2 Basic Configurations Commands

2.1 CLI Overview Commands

2.1.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

2.1.2 assistant task

Function

The **assistant task** command creates an assistant task.

The **undo assistant task** command deletes an assistant task.

By default, no assistant task is created.

Format

assistant task *task-name*

undo assistant task *task-name*

Parameters

Parameter	Description	Value
task-name	Specifies the name of an assistant task.	The value is a string of 1 to 15 characters. It can consist of only underscores (_), letters, and digits, and must start with a letter.

Views

System view

Default Level

3: Management level

Usage Guidelines

An assistant task is a virtual assistant on a device to realize automatic maintenance and management. After you create an assistant task and bind it to a batch of files to be processed, the device performs operations or configurations when it is unattended. Assistant tasks are mainly used for scheduled system upgrade or configuration.

NOTE

You can create a maximum of five assistant tasks on a device.

Example

Create an assistant task.

```
<HUAWEI> system-view
[HUAWEI] assistant task test
```

2.1.3 command-privilege level

Function

The **command-privilege level** command sets a command privilege level in a specified view.

The **undo command-privilege** command restores the default level.

By default, each command in each view has a default command privilege level.

Format

command-privilege level *level* **view** *view-name command-key*

undo command-privilege [**level** *level*] **view** *view-name command-key*

Parameters

Parameter	Description	Value
level *level*	Specifies a command privilege level.	The value is an integer that ranges from 0 to 15.
view *view-name*	Specifies a view name. You can enter a question mark (?) in the terminal GUI to obtain all view names in the command view. For example: ● shell: user view ● system: system view ● vlan: VLAN view	-
command-key	Specifies a command. The command must be entered manually because automatic command line completion is not supported.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The system divides commands into levels for management. Each command in views has a specified level. The device administrator can change a command privilege level as required so that a lower-level user can use certain high-level commands. The device administrator can also increase the command privilege level to a larger value to improve device security.

Precautions

- The rules for using this command to set the command privilege level of a specified view are as follows:
  - When you degrade the target command, all keywords in the command are degraded.
  - When you upgrade the target command, only the last keyword in the command is upgraded.

  - When you set a level for the target command, the levels of all commands (in the same view) starting with this command are changed.
  - When you set a level for the target command, the keyword level in other commands having the same index as the keyword whose level is changed is also changed.
  - If the level of keywords that have the same index is modified for multiple times, the latest configured level takes effect.
- Do not change the default command privilege level. If you need to change it, consult with professional personnel to ensure that routine operation and maintenance are not affected and security risks are avoided.
- If parameters are specified in the command whose privilege level is configured using the **command-privilege level** command, enter these parameters, for example, **command-privilege level 1 view shell tftp 10.1.1.1 get vrpcfg.txt cfcard:/vrpcfg.bak**.

Example

Set the privilege level of the **save** command to 5.

```
<HUAWEI> system-view
[HUAWEI] command-privilege level 5 view shell save
```

2.1.4 command-privilege level rearrange

Function

The **command-privilege level rearrange** command upgrades command privilege levels in batches.

The **undo command-privilege level rearrange** command restores the default command privilege levels in batches.

By default, the command privilege levels assigned by the system during registration are used.

Format

command-privilege level rearrange

undo command-privilege level rearrange

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Each command registered on a device is assigned a default level 0, 1, 2, or 3. These levels correspond to the visit level, monitoring level, configuration level, and management level. You can run the **command-privilege level rearrange** command to upgrade all the level-2 and level-3 commands to level-10 and level-15 commands in batches. The level-0 and level-1 commands remain unchanged.

Precautions

- You can change the levels of the commands that are not separately changed by the **command-privilege level** command. The levels of the commands that are separately changed by the **command-privilege level** command cannot be upgraded.
- You can restore the levels of the commands that are upgraded in batches. The levels of the commands that are separately changed by the **command-privilege level** command cannot be upgraded.
- After the **command-privilege level rearrange** command is run, users at Level 2 to Level 9 are not allowed to run commands defaulted to Level 2, and users at Level 3 to Level 14 are not allowed to run commands defaulted to Level 3. If some users are required to have the same command privilege as that before the command privilege level promotion, you are advised to adjust the levels of all users on the device.
- After the **undo command-privilege level rearrange** command is run, users at level 3 to level 14 are allowed to run commands defaulted to level 3, and users at level 2 to level 9 are allowed to run commands defaulted to level 2. If some users are required to have the same command privilege as that before the command privilege level decrease, you are advised to adjust the levels of all users on the device.
- You can use the **command-privilege level rearrange** command only when your user privilege level is 15.
- After the levels of the commands are upgraded in batches and before the levels of the commands are restored, upgrading the levels of the commands is invalid and does not change the current status of the commands.

Example

Change the levels of the current commands in batches.

```
<HUAWEI> system-view
[HUAWEI] command-privilege level rearrange
```

2.1.5 diagnose

Function

The **diagnose** command enables a device to enter the diagnostic view from the system view.

Format

diagnose

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Diagnostic commands are mainly used for fault diagnosis. However, running certain commands may cause device faults or service interruptions. Therefore, use these diagnostic commands under the instruction of technical support personnel.

Example

Enable a device to enter the diagnostic view.

```
<HUAWEI> system-view
[HUAWEI] diagnose
[HUAWEI-diagnose]
```

2.1.6 display assistant task history

Function

The **display assistant task history** command displays operation records of assistant tasks.

Format

display assistant task history [*task-name*]

Parameters

Parameter	Description	Value
task-name	Specifies the name of an assistant task.	The value is a string of 1 to 15 characters consisting only of underscores (_), letters, and digits, and must start with a letter.

Views

All views

Default Level

3: Management level

Usage Guidelines

The five latest operations of each assistant task are displayed in order from earliest to latest.

Example

Displays operation records of assistant tasks.

```
<HUAWEI> display assistant task history
--------------------------------------------------------------------------------
Assistant task name: nemo
--------------------------------------------------------------------------------
Assistant task name: song
 Action type    : Batch file
 Batch file name: reboottest.bat
 Start time     : 2012-07-16 09:25:00
 End time       : 2012-07-16 09:25:00
 State          : Finished

 Action type    : Batch file
 Batch file name: reboottest.bat
 Start time     : 2012-07-16 09:24:00
 End time       : 2012-07-16 09:24:00
 State          : Finished

--------------------------------------------------------------------------------
Assistant task name: xu
 Action type    : Batch file
 Batch file name: reboottest.bat
 Start time     : 2012-07-16 09:25:00
 End time       : 2012-07-16 09:25:00
 State          : Finished

 Action type    : Batch file
 Batch file name: reboottest.bat
 Start time     : 2012-07-16 09:24:00
 End time       : 2012-07-16 09:24:00
 State          : Finished

 Action type    : Batch file
 Batch file name: reboottest.bat
 Start time     : 2012-07-16 09:23:00
 End time       : 2012-07-16 09:23:00
 State          : Finished

--------------------------------------------------------------------------------
```

Table 2-1 Description of the **display assistant task history** command output

Item	Description
Assistant task name	Task name. This parameter is configured using the **assistant task** command.
Action type	Operation that an assistant task performs.

Item	Description
Batch file name	Name of the batch file used by an assistant task. This parameter is configured using the **perform batch-file** command.
Start time	Operation start time of an assistant task.
End time	Operation end time of an assistant task.
State	Running status of an assistant task. • **Running** indicates that the assistant task is in operating. • **Finished** indicates that the assistant task has finished operating.

2.1.7 display component

Function

The **display component** command displays information about a registered component.

Format

display component [*component-name*] [**slot** *slot-id*]

Parameters

Parameter	Description	Value
component-name	Displays information about a component with a specified ID.	The value ranges from 0 to FFFFFFFF, in hexadecimal notation. **0** indicates brief information about all components, and **FFFFFFFF** indicates detailed information about all components. The default value is **FFFFFFFF**.

Parameter	Description	Value
slot *slot-id*	• Displays information about registered components on a specified slot if stacking is not configured. • Displays information about registered components on a specified stack member device if stacking is configured.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display component** command displays information about a registered component.

Example

Display brief information about all registered components.

```
<HUAWEI> display component 0


------------------------------------------------------
 No.   CompID      CompVer        CompName
 0     0x00003391  1.0.0.0        DNS
 1     0x000001f4  1.0.0.0        COMMON
 2     0x00002ee1  1.0.0.0        NSPCOMMON
 3     0x0000332d  1.0.0.0        NSPNOLIBCOMMON
 4     0x000032c9  1.0.0.0        NFPCOMMON
 5     0x00002c89  1.0.0.0        SECAPP
 6     0x000027da  1.0.0.0        TRUNK
 7     0x00002775  1.0.0.0        L2IF
 8     0x00002af9  1.0.0.0        NQAC_BASIC
 9     0x00002b5d  1.0.0.0        NQAS_BASIC
 10    0x00002e19  1.0.0.0        VPLS BASIC
 11    0x000000c8  1.0.0.0        PPMNG
 12    0x000000ce  1.0.0.0        ND
 13    0x000000cf  1.0.0.0        ADDR
 14    0x000000c9  1.0.0.0        ICMP6
 15    0x000000cd  1.0.0.0        PMTU
 16    0x000000df  1.0.0.0        IPSEC6-IPV6
 17    0x000000de  1.0.0.0        IPSEC6-POLICY
 18    0x000000dc  1.0.0.0        IPSEC6-SAPRO
 19    0x000000cb  1.0.0.0        UDP6
 20    0x000000cc  1.0.0.0        RIP6
 ---- More ----
```


Table 2-2 Description of the **display component** command output

Item	Description
No.	Number.
CompID	Component ID.
CompVer	Component version.
CompName	Component name.

2.1.8 display history-command

Function

The **display history-command** command displays the historical commands stored on a device.

Format

display history-command [**all-users**]

Parameters

Parameter	Description	Value
all-users	Displays information about the successfully matched commands that are executed by all users. If *all-users* is not specified, successfully matched historical commands executed by the current user are displayed.	-

Views

All views

Default Level

display history-command: 0: Visit level

display history-command all-users: 3: Management level

Usage Guidelines

Usage Scenario

The terminal automatically saves the history commands entered by the user, that is, records any keyboard entry of the user with **Enter** as the unit.

By default, the **display history-command** command displays a maximum of 10 historical commands. If the number of historical commands is less than 10, the

display history-command command output displays all of them. Run **history-command max-size** command to set the size of the historical command buffer.

Precautions

Commands run by users are automatically saved on the terminal. Any input that ends with **Enter** is saved as a historical command.

NOTE

- Commands are saved in the same format as those users entered. If an entered command is incomplete, the saved command is also incomplete.
- If a command is run several times, only the latest one is saved. If the command is run in different formats, they all saved as different commands.

