<th>Upgrade Way</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Service Upgrade</td>
</tr>
</tbody>
</table>

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 36, the IRF fabric has two members.
Upgrade feature1 from R0201 to R0202. The two versions are incompatible.
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

# Display active software images.
<Sysname> display install active

# 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

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:

<table>
<thead>
<tr>
<th>flash:/feature1-r0202.bin</th>
<th>Running Version</th>
<th>New Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Alpha 0201</td>
<td>Alpha 0202</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Slot</th>
<th>Upgrade Way</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Reboot</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>flash:/feature1-r0202.bin</th>
<th>Running Version</th>
<th>New Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Alpha 0201</td>
<td>Alpha 0202</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Slot</th>
<th>Upgrade Way</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Reboot</td>
</tr>
</tbody>
</table>

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 37, 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.
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

# 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:

<table>
<thead>
<tr>
<th></th>
<th>Running Version</th>
<th>New Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alpha 0201</td>
<td>Alpha 0202</td>
<td></td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th></th>
<th>Running Version</th>
<th>New Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alpha 0201</td>
<td>Alpha 0202</td>
<td></td>
</tr>
</tbody>
</table>

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 38, the IRF fabric has two members.
Upgrade feature1 from R0201 to R0202. The two versions are compatible.

Figure 38 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
# 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
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

Upgrading summary according to the following table:

<table>
<thead>
<tr>
<th></th>
<th>Running Version</th>
<th>New Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot 2</td>
<td>Alpha 0201</td>
<td>Alpha 0202</td>
</tr>
</tbody>
</table>

Influenced service according to the following table on slot 2:

<table>
<thead>
<tr>
<th>feature1</th>
<th>Slot</th>
<th>Upgrade Way</th>
</tr>
</thead>
<tbody>
<tr>
<td>feature1</td>
<td>2</td>
<td>Service Upgrade</td>
</tr>
</tbody>
</table>

<sysname> install activate feature flash:/feature1-r0202.bin slot 1 test

Upgrade summary according to the following table:

<table>
<thead>
<tr>
<th></th>
<th>Running Version</th>
<th>New Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot 1</td>
<td>Alpha 0201</td>
<td>Alpha 0202</td>
</tr>
</tbody>
</table>

Influenced service according to the following table on slot 1:

<table>
<thead>
<tr>
<th>feature1</th>
<th>Slot</th>
<th>Upgrade Way</th>
</tr>
</thead>
<tbody>
<tr>
<td>feature1</td>
<td>1</td>
<td>Service Upgrade</td>
</tr>
</tbody>
</table>

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

Overwrite it?[Y/N]: y

Upgrading summary according to the following table:

<table>
<thead>
<tr>
<th></th>
<th>Running Version</th>
<th>New Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot 2</td>
<td>Alpha 0201</td>
<td>Alpha 0202</td>
</tr>
</tbody>
</table>
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 38, 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 slot 2:
  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 39, the IRF fabric has two members.
Patch the software images running on the members.

Figure 39 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

128
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.

ℹ️ 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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display files or folders.</td>
<td>dir [ /all ] [ file-url ]</td>
<td>N/A</td>
</tr>
<tr>
<td>Create a folder on a storage medium.</td>
<td>mkdir directory</td>
<td>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.</td>
</tr>
<tr>
<td>Display the current path.</td>
<td>pwd</td>
<td>N/A</td>
</tr>
<tr>
<td>Copy a file.</td>
<td>copy file-url-source file-url-dest</td>
<td>N/A</td>
</tr>
<tr>
<td>Move a file.</td>
<td>move file-url-source file-url-dest</td>
<td>The destination folder must have enough space for the file.</td>
</tr>
<tr>
<td>Display the contents of a file.</td>
<td>more file-url</td>
<td>N/A</td>
</tr>
<tr>
<td>Permanently delete a file.</td>
<td>delete file-url</td>
<td>N/A</td>
</tr>
</tbody>
</table>
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 port 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 port

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 port.
- Bring up the management Ethernet port.
- If the servers reside on a different network, specify a gateway for the management Ethernet port.

To configure the management Ethernet port on an IPv4 network:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter management Ethernet port view.</td>
<td><code>interface m-eth0</code></td>
<td>N/A</td>
</tr>
<tr>
<td>3. Assign an IPv4 address to the port.</td>
<td>`ip address ip-address { mask-length</td>
<td>mask }`</td>
</tr>
<tr>
<td>4. Specify an IPv4 gateway for the port.</td>
<td><code>ip gateway ip-address</code></td>
<td>By default, the management Ethernet port has no IPv4 gateway configured.</td>
</tr>
<tr>
<td>5. Bring up the port.</td>
<td><code>undo shutdown</code></td>
<td>By default, the management Ethernet port is up.</td>
</tr>
<tr>
<td>6. Return to system view.</td>
<td><code>quit</code></td>
<td>N/A</td>
</tr>
</tbody>
</table>

To configure the management Ethernet port on an IPv6 network:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2. Enter management Ethernet port view.</td>
<td><code>interface m-eth0</code></td>
<td>N/A</td>
</tr>
</tbody>
</table>
### 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 count | -s size ] * ip-address`

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 count | -s size ] * ipv6-address`

### 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:

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

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

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

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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load a system image.</td>
<td>install load system-package</td>
</tr>
</tbody>
</table>

Rebooting the device

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reboot the current member device.</td>
<td>reboot</td>
</tr>
</tbody>
</table>
Displaying device information in emergency shell mode

Execute `display` commands in any view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display copyright information.</td>
<td><code>display copyright</code></td>
</tr>
<tr>
<td>Display software package information.</td>
<td><code>display install package package</code></td>
</tr>
<tr>
<td>Display management Ethernet port information.</td>
<td><code>display interface m-eth0</code></td>
</tr>
<tr>
<td>Display IPv4 routing information.</td>
<td><code>display ip routing-table</code></td>
</tr>
<tr>
<td>Display IPv6 routing information.</td>
<td><code>display ipv6 routing-table</code></td>
</tr>
<tr>
<td>Display boot image version information.</td>
<td><code>display version</code></td>
</tr>
</tbody>
</table>

Emergency shell usage example

Network requirements

As shown in Figure 40, 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 40 Network diagram

Usage procedure

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

```
<boot>dir
Directory of flash:
  0  -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-r2418p01.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
```
The output shows that the boot image is present but the system image is not. The available space is 147072 KB, enough for saving the system image.

# Identify the boot image version.

```
<boot>display version
HPE Comware Software, Version 7.1.045, Release 2418P01
Copyright (c) 2010-2015 Hewlett Packard Enterprise Development LP
HPE 5700-48XG uptime is 0 weeks, 2 days, 7 hours, 50 minutes
Last reboot reason : Cold reboot
Boot image: flash:/5700-cmw710-boot-r2418p01.bin
Boot image version: 7.1.045, Release 2418P01
    Compiled Sep 16 2014 13:44:42
FF 5700-48XG with 2 Processors
BOARD TYPE:         FF 5700-48XG Switch
DRAM:               2048M bytes
FLASH:              512M bytes
```

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

```
<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-r2418p01.bin
```

# Identify whether the system image matches the boot image.

```
<boot> display install package flash:/5700-cmw710-system-r2418p01.bin
flash:/5700-cmw710-system-r2418p01.bin
[Package]
Vendor: HPE
Product: 5700
Service name: system
Platform version: 7.1.045
Product version: Release 2418P01
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-r2418p01.bin
Check package flash:/5700-cmw710-system-r2418p01.bin ...
Extracting package ...

Loading...
Line aux0 is available.

Press ENTER to get started.

After you press Enter, the following information appears:
<System>
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

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

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:

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

If you power cycle an HPE 5700, the system time settings are restored to the defaults. You must configure the settings again.

To specify the system time source:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2. Specify the system time source.</td>
<td>`clock protocol { none</td>
<td>ntp</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Set the UTC time.</td>
<td><code>clock datetime time date</code></td>
<td>By default, the UTC time is the factory-default time.</td>
</tr>
<tr>
<td>2. Enter system view.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>3. Set the local time zone.</td>
<td>`clock timezone zone-name { add</td>
<td>minus } zone-offset`</td>
</tr>
<tr>
<td>4. Set the daylight saving time.</td>
<td><code>clock summer-time name start-time start-date end-time end-date add-time</code></td>
<td>By default, daylight saving time is disabled.</td>
</tr>
</tbody>
</table>
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) 2010-2015 Hewlett Packard Enterprise Development LP          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
****************************************************************************
```

To enable displaying the copyright statement:

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

Configuring banners

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

Banner types

The system supports the following banners:

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

```plaintext
<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:

```plaintext
<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:

```plaintext
<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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the legal banner</td>
<td>header legal text</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the MOTD banner</td>
<td>header motd text</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the login banner</td>
<td>header login text</td>
</tr>
<tr>
<td>5.</td>
<td>Configure the incoming banner</td>
<td>header incoming text</td>
</tr>
<tr>
<td>6.</td>
<td>Configure the shell banner</td>
<td>header shell text</td>
</tr>
</tbody>
</table>
Setting the system operating mode

The device can operate in the following modes:

- **advance**—Advanced mode.
- **standard**—Standard mode.
- **expert**—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 expert mode. For more information about FCoE over S-Channel, see *FC and 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>system-view</code></td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>`system-working-mode { advance</td>
<td>standard</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reboot an IRF member device</td>
<td><code>reboot [slot slot-number] [force]</code></td>
<td>Use this command in user view</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the reboot date and</td>
<td><code>scheduler reboot at time [date]</code></td>
<td>By default, no reboot date or time is specified.</td>
</tr>
<tr>
<td>time.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specify the reboot delay</td>
<td><code>scheduler reboot delay time</code></td>
<td>By default, no reboot delay time is specified.</td>
</tr>
<tr>
<td>time.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 non-periodic schedule or a periodic schedule. A non-periodic 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 can have a maximum of 64 user roles. After the limit is reached, you cannot assign additional user roles to the schedule. A command in a schedule can be executed if it is permitted by one or more user roles of the schedule.
- Assigning the security-audit user role to a schedule removes the other user role assignments for the schedule. Assigning any other user roles to a schedule removes the security-audit user role.
role assignment for the schedule. Only the remaining user role assignments take effect. For more information about user roles, see “Configuring RBAC.”

- 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 non-periodic schedule for the device:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a job.</td>
<td>scheduler job <em>job-name</em></td>
</tr>
<tr>
<td>3.</td>
<td>Assign a command to the job.</td>
<td>command <em>id command</em></td>
</tr>
<tr>
<td>4.</td>
<td>Exit system view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Create a schedule.</td>
<td>scheduler schedule <em>schedule-name</em></td>
</tr>
<tr>
<td>6.</td>
<td>Assign a job to a schedule.</td>
<td>job <em>job-name</em></td>
</tr>
<tr>
<td>7.</td>
<td>Assign user roles to the schedule.</td>
<td>user-role <em>role-name</em></td>
</tr>
</tbody>
</table>
| 8.   | Specify an execution time table for the non-periodic schedule. | - Specify the execution date and time: *time at time date*  
- Specify the execution days and time: *time once at time [ month-date month-day | week-day week-day&<1-7> ]*  
- Specify the execution delay time: *time once delay time* | 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a job.</td>
<td>scheduler job <em>job-name</em></td>
</tr>
<tr>
<td>3.</td>
<td>Assign a command to the job.</td>
<td>command <em>id command</em></td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>4.</td>
<td>Exit system view.</td>
<td>quit</td>
</tr>
<tr>
<td>5.</td>
<td>Create a schedule.</td>
<td>scheduler schedule schedule-name</td>
</tr>
<tr>
<td>6.</td>
<td>Assign user roles to the schedule.</td>
<td>user-role role-name</td>
</tr>
<tr>
<td>7.</td>
<td>Assign a job to a schedule.</td>
<td>job job-name</td>
</tr>
<tr>
<td>8.</td>
<td>Specify an execution time table for the periodic schedule.</td>
<td>time repeating at time on:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>time repeating at time on:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Execute the schedule at an interval from the specified time on:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>time repeating at time on:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>time repeating at time on:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configure either command.</td>
</tr>
</tbody>
</table>

You can assign multiple commands to a job. A job with a smaller ID will be executed first.

By default, no schedule exists.

By default, a schedule has the user role of the schedule creator.

By default, no job is assigned to a schedule.

You can assign multiple jobs to a schedule. The jobs will be executed concurrently.

Schedule configuration example

Network requirements

As shown in Figure 41, 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 41 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
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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>undo password-recovery enable</td>
<td>By default, password recovery capability is enabled.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>fan prefer-direction slot slot-number { power-to-port</td>
<td>port-to-power }</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2.</td>
<td>shutdown-interval time</td>
<td>The default setting is 30 seconds.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable CPU usage monitoring.</td>
<td>monitor cpu-usage enable [ slot slot-number [ cpu cpu-number ] ]</td>
</tr>
<tr>
<td>3.</td>
<td>Set the CPU usage sampling interval.</td>
<td>monitor cpu-usage interval interval-value [ slot slot-number [ cpu cpu-number ] ]</td>
</tr>
<tr>
<td>4.</td>
<td>Set CPU usage thresholds.</td>
<td>monitor cpu-usage threshold cpu-threshold [ slot slot-number [ cpu cpu-number ] ]</td>
</tr>
</tbody>
</table>

### 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 42 show how the device generates notifications based on the free-memory thresholds.

### Table 14 Memory alarm notifications and memory alarm-removed notifications

<table>
<thead>
<tr>
<th>Notification</th>
<th>Triggering condition</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minor alarm notification</td>
<td>The amount of free memory space decreases to or below the minor alarm threshold for the first time.</td>
<td>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.</td>
</tr>
<tr>
<td>Severe alarm notification</td>
<td>The amount of free memory space decreases to or below the severe alarm threshold for the first time.</td>
<td>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.</td>
</tr>
<tr>
<td>Critical alarm notification</td>
<td>The amount of free memory space decreases to or below the critical alarm threshold for the first time.</td>
<td>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.</td>
</tr>
<tr>
<td>Critical alarm-removed</td>
<td>The amount of free memory space increases to or above the severe alarm threshold.</td>
<td>N/A</td>
</tr>
<tr>
<td>Severe alarm-removed</td>
<td>The amount of free memory</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Notification

<table>
<thead>
<tr>
<th>Notification</th>
<th>Triggering condition</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>notification</td>
<td>space increases to or above the minor alarm threshold.</td>
<td></td>
</tr>
<tr>
<td>Minor alarm-removed notification</td>
<td>The amount of free memory space increases to or above the normal state threshold.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

#### Figure 42 Memory alarm notification and alarm-removed notification

![Free memory space over time](image)

To set memory thresholds:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | 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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Configure the temperature alarm thresholds.</td>
<td>temperature-limit slot slot-number hotspot sensor-number lowlimit warninglimit [ alarmlimit ]</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td>N/A</td>
</tr>
<tr>
<td>2. Disable all USB interfaces.</td>
<td>usb disable</td>
<td>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 Fundamentals Command Reference.</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the key parameters of transceiver modules.</td>
<td><code>display transceiver { interface [ interface-type interface-number ] }</code></td>
<td>N/A</td>
</tr>
<tr>
<td>Display the electrical label information of transceiver modules.</td>
<td><code>display transceiver manuinfo interface [ interface-type interface-number ]</code></td>
<td>This command cannot display information for some transceiver modules.</td>
</tr>
</tbody>
</table>

### Diagnosing transceiver modules

The device provides the alarm and digital diagnosis features 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 feature, including the temperature, voltage, laser bias current, TX power, and RX power.

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

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

### 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:
<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore the factory-default settings and states.</td>
<td><code>restore factory-default</code></td>
<td>This command takes effect after a device reboot.</td>
</tr>
</tbody>
</table>

### Displaying and maintaining device management configuration

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the system time, date, local time zone, and daylight saving time.</td>
<td><code>display clock</code></td>
</tr>
<tr>
<td>Display the copyright statement.</td>
<td><code>display copyright</code></td>
</tr>
<tr>
<td>Display CPU usage statistics.</td>
<td><code>display cpu-usage [ slot slot-number [ cpu cpu-number ] ]</code></td>
</tr>
<tr>
<td>Display CPU usage monitoring settings.</td>
<td><code>display cpu-usage configuration [ slot slot-number [ cpu cpu-number ] ]</code></td>
</tr>
<tr>
<td>Display historical CPU usage statistics in a chart.</td>
<td><code>display cpu-usage history [ job job-id ] [ slot slot-number [ cpu cpu-number ] ]</code></td>
</tr>
<tr>
<td>Display hardware information.</td>
<td>`display device [ flash</td>
</tr>
<tr>
<td>Display the electronic label information of the device.</td>
<td><code>display device manuinfo [ slot slot-number ]</code></td>
</tr>
<tr>
<td>Display the electronic label information of a fan.</td>
<td><code>display device manuinfo slot slot-number fan fan-id</code></td>
</tr>
<tr>
<td>Display the electronic label information of a power supply.</td>
<td><code>display device manuinfo slot slot-number power power-id</code></td>
</tr>
<tr>
<td>Display the operating statistics for multiple feature modules.</td>
<td>`display diagnostic-information [ hardware</td>
</tr>
<tr>
<td>Display device temperature statistics.</td>
<td><code>display environment [ slot slot-number ]</code></td>
</tr>
<tr>
<td>Display the operating states of fans.</td>
<td><code>display fan [ slot slot-number [ fan-id ] ]</code></td>
</tr>
<tr>
<td>Display memory usage statistics.</td>
<td><code>display memory [ slot slot-number [ cpu cpu-number ] ]</code></td>
</tr>
<tr>
<td>Display memory usage thresholds.</td>
<td><code>display memory-threshold [ slot slot-number [ cpu cpu-number ] ]</code></td>
</tr>
<tr>
<td>Display power supply information.</td>
<td><code>display power [ slot slot-number [ power-id ] ]</code></td>
</tr>
<tr>
<td>Display job configuration information.</td>
<td><code>display scheduler job [ job-name ]</code></td>
</tr>
<tr>
<td>Display job execution log information.</td>
<td><code>display scheduler logfile</code></td>
</tr>
<tr>
<td>Display the automatic reboot schedule.</td>
<td><code>display scheduler reboot</code></td>
</tr>
<tr>
<td>Display schedule information.</td>
<td><code>display scheduler schedule [ schedule-name ]</code></td>
</tr>
<tr>
<td>Display system stability and status information.</td>
<td><code>display system stable state</code></td>
</tr>
<tr>
<td>Task</td>
<td>Command</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Display system working mode information.</td>
<td><code>display system-working-mode</code></td>
</tr>
<tr>
<td>Display system version information.</td>
<td><code>display version</code></td>
</tr>
<tr>
<td>Display the startup software image upgrade history records of the master.</td>
<td><code>display version-update-record</code></td>
</tr>
<tr>
<td>Clear job execution log information.</td>
<td><code>reset scheduler logfile</code></td>
</tr>
</tbody>
</table>
Using Tcl

Comware 7 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 cannot press `Tab` to complete an abbreviated Tcl command.
- No online help information is provided for Tcl commands.
- Successfully executed Tcl commands are not saved to command history buffers.
- You can apply Tcl environment variables to Comware commands.

Using Tcl to configure the device

If you have used a Comware command to enter a subview under Tcl configuration view, you can only use the `quit` command, instead of the `tclquit` command, to return to the upper level view. The `tclquit` command has the same effect as the `quit` command in Tcl configuration view.

To use Tcl to configure the device:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter Tcl configuration view from user view.</td>
<td><code>tclsh</code></td>
<td>Execute this command in user view.</td>
</tr>
<tr>
<td>Execute a Tcl command.</td>
<td><code>Tcl command</code></td>
<td>N/A</td>
</tr>
<tr>
<td>Return from Tcl configuration view to user view.</td>
<td><code>tclquit</code></td>
<td>Execute this command in Tcl configuration view.</td>
</tr>
</tbody>
</table>

Executing Comware commands in Tcl configuration view

Follow these restrictions and guidelines when you execute Comware commands in Tcl configuration view:

- For Comware commands, you can enter `?` to obtain online help or press `Tab` to complete an abbreviated command. For more information, see "Using the CLI."
- The `cli` command is a Tcl command, so you cannot enter `?` to obtain online help or press `Tab` to complete an abbreviated command.
Successfully executed Comware commands are saved to command history buffers. You can use the upper arrow or lower arrow key to obtain executed commands.

To execute multiple Comware commands in one operation:
- Enter multiple Comware commands separated by semi-colons to execute the commands in the order they are entered. For example, `ospf 100; area 0`.
- Specify multiple Comware commands for the `cli` command, quote them, and separate them by a space and a semicolon. For example, `cli "ospf 100 ; area 0"`.
- Specify one Comware command for each `cli` command and separate them by a space and a semicolon. For example, `cli ospf 100 ; cli area 0`.

To execute Comware commands in Tcl configuration view:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter Tcl configuration view</td>
<td><code>tclsh</code></td>
</tr>
<tr>
<td>2.</td>
<td>Execute Comware commands directly.</td>
<td><code>Command</code></td>
</tr>
<tr>
<td>3.</td>
<td>Execute Comware commands by using the <code>cli</code> command.</td>
<td><code>cli command</code></td>
</tr>
</tbody>
</table>
Using Python

Comware 7 provides a built-in Python interpreter that supports the following items:

- Python 2.7 commands.
- Python 2.7 standard API.
- Comware 7 extended API. For more information about the Comware 7 extended API, see "Comware 7 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.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the Python shell from user view.</td>
<td>python</td>
</tr>
</tbody>
</table>

Executing a Python script

Execute a Python script in user view.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Execute a Python script.</td>
<td>python filename</td>
</tr>
</tbody>
</table>

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 43 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 7 extended Python API

The Comware 7 extended Python API is compatible with the Python syntax.

Importing and using the Comware 7 extended Python API

To use the Comware 7 extended Python API, you must import the API to Python. Use either of the following methods to import and use the Comware 7 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:

  ```python
  >>> 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:

  ```python
  >>> from comware import Transfer
  >>> Transfer('tftp', '192.168.1.26', 'test.cfg', 'flash:/test.cfg', user='', password='')
  <comware.Transfer object at 0xb7e5e0e0>
  ```

Comware 7 extended Python API functions

CLI class

CLI

Use CLI to execute Comware 7 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**

```python
# Add a local user with the username test.
<Sysname> python
Python 2.7.3 (default, Jan 24 2016, 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**

```python
# Add a local user and get the output from the command.
<Sysname> python
Python 2.7.3 (default, Jan 24 2016, 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

Use Transfer to download a file from a server.