You can check historical commands using the following methods:

- To check a previous historical command, press the **Up** arrow key or **Ctrl+P**.
- To check a next historical command, press the **Down** arrow key or **Ctrl+N**.

NOTE

To check the previous historical commands on a Windows 9X HyperTerminal, press **Ctrl+P**. The **Up** arrow key does not take effect.

Example

Display the historical commands that have been executed on a terminal.

```
<HUAWEI> display history-command
 system-view
 user-interface vty 0 4
 user privilege level 15
 quit
```

2.1.9 display this

Function

The **display this** command displays the running configurations in the current view.

Format

display this

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After configurations are complete in a certain view, run the **display this** command to check the current configurations.

Precautions

If a configuration parameter uses the default value, this parameter is not displayed. Configurations for functions that do not take effect are not displayed.

If you run the **display this** command in an interface view, configurations of the interface view are displayed. If you run this command in a protocol view, configurations of the protocol view are displayed.

Example

Display the running configuration in the current view.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/1
 port link-type trunk
#
return
```

2.1.10 display this include-default

Function

The **display this include-default** command displays the valid configurations in the current view, including the unchanged default configurations.

NOTE

This command does not display the default configurations that are not modified in the WLAN view.

Format

display this include-default

Parameters

None.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

You can use this command to view the default configurations of physical attributes, basic Ethernet protocols, routing, multicast, QoS, and security features on Ethernet interfaces. The following features are included:

- VLAN management: port-based VLAN assignment, other VLAN assignment methods, PVID, link type, QinQ protocol type, port priority, discard tagged-pkt, and port bridge
- MUX VLAN, voice VLAN, VLAN mapping/stacking, VT enable, and VT miss-drop
- MAC address learning status and priority, port security, sticky MAC, MAC address limiting, and MAC flapping detection
- MSTP, L2PT, DLDP, LLDP, loopback detection, RRPP, SmartLink, SEP, and ERPS
- Ethernet interface physical attributes: speed/duplex, speed auto-negotiation, negotiation, flow control, flow control negotiation, flow-control receive/flow-control negotiation receive, loopback, MDI, jumbo frame, trap/log alarm thresholds, link flapping, EEE, link Up/Down report delay, VCT, inter-frame gap statistics, error packet statistics, URPF, and copper module information
- ARP, ND, Eth-Trunk, and port isolation
- BFD: single-hop BFD, multi-hop BFD, BFD for LSP, and multicast BFD
- Unicast route management, static routes, RIP, OSPF, IS-IS, BGP, and VRRP
- Multicast routing, PIM, IGMP, MLD, IGMP snooping, and MLD snooping
- QoS, ACL, storm suppression, ARP security, IP security, and MFF
- DHCP, DHCPv6, ND Snooping, NAC, and RADIUS

This command can also display the following default global configurations: enabling of the function that sends ICMP host/port unreachable packets, enabling of the function that discards ICMP packets with TTL value 1, rate limit for ARP Miss packets, enabling of ICMP packet rate limiting, and interval for collecting CAR-based traffic statistics. For the support for default settings of the features, see the corresponding device model.

Example

Display the valid configurations and default configurations on VLANIF 10. The following command output is used for reference. The command output on your device may differ from that provided in this example.

```
<HUAWEI> system-view
[HUAWEI] interface Vlanif 10
[HUAWEI-Vlanif10] display this include-default
#
interface Vlanif10
 undo shutdown
 undo set flow-stat interval
 mtu 1500
 undo arp detect-mode unicast
 arp-fake expire-time 3
 undo arp learning disable
 undo arp purge slowly
 undo ipv6 enable
 icmp host-unreachable send
 icmp redirect send
 icmp port-unreachable send
 icmp ttl-exceeded send
```



```
 undo ip verify source-address
 undo ip forward-broadcast
 undo clear ip df
 undo discard srr
 undo discard rr
 undo discard ra
 undo discard ts
 damping time 0
 arp learning strict trust
 undo ntp-service in-interface disable
 undo mpls
 undo arp-proxy enable
 undo arp-proxy inter-sub-vlan-proxy enable
 undo arp-proxy inner-sub-vlan-proxy enable
 undo arp broadcast disable
 undo rrpp snooping enable
 nd optimized-passby enable
 undo urpf
 diffserv-mode uniform
 undo statistic enable both
 undo ipv4 statistic enable both
 undo ipv6 statistic enable both
 undo arp gratuitous-arp send enable
 undo arp anti-attack entry-check enable
 undo arp learning double-tag disable
 arp optimized-passby enable
 undo dhcp select global
 undo dhcp select interface
 undo dhcp select relay
 undo ip address bootp-alloc
 undo ip address dhcp-alloc
 undo arp learning dhcp-trigger
#
return
```

2.1.11 header

Function

The **header** command configures the header information displayed on a terminal when users log in to a connected device.

The **undo header** command deletes the header information displayed on a terminal when users log in to a connected device.

By default, no header information is displayed on terminals when users log in to a connected device.

Format

header { **login** | **shell** } { **information** *text* | **file** *file-name* }

undo header { **login** | **shell** }

Parameters

Parameter	Description	Value
login	Indicates header information displayed on a terminal when a user logs in to the device and a connection between the terminal and the device is activated.	-
shell	Indicates the header displayed on a terminal when the session is set up after the user logs in to the connected device.	-
information *text*	Specifies the header and content.	The value is a string with spaces and carriage returns supported. The maximum length of the string that can be entered at one time is 480 characters.
file *file-name*	Specifies the file name that the header uses.	The value is a string of 1 to 64 characters without spaces. Only the absolute path is supported. The file name must be in the [drive] [path] [file name] format, where [path] is the absolute path of the file. The maximum header file size that can be configured is 2 KB.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To provide some prompts or alarms to users, run the **header** command to configure a title on the device. If a user logs in to the device, the title is displayed.

Procedure

If **information** is specified, the header text starts and ends with the same character. You can set the header text in either of the following modes:

- Non-interactive: enter the header text behind the start character.

  Use the same character at the beginning and end of the header and press **Enter**. If the start and end characters are inconsistent, the system prompts an error message.
- Interactive: enter the start character and press **Enter** to enter the interactive process.

  The system displays a message asking you to enter the correct header information. After you enter the information, enter the same character as the start character. Press **Enter**. The system quits the interactive process.

  During interaction, you can press **Enter** at any time to enter information in the next line.

Precautions

- Before setting the **login** parameter, you must set login authentication parameters; otherwise, no header information about authentication is displayed.
- Before setting the **file** parameter, ensure that the file containing the header exists; otherwise, the file name cannot be obtained. If you change header information after login, the header information that has been displayed in the system does not change, even if you exit and log in to the system again. The header information changes in either of the following cases:
  - You have successfully changed the header information. Before the system restarts, you run this command again. Then you exit and log in to the system again.
  - You have successfully changed the header information. Then you restart the system.
- If you use SSH1.X to log in to the device, only the shell header is displayed.
- If you use SSH2.0 to log in to the device, both login and shell headers are displayed in the login process.
- If the header command is configured several times, only the latest configuration takes effect.
- After configuring the login header, any user that logs in to the system can view the header.
- In the system view, run the **execute** *batch-filename* batch processing command. If the batch processing command contains the **header** { **login** | **shell** } **information** *text* command and *text* contains line feed character **\r\n**, you need to use third-party software to change the hexadecimal value (0D 0A) of the line feed character **\r\n** to (1B 19).

Example

Configure a shell header in non-interactive mode.

```
<HUAWEI> system-view
[HUAWEI] header shell information &Hello! Welcome to system!&     # Enter the header text behind the start character '&' and enter '&' at the end of the header text, and press Enter.
```

Display the shell header if the login succeeds.

```
Hello! Welcome to system!
```

Configure a shell header in interactive mode.


```
<HUAWEI> system-view
[HUAWEI] header shell information %      # Press Enter after entering the start character '%' to start the interactive process.
The banner text supports 480 characters max, including the start and the end cha
racter.If you want to enter more than this, use banner file instead.Input banner
 text, and quit with the character '%':
Hello!
Welcome to system!%      # Press Enter after entering the end character '%' to quit the interactive process.
[HUAWEI] quit
<HUAWEI> quit      // Log off.
```

Press **Enter**. The shell header is displayed when the user logs in again.

```
Hello!
Welcome to system!
<HUAWEI>
```

Specify the file that stores a login header.

```
<HUAWEI> system-view
[HUAWEI] header login file flash:/header-file.txt
```

2.1.12 if-match timer cron

Function

The **if-match timer cron** command sets the time to perform an assistant task.

The **undo if-match timer cron** command cancels the time configured for performing an assistant task.

By default, the time to perform an assistant task is not specified.

Format

if-match timer cron *seconds minutes hours days-of-month months days-of-week* [*years*]

undo if-match timer cron

Parameters

Parameter	Description	Value
seconds	Sets second.	The value is a string of 1 to 64 characters in the cron time format. The string consists of digits 0 to 9 and special characters asterisks (*), hyphens (-), slashes (/), and commas (,). Currently, the device supports only asterisks (*), indicating that the value is accurate to the minute but not the second.

Parameter	Description	Value
minutes	Sets minute.	The value is a string of 1 to 64 characters in the cron time format. The string consists of digits 0 to 9 and special characters asterisks (*), hyphens (-), slashes (/), and commas (,).
hours	Sets hour.	The value is a string of 1 to 64 characters in the cron time format. The string consists of digits 0 to 9 and special characters asterisks (*), hyphens (-), slashes (/), and commas (,).
days-of-month	Sets date.	The value is a string of 1 to 64 characters in the cron time format. The string consists of digits 0 to 9 and special characters asterisks (*), hyphens (-), slashes (/), and commas (,). This parameter is exclusive with the *days-of-week* parameter. At least one of the two contains asterisks (*).
months	Sets month.	The value is a string of 1 to 64 characters in the cron time format. The string consists of digits 0 to 9 and special characters asterisks (*), hyphens (-), slashes (/), and commas (,).

Parameter	Description	Value
days-of-week	Sets week.	The value is a string of 1 to 64 characters in the cron time format. The string consists of digits 0 to 9 and special characters asterisks (*), hyphens (-), slashes (/), and commas (,). The parameter is exclusive with the *days-of-month* parameter. At least one of the two contains asterisks (*).
years	Sets year.	The value is a string of 1 to 64 characters in the cron time format. The string consists of digits 0 to 9 and special characters asterisks (*), hyphens (-), slashes (/), and commas (,). If this parameter is not specified, it refers to all the years between 2000 to 2099.

Views

Assistant task template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **if-match timer cron** command is used to set the time to perform an assistant task. The time is expressed in the cron format defined in UNIX or Linux.

The commonly used time and date format (hh:mm:ss dd-mm-yyyy) can specify only one specific time value. The cron time format is more flexible and can display single or multiple time points, time ranges, and time intervals. The following table describes the expression mode of the cron format.

Expression Mode	Format	Description	Example
Single time point	<time>	<time>: The value is an integer that specifies a specific time value. The value range is dependent on a specific parameter. The range of minutes is 0 to 59. The range of hours is 0 to 23. The range of days-of-month depends on the number of days in a specific month. The range of months is 1 to 12. The range of days-of-week is 0 to 7. The range of years is 2000 to 2099.	Command: if-match timer cron * 0 1 2 5 * 2012 Meaning: perform an assistant task at 1:00 on May 2, 2012.
Multiple time points	<time1>,<time2>,...,<timen>	<timen>: The value is an integer. The value range depends on a specific parameter. Multiple time points are separated by a comma (,) with no space before or after it. The time values in a list can be arranged in any sequence.	Command: if-match timer cron * 0 1,2,3 2 3 * 2012 Meaning: perform an assistant task at the following time points: • 1:00, March 2, 2012 • 2:00, March 2, 2012 • 3:00, March 2, 2012

Expression Mode	Format	Description	Example
Specific time point	<time>/<step>	<time>: The value is an integer that specifies a specific time value. <step>: The value is an integer that specifies the time incremental. The two values are separated by a slash (/) with no space before or after it. The format: <time>,<time>+<step>,<time>+2*<step>,...,<time>+n*<step>. The maximum time (<time>+n*<step>) depends on a specific parameter in the command line.	Command: if-match timer cron * 0 0/10 * 3 * 2012 Meaning: perform an assistant task at the following time points: ● 0:00, March 1, 2012 ● 10:00, March 1, 2012 ● 20:00, March 1, 2012 ● 0:00, March 2, 2012 ● ... ● 10:00, March 31, 2012 ● 20:00, March 31, 2012
Duration	<time1>-<time2>	<time1> and <time2>: The values are integers, specifying the start and end time respectively. <time2> must be later than or equal to <time1>. The two values are separated by a hyphen (-) with no space before or after it. the <time1>-<time2> is same as <time1>,<time1>+1,<time1>+2,.....,<time2>. If <time1> and <time2> are the same, they specify the same time point.	Command: if-match timer cron *0 0-3 1 3 * 2012 Meaning: perform an assistant task at the following time points: ● 0:00, March 1, 2012 ● 1:00, March 1, 2012 ● 2:00, March 1, 2012 ● 3:00, March 1, 2012

Expression Mode	Format	Description	Example
Period	*	If the parameter in the command line is set to *, the parameter may refer to any time point. By setting the parameter to *, you can configure the system to periodically perform an assistant task every year, week, month, day, hour, or minute.	Command: if-match timer cron * 30 10 * 1 1 2012 Meaning: perform an assistant task at 10:30, Monday every week in January, 2012.
Combination	Combination format	All the expression modes can be combined except "period". The expression modes are separated by a comma (,) with no space before or after it.	Command: if-match timer cron * 0 0/10,2,4-5 1 3 * 2012 Meaning: perform an assistant task at the following time points: ● 0:00, March 1, 2012 ● 2:00, March 1, 2012 ● 4:00, March 1, 2012 ● 5:00, March 1, 2012 ● 10:00, March 1, 2012 ● 20:00, March 1, 2012

Precautions

- If you run the **if-match timer cron** command multiple times in the same view, only the latest configuration takes effect.
- The *days-of-month* and *days-of-week* parameters are exclusive. Set one or both of them to "*". If one parameter is set to *, the other one specifies a specific date. If both parameters are set to *, they can refer to any date.
- The minimum unit supported is minute, so set the second parameter to *. The specified assistant task works only once every minute.
- Since the system can perform only one assistant task at a time, the time when one assistant task finished working may be later than the time when the next task is schedule to start. There may be a time span between the time when an assistant task is scheduled to work and the time when it actually starts to work. The **if-match timer cron** command specifies the time when an assistant task is scheduled to work.
- When you enter digits, such as 000002012, the numeric string means the same as 2012.

Example

Configure an assistant task to work at 20:00, 2012-05-04.

```
<HUAWEI> system-view
[HUAWEI] assistant task test
[HUAWEI-assistant-task-test] if-match timer cron * 0 20 4 5 * 2012
[HUAWEI-assistant-task-test] perform 1 batch-file sys.bat
```

Cancel the time for an assistant task to start to work.

```
<HUAWEI> system-view
[HUAWEI] assistant task test
[HUAWEI-assistant-task-test] undo if-match timer cron
```

2.1.13 perform batch-file

Function

The **perform batch-file** command configures an assistant task to process a batch file.

The **undo perform** command disables an assistant task from processing a batch file.

By default, no batch file is configured for an assistant task.

Format

perform *priority* **batch-file** *filename*

undo perform *priority*

Parameters

Parameter	Description	Value
priority	Specifies a priority for an assistant task.	The value is fixed at 1 because one assistant task can process only one batch file.
filename	Specifies the name of the batch file processed by the assistant task.	The file is in *.bat file. **NOTE** The file must be stored in the **flash:/user/bat** directory.

Views

Assistant task template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After you successfully create an assistant task and specify the execution time, you can run this command to configure the device to process a batch file at the specified time.

Prerequisites

An assistant task has been created using the **assistant task** command and the execution time has been specified using the **if-match timer cron** command.

Precautions

To delete an assistant task that is being executed, stop it first. To delete an assistant task to be executed, directly delete it. The device will not execute the assistant task.

Example

Configure the assistant task **huawei** to process the batch file **sys.bat** at 20:00 on 2012-05-04.

```
<HUAWEI> system-view
[HUAWEI] assistant task huawei
[HUAWEI-assistant-task-huawei] if-match timer cron * 0 20 4 5 * 2012
[HUAWEI-assistant-task-huawei] perform 1 batch-file sys.bat
```

Disable an assistant task from processing a batch file.

```
<HUAWEI> system-view
[HUAWEI] assistant task huawei
[HUAWEI-assistant-task-huawei] undo perform 1
Info: Start to delete the action.
[HUAWEI-assistant-task-huawei] display this
#
assistant task huawei
 if-match timer cron * 0 20 4 5 * 2012
#
return
```

2.1.14 quit

Function

The **quit** command returns a device from the current view to a lower-level view. If the current view is the user view, this command exits from the system.

Format

quit

Parameters

None

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

Three types of views are available (listed from a lower level to a higher level):

- User view
- System view
- Service view, such as the interface view

Run the **quit** command to return to a lower-level command view from the current view. Running this command in the user view quits from the system.

Example

Return to the system view from the AAA view and then return to the user view. Quit the system after this.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] quit
[HUAWEI] quit
<HUAWEI> quit
```

2.1.15 reset history-command

Function

The **reset history-command** command deletes historical commands from a device.

Format

reset history-command [**all-users**]

Parameters

Parameter	Description	Value
all-users	Deletes historical commands entered by all users. If this parameter is not specified, the historical commands entered only by the current user are deleted.	-

Views

All views

Default Level

reset history-command: 0: Visit level

reset history-command all-users: 3: Management level

Usage Guidelines

To delete historical commands entered by the current user, run the **reset history-command** command. If a level 3 (or higher) user runs the **reset history-command all-users** command, historical commands entered by all users are deleted.

Example

Delete historical commands entered by the current user.

```
<HUAWEI> reset history-command
```

2.1.16 return

Function

The **return** command returns to the user view from other views (except the user view).

Format

return

Parameters

None

Views

All views

Default Level

0: Visit level

Usage Guidelines

Use the **return** command in other views to return to the user view.

- This command returns to the user view if the current view is another view (but not the user view).
- No change occurs after running this command if the current view is the user view.
- The shortcut keys **Ctrl+Z** functions similarly as the **return** command.

Example

Return to the user view from the user interface view.

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0
[HUAWEI-ui-vty0] return
<HUAWEI>
```

2.1.17 system-view

Function

The **system-view** command enables you to enter the system view from the user view.

Format

system-view

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

You must configure the device in the system view. Run this command in the user view to enter the system view.

Example

Enter the system view.

```
<HUAWEI> system-view
Enter system view, return user view with Ctrl+Z.
[HUAWEI]
```

2.1.18 terminal command forward matched upper-view

Function

The **terminal command forward matched upper-view** command enables forward commands (not in the undo form) to automatically match the upper-level view and return to the upper-level view.

The **undo terminal command forward matched upper-view** command disables forward commands from automatically matching the upper-level view.

By default, forward commands are enabled to automatically match the upper-level view.

Format

terminal command forward matched upper-view

undo terminal command forward matched upper-view

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If forward commands are enabled to automatically match the upper-level view and you run a forward command not registered in the current view, the system automatically switches to the upper-level view to search for the command. If the command is found in that view, the system runs the command. If the command is not found in that view, the system continues the search in the next upper-level view until the system view.

Precautions

The **terminal command forward matched upper-view** command takes effect only for the current login user who runs this command.

Example

Enable forward commands to automatically match the upper-level view.

```
<HUAWEI> terminal command forward matched upper-view
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] sysname ABC
[ABC]
```

Disable forward commands from automatically matching the upper-level view.

```
<HUAWEI> undo terminal command forward matched upper-view
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] sysname ABC
                              ^
Error: Unrecognized command found at '^' position.
```


2.1.19 terminal echo-mode

Function

The **terminal echo-mode** command sets a command output mode.

The default command output mode is **character**.

Format

terminal echo-mode { **character** | **line** }

Parameters

Parameter	Description	Value
character	Specifies a character mode. The system displays the character that you enter in the command line.	-
line	Specifies a line mode. The system displays the character that you enter in the command line only after you press **Enter**, **Tab** or **?**. If you press a shortcut key, such as **Backspace**, **Page Up**, or **Ctrl+A**, it still takes effect.	-

Views

User view

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

When operating a device using the NMS, run this command to change the command output mode to **line** to improve operation efficiency. Common users typically use the **character** mode, so use this mode for common users to improve operation efficiency.

Precautions

- After a user runs this command to set the **line** mode, this mode takes effect only for this user. Other users still use the **character** mode.
- After a user changes the command output mode to **line**, the command output mode automatically switches to **character** when the user exits the device or the device restarts or performs an active/standby switchover.

- This command does not affect interactive inputs for the command line.

Example

Set the command output mode to **line**.