Syntax

```
Transfer(protocol='', host='', source='', dest='', vrf='', 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.
- **vrf**: Specifies the VPN instance to which the remote server belongs. This argument is a case-sensitive string of 1 to 31 characters. If the server belongs to the public network, do not specify this argument.
- **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

```python
<Sysname> python
Python 2.7.3 (default, Jan 24 2016, 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

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

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.

```python
<Sysname> python
Python 2.7.3 (default, Jan 24 2016, 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

[]

164
Using automatic configuration

Overview

When the device starts up without a configuration file, it searches the root directory of its local storage medium for the `autocfg.py`, `autocfg.tcl`, or `autocfg.cfg` file.

- If one of the files exists, the device loads the file to complete automatic configuration.
  
  For the device to use a local file for automatic configuration, save only one of the previously mentioned files in the root directory of the device’s storage medium. For more information about preparing one of the files, see "Preparing the files for automatic configuration."

- If none of the files exists, the device automatically obtains a set of configuration settings from a file server.

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 44, server-based automatic configuration requires the following servers:

- DHCP server.
- File server (TFTP or HTTP server).
- (Optional.) DNS server.

**Figure 44 Network diagram**

![Network diagram](image)

**Server-based automatic configuration task list**

<table>
<thead>
<tr>
<th>Tasks at a glance</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Required.) Configuring the file server</td>
</tr>
<tr>
<td>(Required.) Preparing the files for automatic configuration</td>
</tr>
<tr>
<td>(Required.) Configuring the DHCP server</td>
</tr>
</tbody>
</table>

165
Tasks at a glance

| Optional. | Configuring the DNS server |
| 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable DHCP.</td>
<td>dhcp enable</td>
</tr>
<tr>
<td>3.</td>
<td>Create a DHCP address pool and enter its view.</td>
<td>dhcp server ip-pool pool-name</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the address pool.</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring the DHCP server when a TFTP file server is used

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable DHCP.</td>
<td>dhcp enable</td>
</tr>
<tr>
<td>3.</td>
<td>Create a DHCP address pool and enter its view.</td>
<td>dhcp server ip-pool pool-name</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the address pool.</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Specify a TFTP server.</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Specify the configuration file name.</td>
<td>bootfile-name bootfile-name</td>
</tr>
</tbody>
</table>

### 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.

Server-based automatic configuration examples

Automatic configuration using TFTP server

Network requirements

As shown in Figure 45, 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.
### 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
# 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/  Lease expiration      Type  
   + Hardware address
   + 192.168.2.2    3030-3066-2e65-3233-  May 6 05:21:25 2013   Auto(C)  
   + 642e-3561-6633-2d56-
   + 6c61-6e2d-696e-7465-  
   + 7266-6163-6533
   + 192.168.2.3    3030-3066-2e65-3230-  May 6 05:22:50 2013   Auto(C)  
   + 302e-3232-3033-2d56-
   + 6c61-6e2d-696e-7465-  
   + 7266-6163-6533
   + 192.168.3.2    3030-6530-2e66-6330-  May 6 05:23:15 2013   Auto(C)  
   + 302e-3335-3131-2d56-
   + 6c61-6e2d-696e-7465-  
   + 7266-6163-6531
   + 192.168.3.3    3030-6530-2e66-6330-  May 6 05:24:10 2013   Auto(C)  
   + 302e-3335-3135-2d56-
   + 6c61-6e2d-696e-7465-  
   + 7266-6163-6532
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 46, 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 Switch A.
- Require the administrator to enter the correct username and password at login.

Figure 46 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.

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 Vlan-interface1
   ip address dhcp-alloc
   return
```
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/    Lease expiration      Type
                   Hardware address                        
   192.168.1.2      0030-3030-632e-3239-4574-6830-2f30-2f32  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 47, 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 Switch A.
- 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.
   ```

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 abcabc ;service-type telnet ;quit ;user-interface vty 0 4 ;authentication-mode scheme ;user-role network-admin ;quit ;interface Vlan-interface1 ;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/ Lease expiration  Type  Hardware address
   192.168.1.2  0030-3030-632e-3239-3035-2e36-3736-622d-4574-6830-2f30-2f32  Dec 12 17:41:15 2013  Auto(C)
   3035-2e36-3736-622d-4574-6830-2f30-2f32
   ```

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 IRF setup

### Network requirements

As shown in **Figure 48**, 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 configurations and form an IRF fabric.

**Figure 48 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:

<table>
<thead>
<tr>
<th>File</th>
<th>Content</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>.cfg configuration file</td>
<td>Commands required for IRF setup.</td>
<td>You can create a configuration file by copying and modifying the configuration file of an existing IRF fabric.</td>
</tr>
<tr>
<td>sn.txt</td>
<td>Serial numbers of the member switches.</td>
<td>Each SN uniquely identifies a switch. These SNs will be used for assigning a unique IRF member ID to each member switch.</td>
</tr>
<tr>
<td>(Optional.) .ipe or .bin software image file</td>
<td>Software images.</td>
<td>If the member switches are running different software versions, you must prepare the software image file used for software upgrade.</td>
</tr>
<tr>
<td>.py Python script file</td>
<td>Python commands and APIs that complete the following tasks:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. (Optional.) Verifies that the flash memory has sufficient space for the files to be downloaded.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. Downloads the configuration file and sn.txt.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. (Optional.) Downloads the software image file and specifies it as the main startup image file.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. Resolves sn.txt and assigns a unique IRF member ID to each SN.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e. Specifies the configuration file as the main next-startup configuration file.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>f. Reboots the member switches.</td>
<td>For more information about Python script configuration, see &quot;Using Python.&quot;</td>
</tr>
</tbody>
</table>

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-Ten-GigabitEthernet1/0/1] dhcp select server
   [DeviceA-Ten-GigabitEthernet1/0/1] quit

   # Specify the URL of the script file for the clients.
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.

```bash
<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.
Document conventions and icons

Conventions

This section describes the conventions used in the documentation.

Port numbering in examples

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

Command conventions

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

GUI conventions

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

Symbols

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>⚠️ WARNING!</strong></td>
<td>An alert that calls attention to important information that if not understood or followed can result in personal injury.</td>
</tr>
<tr>
<td><strong>⚠️ CAUTION:</strong></td>
<td>An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.</td>
</tr>
<tr>
<td><strong>ℹ️ IMPORTANT:</strong></td>
<td>An alert that calls attention to essential information.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>An alert that contains additional or supplementary information.</td>
</tr>
<tr>
<td><strong>💡 TIP:</strong></td>
<td>An alert that provides helpful information.</td>
</tr>
</tbody>
</table>
## Network topology icons

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="" alt="icon" /></td>
<td>Represents a generic network device, such as a router, switch, or firewall.</td>
</tr>
<tr>
<td><img src="" alt="icon" /></td>
<td>Represents a routing-capable device, such as a router or Layer 3 switch.</td>
</tr>
<tr>
<td><img src="" alt="icon" /></td>
<td>Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.</td>
</tr>
<tr>
<td><img src="" alt="icon" /></td>
<td>Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.</td>
</tr>
<tr>
<td><img src="" alt="icon" /></td>
<td>Represents an access point.</td>
</tr>
<tr>
<td><img src="" alt="icon" /></td>
<td>Represents a wireless terminator unit.</td>
</tr>
<tr>
<td><img src="" alt="icon" /></td>
<td>Represents a wireless terminator.</td>
</tr>
<tr>
<td><img src="" alt="icon" /></td>
<td>Represents a mesh access point.</td>
</tr>
<tr>
<td><img src="" alt="icon" /></td>
<td>Represents omnidirectional signals.</td>
</tr>
<tr>
<td><img src="" alt="icon" /></td>
<td>Represents directional signals.</td>
</tr>
<tr>
<td><img src="" alt="icon" /></td>
<td>Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.</td>
</tr>
<tr>
<td><img src="" alt="icon" /></td>
<td>Represents a security card, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG card.</td>
</tr>
</tbody>
</table>
Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website: www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website: www.hpe.com/support/hpesc

Information to collect
- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
  o Hewlett Packard Enterprise Support Center Get connected with updates page: www.hpe.com/support/e-updates
  o Software Depot website: www.hpe.com/support/softwaredepot
- To view and update your entitlements, and to link your contracts, Care Packs, and warranties with your profile, go to the Hewlett Packard Enterprise Support Center More Information on Access to Support Materials page: www.hpe.com/support/AccessToSupportMaterials

⚠️ IMPORTANT:
Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.
Websites

<table>
<thead>
<tr>
<th>Website</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Networking websites</strong></td>
<td></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Information Library for Networking</td>
<td><a href="http://www.hpe.com/networking/resourcefinder">www.hpe.com/networking/resourcefinder</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Networking website</td>
<td><a href="http://www.hpe.com/info/networking">www.hpe.com/info/networking</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise My Networking website</td>
<td><a href="http://www.hpe.com/networking/support">www.hpe.com/networking/support</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Networking Warranty</td>
<td><a href="http://www.hpe.com/networking/warranty">www.hpe.com/networking/warranty</a></td>
</tr>
<tr>
<td><strong>General websites</strong></td>
<td></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Information Library</td>
<td><a href="http://www.hpe.com/info/enterprise/docs">www.hpe.com/info/enterprise/docs</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Support Center</td>
<td><a href="http://www.hpe.com/support/hpesc">www.hpe.com/support/hpesc</a></td>
</tr>
<tr>
<td>Hewlett Packard Enterprise Support Services Central</td>
<td>ssc.hpe.com/portal/site/ssc/</td>
</tr>
<tr>
<td>Contact Hewlett Packard Enterprise Worldwide</td>
<td><a href="http://www.hpe.com/assistance">www.hpe.com/assistance</a></td>
</tr>
<tr>
<td>Subscription Service/Support Alerts</td>
<td><a href="http://www.hpe.com/support/e-updates">www.hpe.com/support/e-updates</a></td>
</tr>
<tr>
<td>Software Depot</td>
<td><a href="http://www.hpe.com/support/softwaredepot">www.hpe.com/support/softwaredepot</a></td>
</tr>
<tr>
<td>Customer Self Repair (not applicable to all devices)</td>
<td><a href="http://www.hpe.com/support/selfrepair">www.hpe.com/support/selfrepair</a></td>
</tr>
<tr>
<td>Insight Remote Support (not applicable to all devices)</td>
<td><a href="http://www.hpe.com/info/insightremotesupport/docs">www.hpe.com/info/insightremotesupport/docs</a></td>
</tr>
</tbody>
</table>

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:
www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty, Care Pack Service, or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product’s service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website:
www.hpe.com/info/insightremotesupport/docs

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title,
part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.
Index

A

AAA
  RBAC AAA authorization, 45
  RBAC default user role, 50
  RBAC local AAA authentication user configuration, 54
  RBAC non-AAA authorization, 45
  RBAC user role local AAA authentication, 50
  RBAC user role non-AAA authentication, 51
  RBAC user role remote AAA authentication, 50

abbreviating command, 4

aborting
  ISSU software activate/deactivate operation (install series commands), 116

accessing
  CLI online help, 2
  emergency shell server access, 133
  login management SNMP device access, 34
  RBAC VPN instance access policy, 44

accounting
  login management command accounting, 40, 41
  login management user access control, 35

ACL
  login management command authorization, 38, 39
  login management SNMP access control, 36, 37
  login management SSH login control, 35
  login management Telnet login control, 35
  login management user access control, 35

activating
  ISSU activate operation (install series commands), 116

active

FTP active (PORT) operating mode, 68

airflow direction configuration, 149, 149

alias (command keyword), 4

API
  extended Python API, 160
  extended Python API functions, 160

archiving
  configuration archive, 92
  configuration archive parameters, 93
  configuration archiving (automatic), 94
  running configuration (manual), 94

argument (CLI string/text type), 4

ASCII transfer mode, 68

assigning
  CLI user line assignment, 17
  RBAC local AAA authentication user role, 50
  RBAC non-AAA authentication user role, 51
  RBAC permission assignment, 43
  RBAC remote AAA authentication user role, 50
  RBAC user role, 50
  RBAC user role assignment, 45

authenticating
  FTP basic server authentication, 69
  login management CLI console/AUX none authentication, 19
  login management CLI console/AUX password authentication, 20
  login management CLI console/AUX scheme authentication, 20
  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, 23
login management Telnet login password authentication, 24
login management Telnet login scheme authentication, 25
RBAC local AAA authentication user configuration, 54
RBAC RADIUS authentication user configuration, 56
RBAC temporary user role authorization (HWTACACS authentication), 59
RBAC temporary user role authorization (RADIUS authentication), 63
RBAC user role authentication, 53
RBAC user role local AAA authentication, 50
RBAC user role remote AAA authentication, 50
authorizing
   FTP basic server authorization, 69
   login management command authorization, 38, 39
   login management user access control, 35
   RBAC temporary user role authorization, 52
auto
   automatic configuration archiving, 94
   configuration. See automatic configuration
automatic configuration
   DHCP server, 167
   DNS server, 168
   file preparation, 166
   file server configuration, 166
   gateway, 169
   HTTP server+Python script, 175
   HTTP server+Tcl script, 174
   interface selection, 169
   IRF setup, 176
   server-based, 165, 169
   start, 169
   TFTP server, 169
   USB-based, 165
AUX
   console/AUX common user line settings, 21
   console/AUX none authentication, 19
   console/AUX password authentication, 20
   console/AUX scheme authentication, 20
   login management CLI local console/AUX port login, 19
   login management overview, 14
B
backing up
   main next-startup configuration file, 96
   software upgrade backup image set, 99
banner
   configuration, 140, 140, 141, 141
   incoming type, 140, 140
   legal type, 140, 140
   login type, 140, 140
   MOTD type, 140, 140
   multiple-line input mode, 140, 140
   shell type, 140, 140
   single-line input mode, 140, 140
binary transfer mode, 68
boot loader
   startup image file specification, 103
   startup image file specification (in bulk), 103
   startup image file specification (one by one), 103
Boot ROM
   Boot ROM image preload, 102
   software upgrade image type, 99, 99
   software upgrade methods, 101
   software upgrade preparation, 102
   software upgrade system startup, 100
   startup image file specification, 103, 104
   startup image file specification (in bulk), 103
   startup image file specification (one by one), 103
C
calculating
   file digest, 83
CF card partitioning, 86
changing
file system current working directory, 84
FTP user account, 74
checking
emergency shell server connectivity, 133
CLI
command abbreviation, 4
command entry, 3
command history function use, 7
command hotkey use, 5
command keyword alias configuration, 4
command keyword alias use, 4
command keyword hotkey configuration, 5
command line editing, 3
command redisplay, 6
command-line error message, 6
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, 20
device reboot (immediate), 143, 143
device reboot (scheduled), 143, 143
display command output filtering, 9
display command output line numbering, 8
display command output management, 12
display command output save to file, 11
display command output viewing, 12
displaying login, 33
emergency shell file system management, 131
emergency shell system software image retrieval, 132
emergency shell use, 131, 135
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, 33
online help access, 2
output control, 8
output control keys, 8
return to upper-level view from any view, 2
return to user view, 2
running configuration save, 13
software upgrade, 99
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), 75
IPv4 TFTP client configuration, 78
IPv6 TFTP client configuration, 79
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, 4
CLI command keyword alias use, 4
CLI command keyword hotkey configuration, 5
CLI command line editing, 3
CLI command redisplay, 6
CLI string/text type argument value, 4
CLI undo command form, 3
ISSU command series, 109
ISSU install series commands, 114
ISSU performance by issu series commands, 111
line interface. Use CLI
login management command accounting, 40, 41
login management command authorization, 38, 39
commit delay
  running configuration, 95
committing
  ISSU software changes (install series commands), 116
completing
  software upgrade, 103
  software upgrade (in bulk), 103
  software upgrade (one by one), 103
  software upgrade with a warm reboot, 104
compressing
  file, 82, 82
Comware
  software upgrade Boot image type, 99
  software upgrade feature image, 99
  software upgrade image loading, 99
  software upgrade image redundancy, 99
  software upgrade image type, 99
  software upgrade patch image, 99
  software upgrade system image type, 99
configuration
  startup configuration loading, 88
configuration file
  configuration archive, 92
  configuration archive parameters, 93
  configuration archiving (automatic), 94
  configuration rollback, 92, 94
  content, 90
  device configuration types, 88
  displaying, 98
  encryption, 91
  file formats, 89
  FIPS compliance, 90
  format, 90
  main next-startup file backup, 96
  main next-startup file restore, 97
  management, 88
  next-startup configuration file, 96
  next-startup file delete, 97
  restrictions and guidelines, 91
  running configuration archiving (manual), 94
  running configuration save, 91, 92
  startup file selection, 90
configuring
  automatic configuration (DHCP server), 167
  automatic configuration (DNS server), 168
  automatic configuration (HTTP server+Python script), 175
  automatic configuration (HTTP server+Tcl script), 174
  automatic configuration (IRF setup), 176
  automatic configuration (server-based), 169