```
<HUAWEI> terminal echo-mode line
```

2.2 EasyDeploy Commands

2.2.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

Switches' support for the commander and client roles in EasyDeploy application is as follows:

Role	Product Model	Version	Maximum Number of Managed Clients
Commander	S12700	V200R005C00 and later	255
	S12700E	V200R019C00 and later	255
	S7700	V200R003C00 and later	255
	S9700	V200R003C00 to V200R013C00	255
	S5700-HI	V200R003C00 to V200R005C00	128
	S5710-HI	V200R003C00 to V200R005C00	128
	S6700-EI	V200R003C00 to V200R005C00	128
	S5700-EI	V200R003C00 to V200R005C00	64
	S5710-EI	V200R003C00 to V200R005C00	64
	S5720-HI	V200R006C00 to V200R019C10	128
	S5720-EI	V200R007C00 to V200R019C10	128

Role	Product Model	Version	Maximum Number of Managed Clients
	S5730-HI	V200R012C00 to V200R019C10	128
	S5731-H	V200R013C02 and later	128
	S5731-S	V200R019C00 and later	128
	S5731S-S	V200R019C00 and later	128
	S5731S-H	V200R019C00 and later	128
	S5732-H	V200R019C00 and later	128
	S6720-EI	V200R008C00 and later	128
	S6720S-EI	V200R009C00 and later	128
	S6720-HI	V200R012C00 to V200R019C10	128
	S6730-H	V200R013C02 and later	128
	S6730S-H	V200R019C10 and later	128
	S6730-S	V200R019C00 and later	128
	S6730S-S	V200R019C00 and later	128
	S6735-S	V200R021C00SPC600 and later	128

Role	Product Model	Version	Maximum Number of Managed Clients
Client	• All fixed switch models except S1720GFR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S1730S-S1, and S1720X-E • All modular switch models	V200R003C00 and later	-

2.2.2 activate-file

Function

The **activate-file** command sets the file activation mode and time on the Commander.

The **undo activate-file** command restores the default file activation mode and time.

By default, if downloaded files include the system software (*.cc), devices immediately activate all files by resetting. In addition, if the downloaded files in the batch upgrade scenario include the configuration file, the devices also activate files immediately by resetting.

Format

activate-file { **reload** | { **in** *time* | **delay** *delay-time* } } *

undo activate-file [**reload** | **in** [*time*] | **delay** [*delay-time*]]

Parameters

Parameter	Description	Value
reload	Indicates that the device activates files by resetting.	-
in *time*	Indicates the time when the device activates files.	The format is HH:MM, in which HH indicates hour ranging from 0 to 23 and MM indicates minute ranging from 0 to 59.

Parameter	Description	Value
delay *delay-time*	Indicates the delay after which the device activates files.	The value is an integer that ranges from 0 to 86400, in seconds. The default is 0.

Views

Easy-Operation view, Easy-Operation group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If clients use the default method to activate files, network services will be affected. This issue is especially prominent in the batch upgrade scenario where each upgraded device may carry a lot of services. Resetting these devices will interrupt services. Therefore, the devices should activate files when service volume is small.

Precautions

- If the **reload** parameter is specified, the client activates files by resetting regardless of whether downloaded files include the system software.
- The **undo activate-file** command restores the default file activation mode and time. If the **reload**, **in**, and **delay** parameters are specified in the **undo activate-file** command, the default configurations are restored.
- The file activation mode can be set in the Easy-Operation view or group view. If the client matches a group, the configuration in the group view takes effect for the client.

Example

Set the file activation mode to reset.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] activate-file reload
```

Set the file activation delay to one hour.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] activate-file delay 3600
```

Set the file activation mode to reset and time to 1:00 am.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] activate-file in 1:00 reload
```

Set the file activation mode to reset and time to 1:00 am for group F1.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
```



```
[HUAWEI-easyoperation] group custom ip-address F1
[HUAWEI-easyoperation-group-custom-F1] activate-file in 1:00 reload
```

2.2.3 backup configuration interval

Function

The **backup configuration interval** command enables automatic configuration file backup on the Commander and sets the backup interval and method.

The **undo backup configuration** command disables automatic configuration file backup.

By default, the configuration file is not automatically backed up.

Format

backup configuration interval *interval* [**duplicate**]

undo backup configuration [**interval** [*interval*]] [**duplicate**]

Parameters

Parameter	Description	Value
interval	Indicates the backup interval.	The value is an integer that ranges from 0 to 720, in hours. The default value is 0, indicating that clients do not automatically back up configuration files.
duplicate	Indicates that the backup file is saved as a new file, and the original configuration file is not overwritten. If this parameter is not specified, the original configuration file is overwritten by the backup file.	-

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a faulty client is replaced by a new client, the new client needs to obtain the latest configuration file of the faulty client to minimize impact on service.

Therefore, all clients should periodically back up their configuration files to the file server.

NOTE

This function must be configured before any fault occurs. It is recommended that you configure this function when deploying the network.

Prerequisites

The file server information has been configured on the Commander using the **tftp-server/sftp-server/ftp-server** command.

Precautions

- After this function is configured, all clients managed by the Commander will automatically back up configuration files.
- To disable this function, run the **undo backup configuration** [**interval** [*interval*]] or **undo backup configuration interval duplicate** command, or set the file backup interval to 0.
- If you do not want to keep the original configuration files, run the **undo backup configuration duplicate** command to make the backup files overwrite the original files.
- The naming convention of the configuration files is as follows:
  - If the backup files are saved as new files, name the new files in format vrpcfg-MAC address-year-month-day-hour-minute-second.XXX. XXX is the file name extension, which must be the same as the configuration file name extension being used on the client. For example, if the startup configuration file on a client is **vrpcfg.zip**, the backup file is named in format vrpcfg-MAC address-year-month-day-hour-minute-second.zip.
  - If the backup files overwrite the original files, name the backup files in format vrpcfg-MAC address.XXX. XXX is the file name extension, which must be the same as the configuration file name extension being used on the client.

Example

Set the file backup interval to 12 hours and overwrite the original files with backup files.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] backup configuration interval 12
```

Disable automatic configuration file backup.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] backup configuration interval 0
Warning: This command will cancel the function of backing up configuration. Cont
inue?[Y/N]:y
[HUAWEI-easyoperation]
```


2.2.4 batch-cmd begin

Function

The **batch-cmd begin** command starts online command script editing.

Format

batch-cmd begin

Parameters

None

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In a batch device deployment scenario, you can run this command to start online command script editing. After editing the commands, press **Ctrl**+**C** to exit the editing mode. If you run this command again, the edited commands will be cleared.

Precautions

- Only one network administrator is allowed to edit commands online at one time.
- If no operation is performed in command editing mode within 30 seconds, you automatically exit from the editing mode to the Easy-Operation view.

Example

Start online command script editing.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] batch-cmd begin
Info: Begin to edit batch commands. Press CTRL+C to abort this session.
system-view
vlan batch 10 20
ndp enable
ntdp enable

[HUAWEI-easyoperation]
```


2.2.5 clear topology-error-info

Function

The **clear topology-error-info** command clears faulty link information from the topology.

Format

clear topology-error-info

Parameters

None

Views

Cluster view

Default Level

2: Configuration level

Usage Guidelines

The **clear topology-error-info** command can be run only on the Commander switch.

After a faulty client recovers, run this command to clear faulty link information from the topology. To view the topology information, run the **display cluster-topology-info** command.

Example

Clear information about faulty links and sub-links.

```
<HUAWEI> system-view
[HUAWEI] cluster
[HUAWEI-cluster] display cluster-topology-info
The topology information about the cluster:
<-->:normal device        <++>:candidate device        <??>:lost device
------------------------------------------------------------------------
Total topology node number is 3.
[HUAWEI: Root-00e0-fcb8-d6b6]
|-(GigabitEthernet0/0/2)<??>(GigabitEthernet0/0/1)[00e0-fc67-7f7d]
|-(GigabitEthernet0/0/3)<-->(GigabitEthernet0/0/3)[00e0-fc03-0003]
[HUAWEI-cluster] clear topology-error-info
[HUAWEI-cluster] display cluster-topology-info
The topology information about the cluster:
<-->:normal device        <++>:candidate device        <??>:lost device
------------------------------------------------------------------------
Total topology node number is 2.
[HUAWEI: Root-00e0-fcb8-d6b6]
|-(GigabitEthernet0/0/3)<-->(GigabitEthernet0/0/3)[00e0-fc03-0003]
```


2.2.6 client

Function

The **client** command adds information to the client database or modifies information in the client database.

The **undo client** command deletes information from the client database.

By default, the client database does not contain client information.

Format

client [*client-id*] { { **mac-address** *mac-address* | **esn** *esn* } | **system-software** *file-name* [*version*] | **patch** *file-name* | **configuration-file** *file-name* | **web-file** *file-name* | **license** *file-name* | { **custom-file** *file-name* } &<1-3> } *

undo client *client-id* [**mac-address** [*mac-address*] | **esn** [*esn*] | **system-software** [*file-name* [*version*]] | **patch** [*file-name*] | **configuration-file** [*file-name*] | **web-file** [*file-name*] | **license** [*file-name*] | **custom-file** [*file-name*]]

Parameters

Parameter	Description	Value
client-id	Specifies the client ID, which identifies a client. If this parameter is not specified when you add client information, the system assigns the minimum ID not in use to the client.	The value is an integer. It depends on the maximum number of clients supported by the Commander. For details, see **Maximum Number of Managed Clients** on the Commander.
mac-address *mac-address*	Specifies the MAC address of the client.	The value is in the H-H-H format, where each H contains four hexadecimal digits.
esn *esn*	Specifies the ESN of the client.	The value is a string of 10 to 32 case-insensitive characters without spaces.
system-software *file-name*	Specifies the name of the system software (*.cc) to be loaded to the client.	The value is a string of 4 to 48 case-insensitive characters without spaces.

Parameter	Description	Value
version	Specifies the version of a system software package, for example, V200R023C00. If the specified software version is the same as the software version running on the client, a software upgrade will not be performed for the client.	The value is a string of 11 to 32 case-insensitive characters without spaces.
patch *file-name*	Specifies the name of the patch file (*.pat) to be loaded to the client.	The value is a string of 5 to 48 case-insensitive characters without spaces.
configuration-file *file-name*	Specifies the name of the configuration file (*.zip or *.cfg) to be loaded to the client.	The value is a string of 5 to 48 case-insensitive characters without spaces.
web-file *file-name*	Specifies the name of the web page file (*.web.7z or *.web.zip) to be loaded to the client.	The value is a string of 8 to 64 case-insensitive characters without spaces.
license *file-name*	Specifies the name of the license file (*.dat) to be loaded to the client. **NOTE** The license file is not supported in the Easy-Operation view. The file does not take effect even if you configure it.	The value is a string of 5 to 64 case-insensitive characters without spaces.
custom-file *file-name*	Specifies the name of the user-defined file to be loaded to the client. A maximum of three user-defined files can be specified. The file names are separated by spaces.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a few zero touch clients need to be deployed on a network, you can run this command multiple times to add client information one by one.