  automatic configuration (TFTP server), 169
  command keyword alias, 4
  command keyword hotkey, 5
  configuration archive parameters, 93
  configuration commit delay, 95
  configuration rollback, 92
  device airflow direction, 149, 149
  device as IPv4 TFTP client, 78
  device as IPv6 TFTP client, 79
  device banner, 140, 140, 141, 141
  device CPU usage monitoring, 149, 149
  device name, 138, 138
  device temperature alarm threshold, 151, 151
  emergency shell management Ethernet port, 132
  FTP, 68
  FTP basic server parameters, 68
  FTP client (centralized IRF device), 75
  FTP server (centralized IRF device), 70
  FTP server authentication, 69
  FTP server authorization, 69
  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, 20
login management CLI local console/AUX port
login, 19
login management command
accounting, 40, 41
login management command
authorization, 38, 39
login management common VTY line
settings, 26
login management SNMP access control, 37
login management SSH login, 28
login management SSH login on device, 28
login management Telnet login, 22
login management Telnet login on device, 23
login management Telnet login password
authentication, 24
login management Telnet login scheme
authentication, 25
RBAC, 43, 46, 54
RBAC feature group, 48
RBAC for RADIUS authentication user, 56
RBAC local AAA authentication user, 54
RBAC resource access policies, 48
RBAC temporary user role authorization, 52
RBAC temporary user role authorization
(HWTACACS authentication), 59
RBAC temporary user role authorization
(RADIUS authentication), 63
RBAC user role authentication, 53
RBAC user role interface policy, 48
RBAC user role rules, 46
RBAC user role VLAN policy, 49
RBAC user role VPN instance policy, 49
TFTP, 78

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, 20
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, 8
login management SNMP access, 36
login management SSH logins, 35
login management Telnet logsins, 35
login management user access, 35
RBAC configuration, 43, 46

copying
file, 82

copyright statement display, 140, 140

CPU
device CPU usage monitoring, 149
ISSU command series, 109
ISSU methods, 108

creating
file system directory, 84
RBAC user role, 46

D
deactivating
ISSU deactivate operation (install series
commands), 116

decompressing
file, 82, 82
ISSU IPE file, 114

deleting
file, 83
next-startup configuration file, 97
recycle bin file, 83
detecting
device port status detection timer, 149, 149
device
automatic configuration, 165
automatic configuration (DHCP server), 167
automatic configuration (DNS server), 168
automatic configuration (HTTP server+Python script), 175
automatic configuration (HTTP server+Tcl script), 174
automatic configuration (IRF setup), 176
automatic configuration (server-based), 169
automatic configuration (TFTP server), 169
automatic configuration file preparation, 166
automatic configuration start, 169
CLI command history function use, 7
CLI command redisplay, 6
CLI display command output filtering, 9
CLI display command output line numbering, 8
CLI display command output management, 12
CLI display command output save to file, 11
CLI display command output viewing, 12
CLI output control, 8, 8
CLI running configuration save, 13
CLI use, 1
command help information display, 75
configuration types, 88
emergency shell management Ethernet port configuration, 132
emergency shell reboot, 134
emergency shell server access, 133
emergency shell server connectivity check, 133
emergency shell system software image load, 134
emergency shell use, 131, 135
enter system view from user view, 2
file system management, 80
file system storage media formatting, 85
file system storage media management, 85
file system storage media mount, 86
file system storage media repair, 85
file system storage media unmount, 86
FTP basic server parameters configuration, 68
FTP client, 71
FTP client configuration (centralized IRF device), 75
FTP client connection establishment, 71
FTP configuration, 68
FTP connection termination, 75
FTP connection troubleshooting, 74
FTP manual server connection release, 70
FTP server, 68
FTP server authentication, 69
FTP server authorization, 69
FTP server configuration (centralized IRF device), 70
FTP server directory management, 73
FTP server files, 73
FTP server user account change, 74
IPv4 TFTP client configuration, 78
IPv6 TFTP client configuration, 79
ISSU install series commands, 125, 125
login management modem login, 30
login management SNMP device access, 34
login management SSH login configuration on device, 28
login management SSH server login, 30
login management Telnet login device configuration, 23
login management Telnet server login, 28
management, 138
return to upper-level view from any view, 2
return to user view, 2
running configuration, 88
software upgrade, 99
software upgrade system startup, 100
startup configuration, 88
startup configuration loading, 88
storage media CF card partition, 86
storage media USB disk partition, 86
TFTP configuration, 78
device management
  airflow direction configuration, 149, 149
  banner configuration, 140, 140, 141, 141
  banner input modes, 140, 140
  banner types, 140, 140
  configuration, 138, 138
  copyright statement display, 140, 140
  CPU usage monitoring, 149, 149
  device name configuration, 138, 138
  device reboot, 142, 142
  device reboot (immediate), 143, 143
  device reboot (scheduled), 143, 143
  displaying configuration, 154, 154
  maintaining configuration, 154, 154
  memory usage threshold, 150, 150
  password recovery capability disable, 148, 148
  port status detection timer, 149, 149
  restoring factory-default settings and states, 153, 153
  system operating mode, 142, 142
  system time set, 139, 139
  system time source set, 139, 139
  task scheduling, 143, 143, 145, 145
  temperature alarm threshold, 151, 151
transceiver module
diagnosis, 152, 152, 153, 153
verification, 152, 152, 152, 152
USB interface disable, 152, 152
DHCP
  automatic configuration, 165
  automatic configuration (DHCP server), 167
diagnosing
  device transceiver modules, 152, 152, 153, 153
directory
  file system current working directory change, 84
  file system current working directory display, 84
  file system directory creation, 84
  file system directory information display, 84
  file system directory management, 84
  file system directory removal, 84
  file system management, 80
  FTP server directory management, 73
disabling
  CLI output screen pausing, 8
  device password recovery capability, 148, 148
  device USB interface, 152, 152
  login management Telnet login authentication, 23
displaying
  CLI login, 33
  command help information, 75
  configuration files, 98
  device copyright statement, 140, 140
  device management configuration, 154, 154
  emergency shell mode device information, 135
  file system current working directory display, 84
  file system directory information, 84
  file system file information, 81
  file system text file content, 81
  FTP client, 75
  FTP server, 70
  ISSU, 117
  RBAC settings, 54
software upgrade image settings, 105

DNS
  automatic configuration, 165
  automatic configuration (DNS server), 168
  automatic configuration start, 169

E
  editing command line, 3
  emergency shell
    device information display, 135
    device reboot, 134
    file system management, 131
    management Ethernet port configuration, 132
    server access, 133
    server connectivity check, 133
    software upgrade (Comware), 99
    system software image, 132
    system software image load, 134
    use, 131, 135
  enabling
    CLI command redisplay, 6
    configuration archiving (automatic), 94
    configuration encryption, 91
    device copyright statement display, 140
    RBAC default user role, 50
  encrypting
    private key, 91
    public key, 91
  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, 6
  establishing
    FTP client connection, 71

Ethernet
  emergency shell management Ethernet port configuration, 132

F
  factory-default
    restoring factory-default settings and states, 153
  fast saving running configuration, 91, 92
  file
    calculating digest, 83
    compression, 82
    configuration file content, 90
    configuration file format, 90
    configuration file formats, 89
    configuration file management, 88
    copying, 82
    decompression, 82
    deleting from recycle bin, 83
    deletion, 83
    device configuration startup file selection, 90
    FTP server files, 73
    information display, 81
    ISSU IPE file decompressing, 114
    management, 81
    moving, 82
    name format, 80
    next-startup configuration file, 96
    renaming, 82
    restoration, 83
    software upgrade file naming, 99
    system. See file system
    text content display, 81
  file system
    current working directory change, 84
    current working directory display, 84
    directory creation, 84
    directory information display, 84
    directory management, 84
    directory removal, 84
    file compression, 82, 82
File transfer protocol

Use FTP

Client configuration (centralized IRF device), 75
Client connection establishment, 71
Command help information display, 75
Configuration, 68
Connection maintenance, 74
Connection termination, 75
device as client, 71
device as server, 68
displaying client, 75
displaying server, 70
Emergency shell server access, 133
Emergency shell system software image retrieval, 132
IPv4 TFTP client configuration, 78
IPv6 TFTP client configuration, 79
Local server authentication, 69
Local server authorization, 69
Manual server connection release, 70
Remote server authentication, 69
Remote server authorization, 69
Server configuration (centralized IRF device), 70
Server directory management, 73
Server files, 73
TFTP configuration, 78
Troubleshooting connection, 74
User account change, 74

G

Gateway

Automatic configuration, 169

Group

RBAC feature group configuration, 48

H

History

CLI history function, 7
Hotkey (command), 5

HTTP

Automatic configuration (HTTP server+Python script), 175
automatic configuration (HTTP server+Tcl script), 174
automatic configuration (IRF setup), 176
ISSU feature compatible upgrade (issu series commands), 118
ISSU feature incompatible upgrade (issu series commands), 120
ISSU feature rollback (install series commands), 127, 127
ISSU feature rollback (issu series commands), 122
ISSU feature upgrade (install series commands), 125, 125, 128, 128

HW TACACS
  login management command accounting, 40, 41
  RBAC temporary user role authorization, 59

I
  identifying
    CLI user line, 17

image
  emergency shell system software image retrieval, 132
  ISSU inactive software image removal (install series commands), 117
  ISSU patch image (install series commands), 115
  ISSU software image (install series commands), 114
  ISSU software image upgrade (install series commands), 114
  software upgrade Boot ROM image type, 99
  software upgrade Comware Boot image type, 99
  software upgrade Comware image loading, 99
  software upgrade Comware image redundancy, 99
  software upgrade Comware image type, 99
  software upgrade Comware system image type, 99
  startup image file specification, 103, 104
  startup image file specification (in bulk), 103
  startup image file specification (one by one), 103

Import
  extended Python API, 160
  incoming banner type, 140, 140

In-Service Software Upgrade. Use ISSU install series commands
  ISSU feature uninstall, 115
  ISSU patch image uninstall, 115
  ISSU software configuration rollback, 115
  ISSU software image installation, 114
  ISSU software image upgrade, 114
  installing, 114, See also install series commands
  ISSU software images (install series commands), 114
  interface, 14, See also line

IP
  FTP configuration, 68
  TFTP configuration, 78
  IPE file (ISSU), 114

IPv4
  emergency shell management Ethernet port configuration, 132
  emergency shell server access, 133
  emergency shell server connectivity check, 133
  FTP client connection establishment, 71
  TFTP client configuration, 78

IPv6
  emergency shell management Ethernet port configuration, 132
  emergency shell server access, 133
  emergency shell server connectivity check, 133
  FTP client connection establishment, 71
  TFTP client configuration, 79

IRF
  automatic configuration (IRF setup), 176
  Boot ROM image preload, 102
  emergency shell device reboot, 134
emergency shell use, 131, 135
FTP client configuration (centralized IRF device), 75
FTP server configuration (centralized IRF device), 70
ISSU, 108
ISSU (install series commands), 114
ISSU feature compatible upgrade (issu series commands), 118
ISSU feature incompatible upgrade (issu series commands), 120
ISSU feature rollback (install series commands), 122
ISSU feature rollback (issu series commands), 127, 127
ISSU feature upgrade (install series commands), 125, 125, 128, 128
ISSU for multichassis IRF fabric, 111
ISSU for single-chassis IRF fabric, 113
ISSU install series commands, 125, 125
ISSU issu series commands, 118
ISSU methods, 108
ISSU overview, 108
ISSU performance by issu series commands, 111
ISSU software image verification (install series commands), 116
non-ISSU software upgrade method, 105