Precautions

- Clients search the matching database by searching for their MAC addresses or ESNs in the database; therefore, the mappings between clients and MAC addresses or ESNs must be configured. When a client finds a matching database, it obtains information mapping its client ID, including system software name and patch file name.
- This command can be executed once or multiple times to configure the mappings between clients and MAC addresses or ESNs and specify information about the files to be downloaded.
- To delete all information about a client, run the **undo client** *client-id* command. To delete an item from a client's information, run the **undo** command with the item specified.

  NOTE

  When parameters are specified in this **undo** command to delete specified information, this command takes effect only for the manually configured clients.
- Each Commander supports a limited number of clients; therefore, the client information that can be added to the client database is also limited.
- You can specify a path for each file.

Example

Add client information in which MAC address is 00e0-fc12-3456, configuration file is **vrpcfg.zip**, and file path is /configfile/.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] client mac-address 00e0-fc12-3456 configuration-file configfile/vrpcfg.zip
```

Add client information in which client ID is 3, ESN is 210235165110xxxxxxxx, system software name is **test.cc**, and user-defined file names are **header.txt** and **aaa.bat**.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] client 3 esn 210235165110xxxxxxxx
[HUAWEI-easyoperation] client 3 system-software test.cc
[HUAWEI-easyoperation] client 3 custom-file header.txt custom-file aaa.bat
```

Delete the configuration file of the client with client ID 4.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] undo client 4 configuration-file
```

Delete all information about the client with client ID 5.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] undo client 5
```


2.2.7 client aging-time

Function

The **client aging-time** command ages the lost state clients in the client database and specifies the aging time.

The **undo client aging-time** command cancels the configuration.

By default, the lost state clients in the client database are not aged.

Format

client aging-time *aging-time*

undo client aging-time [*aging-time*]

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time for clients in the lost state.	The value is an integer that ranges from 72 to 720, in hours.

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Information about clients configured by the network administrator or automatically learned is saved in the client database. The Commander considers that a client to be in the lost state if the client does not respond after two minutes.

The maximum number of clients managed by the Commander depends on the device specifications. If the number of clients exceeds the upper limit, new client information cannot be configured on the Commander. To prevent clients in the lost state from occupying the database resources for a long time, enable the function of aging lost state clients. When the aging time expires, lost state clients are deleted. If some clients in the lost state occupy the database resources for a long time, run the **reset easy-operation client-offline** command to delete these clients.

Precautions

- Automatically learned clients are deleted after their aging time expires.
- Manually configured clients are not deleted but their status changes to unknown.

Example

Enable the function of aging lost state clients and set the aging time to 72 hours.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] client aging-time 72
```

2.2.8 client auto-clear enable

Function

The **client auto-clear enable** command enables clients to automatically clear storage space. This command is run on the Commander.

The **undo client auto-clear enable** command disables clients from clearing storage space.

By default, this function is disabled on the Commander.

Format

client auto-clear enable

undo client auto-clear enable

Parameters

None

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If storage space on a client is insufficient, the client cannot download files. This command enables clients to automatically clear storage space to ensure a sufficient storage space.

Precautions

- Clients clear storage space only when the storage space is insufficient for a system software package. In addition, they only delete non-startup system software packages to create space.
- This function is invalid for certain file server types. If the file server is a TFTP server, this function does not take effect because the TFTP server does not return file size to clients. If an FTP or SFTP server cannot return file size, this

function does not take effect, either. An S switch serving as an FTP or a TFTP file server does not support the function of returning file size.

Example

Enable clients to automatically clear storage space.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] client auto-clear enable
```

2.2.9 client auto-join enable

Function

The **client auto-join enable** command enables clients to automatically join the management domain of a Commander. This command is run on the Commander.

The **undo client auto-join enable** command disables clients from joining the management domain of a Commander.

By default, clients do not automatically join the Commander management domain.

Format

client auto-join enable

undo client auto-join enable

Parameters

None

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After this function is enabled and the Commander IP address is configured on clients, the Commander automatically learns the basic information about clients, saves the information to the client database, and assigns a client ID to each client.

Client information learned by the Commander includes MAC addresses, ESNs, IP addresses, device types, device models, current system software names, configuration files, and patch files on the clients. The Commander monitors and manages basic information and version files of all clients in the management domain.

In batch upgrade scenario, you can determine the devices to be upgraded according to the client information.

To prevent unknown clients from joining the management domain, disable this function.

Precautions

- In the batch upgrade scenario, run the **easy-operation commander ip-address** command to configure the Commander IP address on the clients.

  In the zero touch device deployment or faulty device replacement scenario, if you require that the clients still be managed by the Commander after completing the EasyDeploy process, add the Commander IP address to the configuration file to be downloaded by the clients.
- To view the client information learned by the Commander, run the **display easy-operation client** command.
- If the learned client information already exists in the client database (statically configured using **client**), the client database is updated.
- After information about a client is stored in the client database, the client status becomes LOST if the client goes offline. When the client goes online, the client joins the management domain again and its status becomes Running.

Example

Enable clients to automatically join the management domain of a Commander.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] client auto-join enable
Warning: The commander will create the client information in database automatica
lly when received message from unknown client. Continue? [Y/N]: y
[HUAWEI-easyoperation]
```

2.2.10 client replace

Function

The **client replace** command adds or modifies client replacement information.

The **undo client replace** command deletes client replacement information.

By default, no client replacement information exists.

Format

client *client-id* **replace** { [**mac-address** *mac-address* | **esn** *esn*] | **system-software** *file-name* [*version*] | **patch** *file-name* | **web-file** *file-name* | **license** *file-name* | { **custom-file** *file-name* } &<1-3> } *

undo client *client-id* **replace** [**mac-address** [*mac-address*] | **esn** [*esn*] | **system-software** [*file-name* [*version*]] | **patch** [*file-name*] | **web-file** [*file-name*] | **license** [*file-name*] | **custom-file** [*file-name*]]

Parameters

Parameter	Description	Value
client-id	Indicates the ID of a faulty client.	The value is an integer. It depends on the maximum number of clients supported by the Commander. For details, see **Maximum Number of Managed Clients** on the Commander.
mac-address *mac-address*	Indicates the MAC address of the new client.	The value is in the H-H-H format, where each H contains four hexadecimal digits.
esn *esn*	Indicates the ESN of the new client.	The value is a string of 10 to 32 case-insensitive characters without spaces.
system-software *file-name*	Specifies the name of the system software (*.cc) to be loaded to the new client.	The value is a string of 4 to 48 case-insensitive characters without spaces.
version	Specifies the version of a system software package, for example, V200R023C00. If the specified software version is the same as the software version running on the client, a software upgrade will not be performed for the client.	The value is a string of 11 to 32 case-insensitive characters without spaces.
patch *file-name*	Specifies the name of the patch file (*.pat) to be loaded to the new client.	The value is a string of 5 to 48 case-insensitive characters without spaces.
web-file *file-name*	Specifies the name of the web page file (*.web.7z or *.web.zip) to be loaded to the new client.	The value is a string of 8 to 64 case-insensitive characters without spaces.
license *file-name*	Specifies the name of the license file (*.dat) to be loaded to the new client. **NOTE** The license file is not supported in the Easy-Operation view. The file does not take effect even if you configure it.	The value is a string of 5 to 64 case-insensitive characters without spaces.

Parameter	Description	Value
custom-file *file-name*	Specifies the name of the user-defined file to be loaded to the new client. A maximum of three user-defined files can be specified. The file names are separated by spaces.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a client becomes faulty due to a hardware failure, run this command to add replacement information for the faulty client. After a new client is installed on the network to replace the faulty client, the new client can quickly obtain the configuration file of the faulty client, minimizing impact on services. You can also specify other files that can be loaded on the new client.

Precautions

- A new client finds matching replacement information by searching for its own MAC address or ESN; therefore, the mapping between the new client and MAC address or ESN must be configured. After finding matching information, the new client downloads the configuration file and other specified files of the faulty client from the file server.
- Before replacing the faulty client with a new client, ensure that the EasyDeploy function has been configured on the network and the **backup configuration interval** command has been run on the Commander to enable automatic configuration file backup. If this command has not been run, the new client cannot obtain the latest configuration file of the faulty client.
- This command can be run once or multiple times to configure the mappings between the new client and MAC address or ESN and specify information about the files to be downloaded.
- To delete all replacement information about a client, run the **undo client** *client-id* **replace** command. To delete an item from a client's replacement information, run the **undo** command with the item specified.
- This command is not recorded in the configuration file.

Example

Replace client 3 with a client that has a MAC address xxxx-xxxx-xxxx. The new client only needs to download the configuration file of client 3.


```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] client 3 replace mac-address xxxx-xxxx-xxxx
```

Replace client 3 with a client that has a MAC address xxxx-xxxx-xxxx. The new client needs to download the configuration file, system software, and user-defined file of client 3.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] client 3 replace mac-address xxxx-xxxx-xxxx
[HUAWEI-easyoperation] client 3 replace system-software test.cc V200R023C00
[HUAWEI-easyoperation] client 3 replace custom-file header.txt custom-file aaa.bat
```

2.2.11 cluster

Function

The **cluster** command displays the cluster view.

Format

cluster

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After entering the cluster view on the Commander, you can configure a cluster management VLAN and then configure the Commander as the network topology collection device so that the Commander only collects topology information of clients in the VLAN.

Example

Enter the cluster view.

```
<HUAWEI> system-view
[HUAWEI] cluster
[HUAWEI-cluster]
```

2.2.12 cluster enable

Function

The **cluster enable** command enables the cluster function.

The **undo cluster enable** command disables the cluster function.

The **cluster disable** command disables the cluster function.

By default, the cluster function is enabled.

Format

cluster enable

undo cluster enable

cluster disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before configuring the Commander as the network topology collection device, you need to configure a cluster management VLAN in the cluster view on the Commander so that the Commander only collects topology information of clients in the VLAN. Before configuring a cluster management VLAN on an S series switch, you must run the **cluster enable** command to enable the cluster function so that you can enter the cluster view.

Example

Enable the cluster function on a device.

```
<HUAWEI> system-view
[HUAWEI] cluster enable
```

2.2.13 cluster-multimac

Function

The **cluster-multimac** command assigns a multicast address to a cluster.

The **undo cluster-multimac** command restores the default multicast address of the cluster.

By default, the multicast address of the cluster is 0180-C200-000A.

Format

cluster-multimac *mac-address*

undo cluster-multimac

Parameters

Parameter	Description	Value
mac-address	Specifies the multicast MAC address of a cluster.	The value is in the format of H-H-H. Each H stands for a 4-digit hexadecimal number. The value ranges from 0180-C200-0004 to 0180-C200-0007, 0180-C200-0009 to 0180-C200-0010 and 0180-C200-0020 to 0180-C200-002F. The default value is 0180-C200-000A.

Views

Cluster view

Default Level

2: Configuration level

Usage Guidelines

Before setting up a cluster, you need to assign a multicast MAC address to the cluster or use the default multicast MAC address. To enhance the network security or if the default multicast MAC address is being used by other services on the network, you can reassign a multicast MAC address to the cluster within the permitted range. Once the cluster is set up, you cannot change the multicast MAC address of the cluster. All the devices in the cluster must be assigned the same multicast MAC address.

Example

Assign multicast address 0180-c200-0004 to a cluster.

```
<HUAWEI> system-view
[HUAWEI] cluster
[HUAWEI-cluster] cluster-multimac 0180-c200-0004
```

Restore the default multicast address of the cluster.

```
<HUAWEI> system-view
[HUAWEI] cluster
[HUAWEI-cluster] undo cluster-multimac
```

2.2.14 configuration-file

Function

The **configuration-file** command specifies the configuration file information to be downloaded by clients.

The **undo configuration-file** command deletes information about the configuration file to be downloaded.

Format

configuration-file *file-name*

undo configuration-file [*file-name*]

Parameters

Parameter	Description	Value
file-name	Specifies the name of the configuration file (*.zip or *.cfg) to be loaded to the client. A file path can be specified.	The value is a string of 5 to 48 case-insensitive characters without spaces.

Views

Easy-Operation view, Easy-Operation group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To deploy a zero touch client or reload a configuration file to clients, use this command to specify the configuration file.

Precautions

Information about the files to be downloaded can be set in the Easy-Operation view or Easy-Operation group view:

- The file information set in the Easy-Operation view is the default file information. If no file information is set in the group database or client database, the group or client uses the default file information.
- The files specified in the Easy-Operation group view can be downloaded by the clients that match the group.

NOTICE

The names of the files to be downloaded cannot be the same as system configuration files. Otherwise, the upgrade fails.

Example

Configure the default configuration file information.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] configuration-file easy/vrpcfg.zip
```

Configure the configuration file information for a MAC address-based group.


```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] group custom mac-address test
[HUAWEI-easyoperation-group-custom-test] configuration-file vrpcfg.zip
```

2.2.15 custom-file

Function

The **custom-file** command specifies a user-defined file to be downloaded by clients.

The **undo custom-file** command deletes the configured user-defined file information.

Format

{ **custom-file** *file-name* } &<1-3>

undo custom-file [*file-name*]

Parameters

Parameter	Description	Value
file-name	Specifies the name of a user-defined file to be loaded to the client. A file path can be specified. A maximum of three user-defined files can be specified. The file names are separated by spaces.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

Easy-Operation view, Easy-Operation group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When clients need to download user-defined files, such as batch processing file and login header file, use this command.

Precautions

Information about the files to be downloaded can be set in the Easy-Operation view or Easy-Operation group view:

- The file information set in the Easy-Operation view is the default file information. If no file information is set in the group database or client database, the group or client uses the default file information.

- The files specified in the Easy-Operation group view can be downloaded by the clients that match the group.

NOTICE

The names of the files to be downloaded cannot be the same as system user-defined files. Otherwise, the upgrade fails.

Example

Configure the default user-defined file information.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] custom-file easy/mydoc.bat
```

Configure the user-defined file information for a MAC address-based group.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] group custom mac-address test
[HUAWEI-easyoperation-group-custom-test] custom-file mydoc.bat custom-file header.txt
```

2.2.16 display easy-operation batch-cmd result

Function

The **display easy-operation batch-cmd result** command displays the batch configuration execution result.

Format

display easy-operation batch-cmd result

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the batch configuration execution result, run the **display easy-operation batch-cmd result** command. The result is saved in the memory of clients. If the script contains commands used to clear the client memory, such as the **reboot** command, the result cannot be checked using the **display easy-operation batch-cmd result** command after the commands are delivered to clients.

Example

Display the execution result of batch configuration.

```
<HUAWEI> display easy-operation batch-cmd result
This operation will take some seconds, please wait.....
-------------------------------------------------------------
 ID   Total  Successful    Failed    Time
-------------------------------------------------------------
  1     10         10         0    2013-09-12  12:57:02
  2     10         10         0    2013-09-12  12:57:02
  3     10         10         0    2013-09-12  12:57:02
-------------------------------------------------------------
```

Table 2-3 Description of the **display easy-operation batch-cmd result** command output

Item	Description
ID	Client ID.
Total	Total number of commands delivered.
Successful	Number of commands successfully executed.
Failed	Number of commands failed to be executed.
Time	Time when command execution was complete on the client.

2.2.17 display easy-operation client

Function

The **display easy-operation client** command displays client information on the Commander.

Format

display easy-operation client [*client-id* | **mac-address** *mac-address* | **esn** *esn* | **verbose**]

Parameters

Parameter	Description	Value
client-id	Displays detailed information about a client with a specified client ID.	The value is an integer. It depends on the maximum number of clients supported by the Commander. For details, see **Maximum Number of Managed Clients** on the Commander.
mac-address *mac-address*	Displays detailed information about a client with a specified MAC address.	The value is in the H-H-H format, where each H contains four hexadecimal digits.
esn *esn*	Displays detailed information about a client with a specified ESN.	The value is a string of 10 to 32 case-insensitive characters without spaces.
verbose	Displays detailed information about all clients.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays client information that the Commander dynamically obtains from a client, including the client's host name, MAC address, ESN, IP address, device type, and information about the files that have been downloaded to the client.

If the client state is UNKNOWN in the command output, the displayed MAC address and ESN are manually configured. If the client state is not UNKNOWN, the displayed MAC address and ESN values are dynamically obtained from the client. To modify the configuration of a client in a state other than UNKNOWN to match a new device, run the **undo client** *client-id* command to delete the current client configuration first.

If no optional parameter is specified in the command, the command displays brief client information dynamically obtained from the client database.

Example

Display brief client information.

```
<HUAWEI> display easy-operation client
The total number of client is : 4

--------------------------------------------------------------------------------
 ID   Mac address    ESN                 IP address       State
--------------------------------------------------------------------------------
 1    00E0-FC12-ABCD 2102113089P0xxxxxxxx      192.168.150.208  RUNNING
 2    00E0-FC12-0701 -                    -          INITIAL
 3    -              210235182810xxxxxxxx      192.168.150.210  INITIAL
 4    00E0-FC12-2123 210235276310xxxxxxxx      192.168.150.122  RUNNING
--------------------------------------------------------------------------------
```

Display detailed information about the client with MAC address 0018-1111-2123.

```
<HUAWEI> display easy-operation client mac-address 0018-1111-2123
--------------------------------------------------------------------------------
 Client ID                  : 4
 Host name                  : HUAWEI
 Mac address                : 00e0-fc12-3456
 ESN                        : 210235276310xxxxxxxx
 IP address                 : 192.168.150.122
 Model                      : S5728C-EI
 Device Type                : S5700-EI
 System-software file       : flash:/s5700-ei-v200r003c00.cc
 System-software version    : V200R003C00
 Configuration file         : flash:/122.cfg
 Patch file                 : -
 WEB file                   : -
 License file               : -
 System CPU usage           : 6%
 System Memory usage        : 55%
 Backup configuration file  : -
 Backup result              : -
 Last operation result      : -
 Last operation time        : 0000-00-00  00:00:00
 State                      : RUNNING
 Aging time left (hours)    : -
--------------------------------------------------------------------------------
```

Table 2-4 Description of the **display easy-operation client** command output

Item	Description
ID/Client ID	Client ID.
Host name	Client host name.
Mac address	Client MAC address.
ESN	Client ESN.
IP address	Client IP address.

Item	Description
State	Client status. • INITIAL: The client is performing initialization. The client information has been added to the Commander, but the client has not obtained an IP address, so the client cannot communicate with the Commander. • UPGRADING: The client is upgrading the software. • RUNNING: The client is running. • LOST: The Commander does not receive the response from the client in 2 minutes. A stack enters the LOST state when its system MAC address changes. • CONFIGURING: Batch configuration status. • UNKNOWN: The client status is unknown. This state rarely appears.
Model	Device model of the client.
Device Type	Device type of the client.
System-software file	Current system software name of the client.
System-software version	Current system version of the client.
Configuration file	Current configuration file name of the client.
Patch file	Current patch file name of the client.
WEB file	Current web page file name of the client.
License file	Current license file name of the client.
System CPU usage	CPU usage of the client.
System Memory usage	Memory usage of the client.
Backup configuration file	Current backup configuration file name of the client.
Last operation result	Last operation result.
Last operation time	Last operation time.
Backup result	File backup result.
Aging time left	Remaining aging time.

2.2.18 display easy-operation client replace

Function

The **display easy-operation client replace** command displays client replacement information on the Commander.

Format

display easy-operation client replace [**verbose**]

display easy-operation client *client-id* **replace**

Parameters

Parameter	Description	Value
verbose	Displays detailed client replacement information.	-
client-id	Displays replacement information about a client with a specified client ID.	The value is an integer. It depends on the maximum number of clients supported by the Commander. For details, see **Maximum Number of Managed Clients** on the Commander.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display easy-operation client** command displays brief client replacement information.

The replacement information is configured using the **client replace** command.

Example

Display brief client replacement information.

```
<HUAWEI> display easy-operation client replace
The total number of replacement information is :  1

------------------------------------------------------------
 ID     Replaced Mac     Replaced Esn     Status
```



```
-------------------------------------------------------------
 3      00e0-fc12-3456   -              enable
-------------------------------------------------------------
```

Display detailed client replacement information.

```
<HUAWEI> display easy-operation client replace verbose
-------------------------------------------------------------
 Client ID           : 3
 Mac address         : 00e0-fc12-3456
 ESN                 : -
 System-software file : -
 Configuration file   : 1.cfg
 Patch file          : -
 WEB file            : -
 License file        : -
 Customs file 1      : header.txt
 Customs file 2      : aaa.bat
 Customs file 3      : 1
 Status              : disable
-------------------------------------------------------------
```

Display replacement information of client 3.