software activate/deactivate (install series commands), 116
software configuration rollback (install series commands), 115
software image (install series commands), 114
software image upgrade (install series commands), 114
software image verification (install series commands), 116
software upgrade Comware image method, 101
software upgrade non-ISSU method, 101

ISSU

Boot ROM image preload, 102
command series, 109
displaying, 117
equipment shell use, 131, 135
feature compatible upgrade (issu series commands), 118
feature incompatible upgrade (issu series commands), 120
feature rollback (install series commands), 127, 127
feature rollback (issu series commands), 122
feature uninstall (install series commands), 115
feature upgrade (install series commands), 125, 125, 128, 128
inactive software image removal (install series commands), 117
install series commands, 114, 125, 125
IPE file decompression (install series commands), 114
issu series commands, 111, 118
maintaining, 117
methods, 108
multichassis IRF fabric, 111
non-ISSU software upgrade, 105
overview, 108
patch image uninstall (install series commands), 115
single-chassis IRF fabric, 113
software activate/deactivate (install series commands), 116
software configuration rollback (install series commands), 115
software image (install series commands), 114
software image upgrade (install series commands), 114
software image verification (install series commands), 116
software upgrade Comware image method, 101
software upgrade non-ISSU method, 101
software upgrade procedure, 102
troubleshooting, 118
troubleshooting failure to execute, 118
K
key
  command hotkey, 5
keyword alias configuration, 4
L
LAN
  device management, 138
legal banner type, 140, 140
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, 26
loading
  emergency shell system software image, 134
local
  RBAC local AAA authentication user configuration, 54
  RBAC user role local AAA authentication, 50
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, 20
  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, 30
  login management SSH login, 28
  login management SSH login configuration on device, 28
  login management SSH server login, 30
  login management Telnet login, 22
  login management Telnet login device configuration, 23
  login management Telnet login max number concurrent users, 26
  login management Telnet login none authentication, 23
  login management Telnet login password authentication, 24
  login management Telnet login scheme authentication, 25
  login management Telnet server login, 28
  login management VTY common line settings, 26
login
  device banner login type, 140, 140
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, 20
  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, 33
DSCP value for outgoing Telnet packet, 26
maintaining CLI login, 33
modem login, 30
overview, 14
SNMP access control, 37
SNMP device access, 34
SSH login, 28
SSH login control, 35
SSH login on device, 28
SSH server login, 30
Telnet login, 22
Telnet login control, 35, 35
Telnet login device configuration, 23
Telnet login max number concurrent users, 26
Telnet login none authentication, 23
Telnet login password authentication, 24
Telnet login scheme authentication, 25
Telnet server login, 28
user access control, 35
user lines, 17
VTY common line settings, 26

M

main
software upgrade image set, 99
main next-startup configuration file, 96, 97
maintaining
CLI login, 33
device management configuration, 154, 154
FTP connection, 74
ISSU, 117
RBAC settings, 54
software upgrade image settings, 105
management Ethernet port configuration, 132
managing
CLI display command output, 12
configuration files, 88
device. See device management
emergency shell file system, 131
file system, 80

file system directories, 84
file system files, 81
file system storage media, 85
FTP server directories, 73
manual
FTP server connection release, 70
memory
device memory usage threshold, 150, 150
message
CLI command line error message, 6
message-of-the-day (MOTD) banner type, 140, 140
MIB
login management SNMP device access, 34
mode
device system operating mode, 142, 142
file system file/folder alert operation mode, 87
file system file/folder quiet operation mode, 87
FTP active (PORT) operating mode, 68
FTP ASCII transfer mode, 68
FTP binary transfer mode, 68
FTP passive (PASV) operating mode, 68
login management none CLI authentication, 18
login management password CLI authentication, 18
login management scheme CLI authentication, 18
modem
login, 30
login management overview, 14
module
device transceiver module
diagnosis, 152, 152, 153, 153
device transceiver module
verification, 152, 152, 152, 152
monitoring
device CPU usage, 149
mounting
file system storage media, 86
moving
file, 82
MPU
emergency shell device reboot, 134
emergency shell use, 131, 135
ISSU, 108
ISSU (install series commands), 114
ISSU (issu series commands), 111
ISSU methods, 108
ISSU overview, 108
multiple-line banner input mode, 140, 140

N
naming
device name configuration, 138, 138
file name formats, 80
file rename, 82
software upgrade files, 99
storage media naming rules, 80

network
automatic configuration (DHCP server), 167
automatic configuration (DNS server), 168
automatic configuration (HTTP server+Python script), 175
automatic configuration (HTTP server+Tcl script), 174
automatic configuration (IRF setup), 176
automatic configuration (TFTP server), 169
automatic configuration file preparation, 166
automatic configuration gateway, 169
automatic configuration start, 169
command help information display, 75
device airflow direction configuration, 149, 149
device as FTP client, 71
device as FTP server, 68
device banner configuration, 140, 140
device banner input modes, 140, 140
device banner types, 140, 140
device copyright statement display, 140, 140
device CPU usage monitoring, 149, 149
device factory-default settings and states, 153
device management task scheduling, 143, 143, 145, 145
device memory usage threshold, 150, 150
device name configuration, 138, 138
device password recovery capability disable, 148, 148
device port status detection timer, 149, 149
device reboot, 142, 142
device reboot (immediate), 143, 143
device reboot (scheduled), 143, 143
device system operating mode, 142, 142
device system time set, 139, 139
device system time source set, 139, 139
device temperature alarm threshold, 151, 151
device transceiver module diagnosis, 152, 152, 153, 153
device transceiver module verification, 152, 152, 152, 152
device USB interface disable, 152, 152
emergency shell device reboot, 134
emergency shell management Ethernet port configuration, 132
emergency shell server access, 133
emergency shell system software image load, 134
file system directory management, 84
file system file management, 81
file system storage media management, 85
FTP basic server parameters configuration, 68
FTP client configuration (centralized IRF device), 75
FTP client connection establishment, 71
FTP connection termination, 75
FTP connection troubleshooting, 74
FTP manual server connection release, 70
FTP server authentication, 69
FTP server authorization, 69
FTP server configuration (centralized IRF device), 70
FTP server directory management, 73
FTP server files, 73
FTP user account change, 74
IPv4 TFTP client configuration, 78
IPv6 TFTP client configuration, 79
ISSU command series, 109
ISSU feature (install series commands), 115
ISSU for multichassis IRF fabric, 111
ISSU for single-chassis IRF fabric, 113
ISSU inactive software image removal (install series commands), 117
ISSU IPE file decompressing (install series commands), 114
ISSU patch image (install series commands), 115
ISSU preparation, 109
ISSU software activate/deactivate (install series commands), 116
ISSU software changes commit (install series commands), 116
ISSU software configuration rollback (install series commands), 115
ISSU software image (install series commands), 114
ISSU software image upgrade (install series commands), 114
ISSU software image verification (install series commands), 116
login management command accounting, 40, 41
login management command authorization, 38, 39
login management SNMP access control, 36, 37
login management SSH login control, 35
login management Telnet login control, 35, 35
RBAC default user role, 50
RBAC feature group configuration, 48
RBAC local AAA authentication user configuration, 54
RBAC permission assignment, 43
RBAC RADIUS authentication user configuration, 56
RBAC resource access policies, 48
RBAC temporary user role authorization, 52, 54
RBAC temporary user role authorization (HWTACACS authentication), 59
RBAC temporary user role authorization (RADIUS authentication), 63
RBAC user role assignment, 45, 50
RBAC user role authentication, 53
RBAC user role creation, 46
RBAC user role interface policy, 48
RBAC user role local AAA authentication, 50
RBAC user role non-AAA authentication, 51
RBAC user role remote AAA authentication, 50
RBAC user role rule configuration, 46
RBAC user role VPN instance policy, 49
RBAC user role VPN instance policy, 49
network management
automatic configuration, 165
automatic configuration (server-based), 169
CLI use, 1
configuration file management, 88
device management, 138, 138, 138
emergency shell use, 131, 135
extended Python API, 160
extended Python API functions, 160
extended Python API import, 160
extended Python API use, 160
file system management, 80
FTP configuration, 68
ISSU, 108
ISSU (install series commands), 114
ISSU feature compatible upgrade (issu series commands), 118
ISSU feature incompatible upgrade (issu series commands), 120
ISSU feature rollback (install series commands), 127, 127
ISSU feature rollback (issu series commands), 122
ISSU feature upgrade (install series commands), 125, 125, 128, 128
ISSU install series commands, 125, 125
ISSU issu series commands, 118
ISSU methods, 108
ISSU overview, 108
ISSU performance by issu series commands, 111
login management SNMP device access, 34
login management user access control, 35
non-ISSU software upgrade, 105
Python use, 158, 158
RBAC configuration, 43, 46, 54
software upgrade, 99
software upgrade with a warm reboot, 106
Tcl use, 156
TFTP configuration, 78
next-startup configuration file, 97
NMS
login management SNMP device access, 34
non-AAA authentication (RBAC), 51
non-AAA authorization (RBAC), 45
none
login management CLI authentication mode, 18
login management CLI console/AUX none authentication, 19
login management Telnet login none authentication, 23
numbering
CLI display command output lines, 8
O
obtaining

emergency shell system software image, 132
RBAC temporary user role authorization, 54
online
CLI online help access, 2
outputting
CLI display command output filtering, 9
CLI display command output management, 12
CLI display command output view, 12
CLI display comment output to file, 11
CLI output control, 8
CLI output control keys, 8
CLI output line numbering, 8
P
parameter
configuration archive parameters, 93
device management, 138, 138
FTP basic server parameters configuration, 68
partitioning
storage media CF card partition, 86
storage media USB disk, 86
passive
FTP passive (PASV) operating mode, 68
password
device password recovery capability disable, 148, 148
login management CLI authentication mode, 18
login management CLI console/AUX password authentication, 20
login management Telnet login password authentication, 24
login management Telnet login scheme authentication, 25
patch
ISSU patch image, 115
software upgrade Comware patch image, 99
pausing between CLI output screens, 8
performing
ISSU, 108
ISSU (install series commands), 114
ISSU by issu series commands, 111
ISSU feature compatible upgrade (issu series commands), 118
ISSU feature incompatible upgrade (issu series commands), 120
ISSU feature rollback (install series commands), 127, 127
ISSU feature rollback (issu series commands), 122
ISSU feature upgrade (install series commands), 125, 125, 128, 128
ISSU for multichassis IRF fabric, 111
ISSU for single-chassis IRF fabric, 113
ISSU install series commands, 125, 125
ISSU issu series commands, 118
permitting
RBAC permission assignment, 43
RBAC user role assignment, 45
policy
RBAC interface access policy, 44
RBAC resource access policies, 48
RBAC user role assignment, 50
RBAC user role interface policy, 48
RBAC user role local AAA authentication, 50
RBAC user role non-AAA authentication, 51
RBAC user role remote AAA authentication, 50
RBAC user role VLAN policy, 49
RBAC user role VPN instance policy, 49
RBAC VLAN access policy, 44
RBAC VPN instance access policy, 44
port
device status detection timer, 149, 149
emergency shell management Ethernet port configuration, 132
preloading
Boot ROM image, 102
preparing
ISSU, 109
software upgrade (non-ISSU), 102
procedure
abbreviating CLI command, 4
aborting ISSU software activate/deactivate (install series commands), 116
accessing CLI online help, 2
accessing server with emergency shell, 133
archiving running configuration (manual), 94
assigning RBAC local AAA authentication user role, 50
assigning RBAC non-AAA authentication user role, 51
assigning RBAC remote AAA authentication user role, 50
assigning RBAC user role, 50
backing up main next-startup configuration file, 96
calculating file digest, 83
changing current working directory, 84
changing FTP user accounts, 74
checking emergency shell server connectivity with emergency shell, 133
committing ISSU software changes (install series commands), 116
completing software upgrade, 103
completing software upgrade (in bulk), 103
completing software upgrade (one by one), 103
completing software upgrade with a warm reboot, 104
compressing file, 82, 82
configuring automatic configuration (DHCP server), 167
configuring automatic configuration (DNS server), 168
configuring automatic configuration gateway, 169
configuring CLI command hotkey, 5
configuring CLI command keyword alias, 4
configuring configuration archive parameters, 93
configuring configuration commit delay, 95
configuring configuration rollback, 92
configuring device airflow direction, 149, 149
configuring device as IPv4 TFTP client, 78
configuring device as IPv6 TFTP client, 79
configuring device banner, 140, 140, 141, 141
configuring device CPU usage monitoring, 149
configuring device name, 138, 138
configuring device temperature alarm threshold, 151, 151
configuring emergency shell management Ethernet port, 132
configuring FTP basic server parameters, 68
configuring FTP client (centralized IRF device), 75
configuring FTP server (centralized IRF device), 70
configuring FTP server local authentication, 69
configuring FTP server local authorization, 69
configuring FTP server remote authentication, 69
configuring FTP server remote authorization, 69
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, 20
configuring login management CLI local console/AUX port login, 19
configuring login management command accounting, 40, 41
configuring login management command authorization, 38, 39
configuring login management SNMP access control, 37
configuring login management SSH login, 28
configuring login management SSH login on device, 28
configuring login management Telnet login, 22
configuring login management Telnet login on device, 23
configuring login management Telnet login password authentication, 24
configuring login management Telnet login scheme authentication, 25
configuring login management VTY common line settings, 26
configuring RBAC, 46, 54
configuring RBAC feature group, 48
configuring RBAC for RADIUS authentication user, 56
configuring RBAC local AAA authentication user, 54
configuring RBAC resource access policies, 48
configuring RBAC temporary user role authorization, 52
configuring RBAC temporary user role authorization (HWTACACS authentication), 59
configuring RBAC temporary user role authorization (RADIUS authentication), 63
configuring RBAC user role authentication, 53
configuring RBAC user role interface policy, 48
configuring RBAC user role rules, 46
configuring RBAC user role VLAN policy, 49
configuring RBAC user role VPN instance policy, 49
controlling CLI output, 8, 8
controlling login management SNMP access, 36
controlling login management SSH logins, 35
controlling login management Telnet logins, 35, 35
copying file, 82
creating directory, 84
creating RBAC user role, 46
decompressing file, 82, 82
decompressing ISSU IPE file (install series commands), 114
deleting file, 83
deleting file from recycle bin, 83
deleting next-startup configuration file, 97
diagnosing device transceiver module, 152, 152, 153, 153
disabling device USB interface, 152, 152
disabling CLI console/AUX authentication, 19
disabling CLI output screen pausing, 8
disabling device password recovery capability, 148, 148
disabling login management Telnet login authentication, 23
displaying CLI login, 33
displaying command help information, 75
displaying configuration files, 98
displaying current working directory, 84
displaying device management configuration, 154, 154
displaying directory information, 84
displaying emergency shell mode device information, 135
displaying file information, 81
displaying FTP client, 75
displaying FTP server, 70
displaying ISSU, 117
displaying RBAC settings, 54
displaying software upgrade image settings, 105
displaying text file content, 81
editing CLI command line, 3
enabling CLI redisplay of entered-but-not-submitted command, 6
enabling configuration archiving (automatic), 94
enabling configuration encryption, 91
enabling device copyright statement display, 140, 140
enabling RBAC default user role, 50
entering CLI command, 3
entering CLI string/text type argument value, 4
entering Python shell, 158
entering system view from user view, 2
establishing FTP client connection, 71
executing Comware commands in Tcl configuration view, 156
executing Python script, 158
filtering CLI display command output, 9
formatting file system storage media, 85
installing ISSU software images (install series commands), 114
loading emergency shell system software image, 134
logging in through modems, 30
logging in to SSH server (device login), 30
logging in to Telnet server (device login), 28
maintaining CLI login, 33
maintaining device management configuration, 154, 154
maintaining FTP connection, 74
maintaining ISSU, 117
maintaining RBAC settings, 54
maintaining software upgrade image settings, 105
managing CLI display command output, 12
managing file system (emergency shell), 131
managing file system directories, 84
managing file system files, 81
managing file system storage media, 85
managing FTP server directories, 73
manually releasing FTP server connection, 70
mounting file system storage media, 86
moving file, 82
numbering CLI display command output lines, 8
obtaining emergency shell system software image, 132
obtaining RBAC temporary user role authorization, 54
partitioning CF card, 86
partitioning USB disk, 86
pausing between CLI output screens, 8
performing ISSU, 108
performing ISSU (install series commands), 114
performing ISSU feature compatible upgrade (issu series commands), 118
performing ISSU feature incompatible upgrade (issu series commands), 120
performing ISSU feature rollback (install series commands), 127, 127
performing ISSU feature rollback (issu series commands), 122
performing ISSU feature upgrade (install series commands), 125, 125, 128, 128
performing ISSU for multichassis IRF fabric, 111
performing ISSU for single-chassis IRF fabric, 113
performing ISSU install series commands, 125, 125
performing ISSU issu series commands, 118
preloading Boot ROM image, 102
preparing automatic configuration files, 166
preparing for software upgrade (non-ISSU), 102
rebooting device, 142, 142
rebooting device (immediate), 143, 143
rebooting device (scheduled), 143, 143
rebooting device with emergency shell, 134
removing directory, 84
removing ISSU inactive software image (install series commands), 117
renaming file, 82
repairing file system storage media, 85
restoring factory-default settings and states, 153
restoring file, 83
restoring main next-startup configuration file, 97
returning to upper-level view from any view, 2
returning to user view, 2
rolling back configuration, 94
rolling back ISSU software configuration (install series commands), 115
saving CLI display command output to file, 11
saving CLI running configuration, 13
saving running configuration, 91, 92
scheduling device management task, 143, 143, 145, 145
setting automatic configuration interface, 169
setting device memory usage threshold, 150, 150
setting device port status detection timer, 149, 149
setting device system operating mode, 142, 142
setting device system time, 139, 139
setting DSCP value for outgoing Telnet packet, 26
setting file/folder operation mode, 87
setting login management Telnet login max number concurrent users, 26
specifying device system time source, 139, 139
specifying next-startup configuration file, 96
specifying startup image file, 103, 104
specifying startup image file (in bulk), 103
specifying startup image file (one by one), 103
terminating FTP connection, 75
troubleshooting FTP connection, 74
troubleshooting ISSU, 118
troubleshooting ISSU failure to execute, 118
troubleshooting RBAC local user access permissions, 66
troubleshooting RBAC login attempts by RADIUS users fail, 66
understanding CLI command-line error message, 6
uninstalling ISSU feature (install series commands), 115
uninstalling ISSU patch images (install series commands), 115
unmounting file system storage media, 86
upgrading ISSU software images (install series commands), 114
upgrading software, 102
upgrading software with a warm reboot, 106
upgrading software with non-ISSU method, 105
using CLI command history function, 7
using CLI command hotkey, 5
using CLI command keyword alias, 4
using CLI undo command form, 3
using emergency shell, 135
using Python, 158
using Tcl to configure the device, 156
verifying device transceiver module, 152, 152, 152, 152
verifying ISSU software image (install series commands), 116
viewing CLI display command output, 12
working with FTP server files, 73

Python
  automatic configuration (HTTP server+Python script), 175
  automatic configuration (IRF setup), 176
  extended API, 160
  extended API functions, 160
  script, 158
  shell, 158
  use, 158, 158

R
RADIUS
  RBAC RADIUS authentication user configuration, 56
  RBAC temporary user role authorization, 63

RBAC
  AAA authorization, 45
  configuration, 43, 46, 54
  default user role, 50
  feature group configuration, 48
  FIPS compliance, 46
  local AAA authentication user configuration, 54
  non-AAA authorization, 45
  permission assignment, 43
  predefined user roles, 44
  RADIUS authentication user configuration, 56
  resource access policies, 44, 48
  rule configuration restrictions, 47
  settings display, 54
  settings maintain, 54
  temporary user role authorization, 54
  temporary user role authorization (HWTACACS authentication), 59
  temporary user role authorization (RADIUS authentication), 63
  temporary user role authorization configuration, 52
  troubleshoot, 66
  troubleshoot local user access permissions, 66
  troubleshoot login attempts by RADIUS users fail, 66
  user role assignment, 45, 50
  user role authentication, 53
  user role creation, 46
  user role interface policy, 48
  user role local AAA authentication, 50
  user role non-AAA authentication, 51
  user role remote AAA authentication, 50
  user role rule configuration, 46
  user role rules, 43
  user role VLAN policy, 49
  user role VPN instance policy, 49
  rebooting
    device, 142, 142
    device (immediate), 143, 143
    device (scheduled), 143, 143
    emergency shell device reboot, 134
remote
  RBAC user role AAA authentication, 50
removing
  file system directory, 84
  ISSU inactive software image (install series commands), 117
renaming
  file, 82
repairing
  file system storage media, 85
resource
  RBAC resource access policies, 48
restoring
  factory-default settings and states, 153
  file, 83
  main next-startup configuration file, 97
restrictions
  partitioning storage media CF cards, 86
  partitioning storage media USB disks, 86
  RBAC rule configuration, 47
  Tcl, 156
unmounting file system storage media, 86
returning
  to upper-level view from any view, 2
  to user view, 2
role
  RBAC default user role, 50
  RBAC predefined user roles, 44
  RBAC temporary user role authorization, 52, 54
  RBAC user role assignment, 45, 50
  RBAC user role authentication, 53
  RBAC user role creation, 46
  RBAC user role interface policy, 48
  RBAC user role local AAA authentication, 50
  RBAC user role non-AAA authentication, 51
  RBAC user role remote AAA authentication, 50
  RBAC user role rule configuration, 46
  RBAC user role VLAN policy, 49
  RBAC user role VPN instance policy, 49
role-based access control. *Use RBAC*
rolling back
  configuration, 92, 94
  ISSU feature rollback (install series commands), 127, 127
  ISSU feature rollback (issu series commands), 122
  ISSU software configuration (install series commands), 115
routing
  FTP configuration, 68
  TFTP configuration, 78, 78
rule
  file system storage media naming, 80
  RBAC command rule, 43
  RBAC feature execute rule, 43
  RBAC feature group rule, 43
  RBAC feature read rule, 43
  RBAC feature write rule, 43
  RBAC OID rule, 43
  RBAC user role rule configuration, 46
  RBAC Web menu rule, 43
  RBAC XML element rule, 43
running configuration
  archiving, 92
  archiving (manual), 94
  CLI save, 13
  commit delay, 95
  device, 88
  encryption, 91
  rollback, 92
  saving (fast mode), 91, 92
  saving (safe mode), 91, 92
S
  safe saving running configuration, 91, 92
saving
  CLI display command output to file, 11
  CLI running configuration, 13
  running configuration, 91, 92
scheduling
  device management task, 143, 143, 145, 145
  device reboot (scheduled), 143, 143
scheme
login management CLI authentication mode, 18
login management CLI console/AUX common user line settings, 21
login management CLI console/AUX scheme authentication, 20

script
extended Python API, 160
extended Python API functions, 160
Python, 158, 158, 158

scripting
automatic configuration (HTTP server+Python script), 175
automatic configuration (HTTP server+Tcl script), 174

security
configuration encryption, 91
device USB interface disable, 152, 152
login management command accounting, 40, 41
login management command authorization, 38, 39
login management SNMP access control, 36, 37