```
<HUAWEI> display easy-operation client 3 replace
-------------------------------------------------------------
 Client ID           : 3
 Mac address         : 00e0-fc12-3456
 ESN                 : -
 System-software file : -
 Configuration file   : 1.cfg
 Patch file          : -
 WEB file            : -
 License file        : -
 Customs file 1      : header.txt
 Customs file 2      : aaa.bat
 Customs file 3      : 1
 Status              : disable
-------------------------------------------------------------
```

Table 2-5 Description of the **display easy-operation client replace** command output

Item	Description
ID/Client ID	Faulty client ID.
Replaced Mac/Mac address	New client MAC address.
Replaced Esn/ESN	New client ESN.
System-software file	System software to be downloaded by the new client.
Configuration file	Configuration file to be downloaded by the new client.
Patch file	Patch file to be downloaded by the new client.
WEB file	Web page file to be downloaded by the new client.

Item	Description
License file	License file to be downloaded by the new client.
Customs file 1	First user-defined file to be downloaded by the new client.
Customs file 2	Second user-defined file to be downloaded by the new client.
Customs file 3	Third user-defined file to be downloaded by the new client.
Status	Status of the replacement. • enable: This function is enabled. • disable: This function is not enabled.

2.2.19 display easy-operation configuration

Function

The **display easy-operation configuration** command displays the configurations on the Commander.

Format

display easy-operation configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command can be run on the Commander or clients.

- When the command is run on the Commander, the Commander role, Commander IP address and port number, file server information, and default downloaded file information are displayed.
- When the command is run on a client, the client role and Commander IP address and port number are displayed.

Example

Display EasyDeploy configuration on the Commander.

```
<HUAWEI> display easy-operation configuration
------------------------------------------------------------------------------
 Role                          : Commander
 Commander IP address          : 192.168.150.128
 Commander UDP port            : 60000
 DTLS status                   : Enable
 IP address of file server     : 192.168.150.200
 Type of file server           : SFTP
 Username of file server       : admin
 Default system-software file  : test.cc
 Default system-software version : -
 Default configuration file    : -
 Default patch file            : -
 Default WEB file              : -
 Default license file          : test.dat
 Default custom file 1         : mydoc.pat
 Default custom file 2         : header.txt
 Default custom file 3         : -
 Auto clear up                 : Disable
 Auto join in                  : Disable
 Topology collection           : Enable
 Activating file time          : In 00:00
 Activating file method        : Default
 Aging time of lost client(hours): -
 Backup configuration file mode  : Default
 Backup configuration file interval(hours): -
------------------------------------------------------------------------------
```

Display EasyDeploy configuration on a client.

```
<HUAWEI> display easy-operation configuration
------------------------------------------------------------------------------
 Role                        : Client
 Commander IP address        : 192.168.150.128(dhcp-alloc)
 Commander UDP port          : 60000
 DTLS status                 : Enable
------------------------------------------------------------------------------
```

Table 2-6 Description of the **display easy-operation configuration** command output

Item	Description
Role	Device role in the EasyDeploy service, which can be Commander or client.

Item	Description
Commander IP address	Commander IP address. It can be configured using the **easy-operation commander ip-address** command. If a client starts with a configuration file and obtains an IP address from a DHCP server, the client can also obtain the Commander IP address from the Option 148 field in the DHCP response message sent from the DHCP server. Therefore, the command output on a client shows whether a Commander IP address is configured using the command (configured) or obtained from the DHCP server (dhcp-alloc). If both two types of Commander IP addresses are available, the client uses the configured one. After the configured Commander IP address is deleted, the client uses the Commander IP address obtains from the DHCP server.
Commander UDP port	Port number used for communication between Commander and clients. It can be configured using the **easy-operation commander ip-address** command.
DTLS status	DTLS status.
IP address of file server	File server IP address. It can be configured using the **tftp-server** or **sftp-server** | **ftp-server** command.
Type of file server	File server type.
Username of file server	User name for accessing the file server.
Default system-software file	Default system software. If no default system software is specified, this field is empty. It can be configured using the **system-software** command.
Default system-software version	Default system software version. If no default system software is specified, this field is empty. It can be configured using the **system-software** command.

Item	Description
Default configuration file	Default configuration file. If no default configuration file is specified, this field is empty. It can be configured using the **configuration-file** command.
Default patch file	Default patch file. If no default patch file is specified, this field is empty. It can be configured using the **patch** command.
Default WEB file	Default web page file. If no default web page file is specified, this field is empty. It can be configured using the **web-file** command.
Default license file	Default license file. If no default license file is specified, this field is empty. It can be configured using the **license** command.
Default custom file 1	First default user-defined file. If no default user-defined file is specified, this field is empty. It can be configured using the **custom-file** command.
Default custom file 2	Second default user-defined file. If no default user-defined file is specified, this field is empty. It can be configured using the **custom-file** command.
Default custom file 3	Third default user-defined file. If no default user-defined file is specified, this field is empty. It can be configured using the **custom-file** command.
Auto clear up	Whether clients are enabled to automatically clear storage space. This function is configured using the **client auto-clear enable** command.

Item	Description
Auto join in	Whether clients are enabled to automatically join the management domain of the Commander. This function is configured using the **client auto-join enable** command.
Topology collection	Whether topology information collection is enabled. This function is configured using the **topology enable** command.
Activating file time	File activation time. If default file activation mode is used, this field displays **Immediately**. It can be configured using the **activate-file** command.
Activating file method	File activation mode. If default file activation mode is used, this field displays **Default**. It can be configured using the **activate-file** command.
Aging time of lost client(hours)	Aging time of a client in lost state. It can be configured using the **client aging-time** command.
Backup configuration file mode	Configuration file backup mode. If default mode is used, this field displays **Default**. It can be configured using the **backup configuration interval** command.
Backup configuration file interval(hours)	Configuration file backup interval. If configuration file backup is disabled, this field displays a hyphen (-). It can be configured using the **backup configuration interval** command.

2.2.20 display easy-operation device-information

Function

The **display easy-operation device-information** command displays device information.

Format

display easy-operation device-information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check device information, run the **display easy-operation device-information** command. The command output includes the MAC address, ESN, model, type, and active/standby state of the device.

This command can be run on the Commander or clients.

If the client is a stack, the displayed MAC address is the MAC address of the stack (MAC address of the master or backup device) and the displayed ESN is the ESN of the master device.

Example

Display the current device information.

```
<HUAWEI> display easy-operation device-information
System MAC: xxxx-xxxx-xxxx
Slot MAC          ESN               Model           Device-Type Role
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
0   xxxx-xxxx-xxxx  210235404310xxxxxxxx S5701-28X-LI-AC    S5700-X-LI  Master
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Table 2-7 Description of the **display easy-operation device-information** command output

Item	Description
System MAC	System MAC address.
Slot	Slot ID.
MAC	Device MAC address.
ESN	Device ESN.
Model	Device model.
Device-Type	Device type.
Role	Active/standby state.

2.2.21 display easy-operation download-status

Function

The **display easy-operation download-status** command displays file download status of clients on the Commander.

Format

display easy-operation download-status [**client** *client-id* | **verbose**]

Parameters

Parameter	Description	Value
client *client-id*	Displays the file download status of a client with a specified client ID.	The value is an integer. It depends on the maximum number of clients supported by the Commander. For details, see **Maximum Number of Managed Clients** on the Commander.
verbose	Displays detailed file download information of clients.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays file download status of clients, including client information (such as the client ID, MAC address, and IP address), scenario (zero touch device deployment, faulty device replacement, or batch upgrade), downloaded files, file download phase, and current status.

A client downloads files in the following sequence: system software, patch file, license file, web page file, configuration file, and user-defined file.

If the **client** *client-id* or **verbose** parameter is not specified, brief file download information of all clients is displayed.

Example

Display brief file download information of all clients.

```
<HUAWEI> display easy-operation download-status
--------------------------------------------------------------------------------
  ID    Mac address    IP address      Method      Phase         Status
--------------------------------------------------------------------------------
  1     00e0-fc12-3456 10.10.10.5      Zero-touch  Sys-file      Upgrading
  2     00e0-fc12-3333 10.10.10.6      Upgrade     Config-file   Failed
  3     00e0-fc12-1A52 10.10.10.7      Zero-touch  Patch-file    Waiting
  4     00e0-fc12-4458 10.10.10.8      Zero-touch  Web-file      Upgrading
--------------------------------------------------------------------------------
```

Display detailed file download information of client 5.

```
<HUAWEI> display easy-operation download-status verbose
The total number of client in downloading files is : 1


--------------------------------------------------------------------------------
 Client ID                  : 5
 Mac address                : 00e0-fc12-2323
 ESN                        : 210235362912xxxxxxxx
 Host name                  : RTF_1-54
 IP address                 : 192.168.14.252
 Method                     : Zero-touch
 IP address of file server  : 192.168.1.88
 Type of file server        : SFTP
 Username of file server    : 1
 Configuration file         : -
 System-software file       : -
 Patch file                 : -
 WEB file                   : -
 License file               : -
 Customs file 1             : -
 Customs file 2             : -
 Customs file 3             : -
 Activating file time       : Immediately
 Activating file method     : Default
 Phase                      : Unknown
 DownloadSize(byte)         : 29916738
 Status                     : Upgrading
 Reason                     : The device will enter getting download-information state.
 Description                : The device will enter getting download-information state.
--------------------------------------------------------------------------------
```

Table 2-8 Description of the **display easy-operation download-status** command output

Item	Description
ID/Client ID	Client ID.
Mac address	Client MAC address.
ESN	Client ESN.
Host name	Client host name.
IP address	Client IP address.

Item	Description
Method	EasyDeploy scenario. • Zero-touch: zero touch device deployment and faulty device replacement. • Upgrade: batch upgrade.
Phase	File download phase: Sys-file, Config-file, Patch-file, Web-file, License-file, Custom-file, Activating, Rebooting, and Unknown.
Status	File download status. • Upgrading: The client is downloading a file. • Waiting: The client is waiting for download. • Failed: The client fails to download a file because its storage space is insufficient or the file to be downloaded does not exist.
IP address of file server	File server IP address.
Type of file server	File server type.
Username of file server	User name for accessing the file server.
System-software file	System software that is being downloaded.
Configuration file	Configuration file that is being downloaded.
Patch file	Patch file that is being downloaded.
WEB file	Web page file that is being downloaded.
License file	License file that is being downloaded.
Customs file 1	First user-defined file that is being downloaded.
Customs file 2	Second user-defined file that is being downloaded.
Customs file 3	Third user-defined file that is being downloaded.

Item	Description
DownloadSize(byte)	Size of a downloaded file. **NOTE** If the system software is upgraded from V200R009 or an earlier version to V200R010 or a later version, this field displays -.
Activating file time	File activation time. **Immediately** indicates that files are activated immediately after they are downloaded.
Activating file method	File activation mode. **Default** indicates the default activation mode; **Reload** indicates that all files are activated by device resetting.
Reason	File download result. For possible results and solutions, see **Table 2-9**.
Description	Result description. For possible results and measures, see **Table 2-9**.