login management SSH login control, 35
login management Telnet login control, 35, 35
login management user access control, 35
RBAC configuration, 43, 46, 54
RBAC default user role, 50
RBAC feature group configuration, 48
RBAC local AAA authentication user configuration, 54
RBAC permission assignment, 43
RBAC RADIUS authentication user configuration, 56
RBAC resource access policies, 48
RBAC temporary user role authorization, 52, 54
RBAC temporary user role authorization (HWTACACS authentication), 59
RBAC temporary user role authorization (RADIUS authentication), 63
RBAC user role assignment, 45, 50
RBAC user role authentication, 53
RBAC user role creation, 46
RBAC user role interface policy, 48
RBAC user role local AAA authentication, 50
RBAC user role non-AAA authentication, 51
RBAC user role remote AAA authentication, 50
RBAC user role rule configuration, 46
RBAC user role VLAN policy, 49
RBAC user role VPN instance policy, 49

selecting
automatic configuration interface, 169

server
automatic configuration (DHCP server), 167
automatic configuration (DNS server), 168
automatic configuration (file server), 166
automatic configuration (HTTP server+Python script), 175
automatic configuration (HTTP server+Tcl script), 174
automatic configuration (IRF setup), 176
automatic configuration (server-based), 169
automatic configuration (TFTP server), 169
automatic configuration file preparation, 166
automatic configuration gateway, 169
automatic configuration start, 169
emergency shell server connectivity check, 133
FTP server directory management, 73

setting
device memory usage threshold, 150, 150
device port status detection timer, 149, 149
device system operating mode, 142, 142
device system time, 139, 139
DSCP value for outgoing Telnet packet, 26
file/folder operation mode, 87
login management Telnet login max number concurrent users, 26
shell
- Python, 158
- shell banner type, 140, 140
- single-line banner input mode, 140, 140

SNMP
- access control, 36, 37
- access management overview, 14
- device access, 34

SNMPv1
- login management SNMP device access, 34

SNMPv2
- login management SNMP device access, 34

SNMPv3
- login management SNMP device access, 34

software
- emergency shell system software image load, 134
- emergency shell system software image retrieval, 132
- emergency shell use, 131, 135
- upgrade. See software upgrade

software upgrade
- Boot ROM image preload, 102
- Boot ROM image type, 99
- CLI method, 99
- completion, 103
- completion (in bulk), 103
- completion (one by one), 103
- completion with a warm reboot, 104
- Comware Boot image type, 99
- Comware feature image, 99
- Comware image loading, 99
- Comware image redundancy, 99
- Comware image type, 99
- Comware patch image, 99
- Comware system image type, 99
- file naming, 99
- image settings display, 105
- image settings maintain, 105
- ISSU, 108
- ISSU (install series commands), 114
- ISSU feature compatible upgrade (issu series commands), 118
- ISSU feature incompatible upgrade (issu series commands), 120
- ISSU feature rollback (install series commands), 127, 127
- ISSU feature rollback (issu series commands), 122
- ISSU feature upgrade (install series commands), 125, 125, 128, 128
- ISSU inactive software image removal (install series commands), 117
- ISSU install series commands, 125, 125
- ISSU IPE file decompressing (install series commands), 114
- ISSU issu series commands, 118
- ISSU overview, 108
- ISSU performance by issu series commands, 111
- ISSU preparation, 109
- ISSU software configuration rollback (install series commands), 115
- ISSU software image (install series commands), 114
- ISSU software image upgrade (install series commands), 114
- methods, 101
- non-ISSU upgrade, 105
- non-ISSU upgrade preparation, 102
- overview, 99
- procedure, 102
- startup image file specification, 103, 104
- startup image file specification (in bulk), 103
- startup image file specification (one by one), 103
- system startup, 100
- upgrade with a warm reboot, 106
- specifying
  - device system time source, 139, 139
- next-startup configuration file, 96
SSH
  login, 28
  login configuration on device, 28
  login control, 35
  login management overview, 14
  server login, 30
starting
  automatic configuration, 169
starting up
  Boot ROM image preload, 102
  software upgrade procedure, 102
  software upgrade system startup, 100
  software upgrade with a warm reboot, 106
  software upgrade with non-ISSU method, 105
startup image file specification, 103, 104
  startup image file specification (in bulk), 103
  startup image file specification (one by one), 103
startup configuration loading, 88
  device configuration startup file selection, 90
  device configuration), 88
  next-startup configuration file, 96
storage media
  CF card partition, 86, 86
  file system management, 80
  file system storage media naming rules, 80
  formatting, 85
  management, 85
  mounting, 86
  repair, 85
  unmounting, 86
  USB disk partition, 86, 86
string type argument value, 4
system
  software upgrade Comware feature image, 99
  software upgrade Comware image loading, 99
  software upgrade Comware image redundancy, 99
  software upgrade Comware patch image, 99
  software upgrade Comware system image type, 99
  software upgrade startup process, 100
system administration
  automatic configuration, 165
  automatic configuration (DHCP server), 167
  automatic configuration (DNS server), 168
  automatic configuration (HTTP server+Python script), 175
  automatic configuration (HTTP server+Tcl script), 174
  automatic configuration (IRF setup), 176
  automatic configuration (server-based), 169
  automatic configuration (TFTP server), 169
  automatic configuration file preparation, 166
  automatic configuration gateway, 169
  automatic configuration interface selection, 169
  automatic configuration start, 169
  CLI command abbreviation, 4
  CLI command entry, 3
  CLI command history function use, 7
  CLI command hotkey configuration, 5
  CLI command hotkey use, 5
  CLI command keyword alias configuration, 4
  CLI command keyword alias use, 4
  CLI command line editing, 3
  CLI command redisplay, 6
  CLI command-line error message, 6
  CLI display command output filtering, 9
  CLI display command output line numbering, 8
  CLI display command output management, 12
  CLI display command output save to file, 11
  CLI display command output viewing, 12
  CLI online help access, 2
  CLI output control, 8, 8
  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, 93
configuration archiving (automatic), 94
configuration file encryption, 91
configuration file formats, 89
configuration file main next-startup file backup, 96
configuration file main next-startup file restore, 97
configuration file management, 88
configuration file next-startup file delete, 97
configuration rollback, 92, 94
device airflow direction configuration, 149, 149
device banner configuration, 140, 140, 141, 141
device banner input modes, 140, 140
device banner types, 140, 140
device configuration startup file selection, 90
device copyright statement display, 140, 140
device CPU usage monitoring, 149, 149
device factory-default settings and states, 153
device management, 138, 138, 138
device management task scheduling, 143, 143, 145, 145
device memory usage threshold, 150, 150
device name configuration, 138, 138
device password recovery capability disable, 148, 148
device port status detection timer, 149, 149
device reboot, 142, 142
device reboot (immediate), 143, 143
device reboot (scheduled), 143, 143
device system operating mode, 142, 142
device system time set, 139, 139
device system time source set, 139, 139
device temperature alarm threshold, 151, 151
device transceiver module diagnosis, 152, 152, 153, 153
device transceiver module verification, 152, 152, 152, 152
device USB interface disable, 152, 152
emergency shell file system management, 131
emergency shell server connectivity check, 133
emergency shell system software image retrieval, 132
emergency shell use, 131, 135
enter system view from user view, 2
executing Comware commands, 156
extended Python API, 160
extended Python API functions, 160
extended Python API import, 160
extended Python API use, 160
file system directory management, 84
file system file management, 81
file system file name formats, 80
file system management, 80
file system storage media management, 85
file system storage media naming rules, 80
FTP configuration, 68
ISSU command series, 109
ISSU feature (install series commands), 115
ISSU feature compatible upgrade (issu series commands), 118
ISSU feature incompatible upgrade (issu series commands), 120
ISSU feature rollback (install series commands), 127, 127
ISSU feature rollback (issu series commands), 122
ISSU feature upgrade (install series commands), 125, 125, 128, 128
ISSU for multichassis IRF fabric, 111
ISSU for single-chassis IRF fabric, 113
ISSU inactive software image removal (install series commands), 117
ISSU install series commands, 125, 125
task scheduling (device management), 143, 143, 145, 145

Tcl
  automatic configuration (HTTP server+Tcl script), 174
  configuring the device, 156
  executing Comware commands, 156
  restrictions, 156
  use, 156

TCP
  device as FTP client, 71
  device as FTP server, 68
  FTP client connection establishment, 71
  FTP configuration, 68
  IPv4 TFTP client configuration, 78
  IPv6 TFTP client configuration, 79
  TFTP configuration, 78

Telnet
  DSCP value for outgoing packet, 26
  login, 22
  login control, 35
  login device configuration, 23
  login management overview, 14
  login max number concurrent users, 26
  login none authentication, 23
  login password authentication, 24
  login scheme authentication, 25
  server login, 28
  VTY common line settings, 26

temperature
  device temperature alarm threshold, 151, 151

terminating
  FTP connection, 75

TFTP, 78, See also FTP
  automatic configuration, 165
  automatic configuration (file server), 166
  automatic configuration (server-based), 169

UDP
  automatic configuration (TFTP server), 169
  automatic configuration start, 169
  configuration, 78
  emergency shell server access, 133
  emergency shell system software image retrieval, 132
  IPv4 client configuration, 78
  IPv6 client configuration, 79

main next-startup configuration file, 96, 97

threshold
  device memory usage, 150, 150
  device temperature threshold alarm, 151, 151

time
  device system time set, 139, 139
  device system time source set, 139, 139

timer
  device port status detection, 149, 149

tool command language. Use Tcl

transceiver
  device module diagnosis, 152, 152, 153, 153
  device module verification, 152, 152, 152

Trivial File Transfer Protocol. Use TFTP

troubleshooting
  FTP connection, 74
  ISSU, 118
  ISSU failure to execute, 118
  RBAC, 66
  RBAC local user access permissions, 66
  RBAC login attempts by RADIUS users fail, 66

U
  undo command form, 3

uninstalling
  ISSU feature (install series commands), 115
  ISSU patch images (install series commands), 115

unmounting
  file system storage media, 86

upgrading
ISSU feature compatible upgrade (issu series commands), 118
ISSU feature incompatible upgrade (issu series commands), 120
ISSU feature upgrade (install series commands), 125, 125, 128, 128
ISSU software images (install series commands), 114
software. See software upgrade

USB
device USB interface disable, 152, 152
disk partitioning, 86

user
interface, 14, See also user line
interface login management VTY common line settings, 26

user access
RBAC configuration, 43, 46, 54
RBAC feature group configuration, 48
RBAC local AAA authentication user configuration, 54
RBAC permission assignment, 43
RBAC predefined user roles, 44
RBAC RADIUS authentication user configuration, 56
RBAC resource access policies, 48
RBAC temporary user role authorization, 52, 54
RBAC temporary user role authorization (HWTACACS authentication), 59
RBAC temporary user role authorization (RADIUS authentication), 63
RBAC user role assignment, 45, 50
RBAC user role authentication, 53
RBAC user role creation, 46
RBAC user role interface policy, 48
RBAC user role local AAA authentication, 50
RBAC user role non-AAA authentication, 51
RBAC user role remote AAA authentication, 50
RBAC user role rule configuration, 46
RBAC user role rules, 43
RBAC user role VLAN policy, 49
RBAC user role VPN instance policy, 49

user access control
login control, 35
login management command accounting, 40, 41
login management command authorization, 38, 39
login management SNMP access control, 36, 37
login management SSH login control, 35
login management Telnet login control, 35, 35

using
automatic configuration, 165
CLI, 1
command history function, 7
command hotkey, 5
command keyword alias, 4
device as FTP client, 71
device as FTP server, 68
Extended Python API, 160, 160
Python, 158, 158
Tcl, 156
undo command form, 3

V
verifying
device transceiver modules, 152, 152, 152
ISSU software image (install series commands), 116

viewing
CLI display command output, 12

VLAN
RBAC user role VLAN policy, 49
RBAC VLAN access policy, 44

VPN
RBAC user role VPN instance policy, 49
RBAC VPN instance access policy, 44

VTY line settings, 26
W

working with

FTP server files, 73