Table 2-9 Download results and solutions

Reason	Description	Solution
Input has been detected in the console	Input has been detected in the console. EasyOperation will stop	During zero touch device deployment, input is detected on the console interface of the device to be deployed, so EasyOperation stops. You are advised to restart the device to restart the deployment process. Do not input anything on the console interface during EasyOperation.
The USB upgrade is working	The USB upgrade is working. EasyOperation will stop	The device is performing USB-based deployment. USB-based deployment and EasyDeploy are mutually exclusive. You are advised to stop one of the two functions.

Reason	Description	Solution
The uni-mng system is working	The uni-mng system is working. EasyOperation will stop	The device is running SVF. SVF and EasyDeploy are mutually exclusive. You are advised to stop one of the two functions.
The device has in initial state	The device is in initial state. EasyOperation will stop	The device is in web initialization mode. Web initial login mode and EasyDeploy are mutually exclusive. You are advised to stop one of the two functions.
Getting download-information failed. The device will get download-information again	Getting download-information failed. The device will be back to initialization state.	The device to be deployed fails to obtain file download information. ● If the device is deployed using an intermediate file, check whether the intermediate file has the correct content and format, whether the network between the device and server that stores the intermediate file is normal, and whether the configured file server user name and password are correct. ● If the device is deployed using the Commander, check whether the network between the device and Commander is normal and whether the configured download information is correct.
Downloading file failed	The system software file and version are wrong. The device will be back to initialization state	The system software version is specified but the system software file is not specified. You need to specify the system software file.

<table>
<tr><th>Reason</th><th>Description</th><th>Solution</th></tr>
<tr><td rowspan="8"></td><td>Downloading the system software file failed. Please check the reason</td><td rowspan="8">1. Check whether a network fault occurs during file download.
2. Check whether the file server that stores files is working properly.
3. Check whether the file names of the system software, patch file, configuration file, license file, web file, and user-defined file are valid.
4. Check whether the system software, patch file, configuration file, license file, web file, and user-defined file to be downloaded have the same names as the current system files.
5. Check whether the device to be upgraded has enough disk space.</td></tr>
<tr><td>Downloading the patch file failed. Please check the reason</td></tr>
<tr><td>Downloading the web file failed. Please check the reason</td></tr>
<tr><td>Downloading the license file failed. Please check the reason</td></tr>
<tr><td>Downloading the configuration file failed. Please check the reason</td></tr>
<tr><td>Downloading the custom file 1 failed. Please check the reason</td></tr>
<tr><td>Downloading the custom file 2 failed. Please check the reason</td></tr>
<tr><td>Downloading the custom file 3 failed. Please check the reason</td></tr>
<tr><td>The file does not exist in the file server</td><td>The file does not exist in the file server</td><td>The file to be downloaded does not exist in the file server. Ensure that the file exists in the file server.</td></tr>
<tr><td>There is no enough space on the device</td><td>There is no enough space on master device or board</td><td>The disk space on the device to be upgraded is insufficient for the system software. Ensure that the device has enough disk space.</td></tr>
<tr><td>The file server is unreachable</td><td>The file server is unreachable</td><td>Check whether the configured file server IP address is correct and whether the network connection between the device and file server is normal.</td></tr>
</table>

Reason	Description	Solution
Authentication on file server fails	Authentication on file server fails	Authentication fails on the file server. Check whether the following configurations are correct: 1. User name and password 2. User management configuration on the file server 3. Other user management configurations
The filename is the same as the system file	The filename of the patch is same as the system patch file	The downloaded patch has the same file name as the system patch file.
	The filename of the system-software is same as the system file	The downloaded patch has the same file name as the system patch file.
Check file failed	System-software crc check error	The CRC check of the downloaded system software fails. Check whether the system software of the file server is correct.
The file is a system file on the other device	The file is system file on other device	The patch to be downloaded is the system file on the standby or slave device.

Reason	Description	Solution
Activate file failed. The device will be back to initialization state after 5 minutes	Activating file failed. The device will be back to initialization state after 5 minutes	File activation because of the following reasons: 1. Failed to set the system software, configuration file, and patch file as next startup files. Check whether these files are available. 2. Failed to start the device. Check whether the device has unsaved configuration, whether next startup files on the master and standby devices are consistent, and whether system files are damaged.
Reboot system failed	The WLAN configuration conflicts with the next startup system software. To prevent configuration loss, use the eDesk tool to convert the configuration, and then specify the new configuration file for next startup	The device has WLAN configurations, which may be lost when the device is upgraded. You need to export the WLAN configurations, use a dedicated tool to convert the configurations, and then import them for use.
Copying file to other device or board failed	Copying file to other device or board failed	Failed to copy files to the standby or slave device. Check whether the file system function is normal and whether boards are installed or removed when files are being copied.
	There is no enough space on other device or board	There is insufficient disk space on the standby or slave device when upgrade files are being copied to the standby or slave device. Ensure that the disk space is enough to store all the upgrade files.

Reason	Description	Solution
The download file was deleted	The download file was deleted in client, please check the environment	The downloaded upgrade files are deleted. Check whether other users have logged in to the device and deleted the files.
Unknown error	Unknown error	An unknown error occurs in the system. Contact technical support personnel.
EasyOperation client operation failed	The file server is not configured. Configure a file server first. Check whether a file server has been configured correctly	Check whether a file server has been configured correctly.

2.2.22 display easy-operation group

Function

The **display easy-operation group** command displays group information on the Commander.

Format

display easy-operation group [**build-in** [*device-type* [**vendor** *vendorname*]] | **custom** [*group-name*]]

Parameters

Parameter	Description	Value
build-in	Displays built-in group information. If the device type is not specified, information about all built-in groups is displayed.	-

Parameter	Description	Value
device-type	Specifies a device type.	The value is an enumerated type and case-insensitive. The following device types are supported: • S2730S-S • S2750-EI • S5700-10P-LI • S5700-EI • S5700-HI • S5700-P-LI • S5700-SI • S5700-TP-LI • S5700-X-LI • S5700S-LI • S5700S-P-LI • S5700S-X-LI • S5710-EI • S5710-HI • S5710-X-LI • S5720-EI • S5720-HI • S5720-LI • S5720-SI • S5720S-LI • S5730-HI • S5730-SI • S5730S-EI • S5731-H • S5731-S • S5731S-H • S5731S-S • S5732-H • S5735-L • S5735-L1 • S5735-L-I • S5735S-L • S5735S-L1 • S5735-S • S5735S-S • S5735S-H

Parameter	Description	Value
		• S5736-S • S6700-EI • S6720-EI • S6720-HI • S6720-LI • S6720-SI • S6720S-S • S6720S-LI • S6720S-SI • S6730-H • S6730S-H • S6730-S • S6730S-S • S6735-S • S9700
vendor *vendorname*	Displays the name of the group created based on the device type of the specified vendor. If no group name is specified, all vendor groups of the corresponding device types are displayed.	The value is a string of case-sensitive characters. It cannot contain spaces.
custom	Displays customized group information. If the group name is not specified, information about all customized groups is displayed.	-
group-name	Specifies the name of a customized group.	The value is a string of 1 to 31 case-sensitive characters without spaces. The character string must start with a letter.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays information about groups on the Commander.

If the **build-in** or **custom** parameter is not specified, brief information about all groups on the Commander is displayed.

Example

Display brief information about all groups on the Commander.

```
<HUAWEI> display easy-operation group
The total number of group configured is : 6
The number of build-in group is         : 2
The number of custom group is           : 4

-------------------------------------------------------------
 Groupname                      Type     MatchType
-------------------------------------------------------------
 AAA                          custom   ip-address
 F1                           custom   ip-address
S5720-HI                        build-in device-type
 test                         custom   mac-address
 test1                        custom   ip-address
-------------------------------------------------------------
```

Display information about built-in groups.

```
<HUAWEI> display easy-operation group build-in
-------------------------------------------------------------------------------
 Group name               : S5720-HI
 Configuration file       : vrpcfg.zip
 System-software file     : S5720-HI.cc
 Patch file               : -
 WEB file                 : -
 License file             : -
 Customs file 1           : -
 Customs file 2           : -
 Customs file 3           : -
 Activating file time     : Immediately
 Activating file method   : Default
-------------------------------------------------------------------------------
```

Display information about the customized group **AAA**.

```
<HUAWEI> display easy-operation group custom AAA
-------------------------------------------------------------------------------
 Group name               : AAA
 Configuration file       : -
 System-software file     : -
 Patch file               : -
 WEB file                 : -
 License file             : -
 Customs file 1           : header.txt
 Customs file 2           : -
 Customs file 3           : -
 Activating file time     : Immediately
 Activating file method   : Default
 Ip-address list          :
  Ip-address       Ip-mask
  192.168.150.110  255.255.255.0
  192.168.150.111  255.255.255.0
  192.168.150.112  255.255.255.0
  192.168.150.113  255.255.255.0
  192.168.150.114  255.255.255.0
  192.168.150.115  255.255.255.0
-------------------------------------------------------------------------------
```


Table 2-10 Description of the **display easy-operation group** command output

Item	Description
Groupname	Group name.
Type	Group type: build-in or custom.
MatchType	Match type of the group. The match type of a built-in group is configured using the **group build-in** command. The match type of a customized group is configured using the **group custom** command.
Configuration file	System software to be downloaded by the clients matching the group. If no system software is specified, this field displays a hyphen (-). It can be configured using the **configuration-file** command.
System-software file	Configuration file to be downloaded by the clients matching the group. If no configuration file is specified, this field displays a hyphen (-). It can be configured using the **system-software** command.
Patch file	Patch file to be downloaded by the clients matching the group. If no patch file is specified, this field displays a hyphen (-). It can be configured using the **patch** command.
WEB file	Web page file to be downloaded by the clients matching the group. If no system software is specified, this field displays a hyphen (-). It can be configured using the **web-file** command.
License file	License file to be downloaded by the clients matching the group. If no license file is specified, this field displays a hyphen (-). It can be configured using the **license** command.

Item	Description
Customs file 1	First user-defined file to be downloaded by the clients matching the group. If no system software is specified, this field displays a hyphen (-). It can be configured using the **custom-file** command.
Customs file 2	Second user-defined file to be downloaded by the clients matching the group. If no system software is specified, this field displays a hyphen (-). It can be configured using the **custom-file** command.
Customs file 3	Third user-defined file to be downloaded by the clients matching the group. If no third user-defined file is specified, this field displays a hyphen (-). It can be configured using the **custom-file** command.
Activating file time	File activation time used by the clients matching the group. If default file activation time is used, this field displays **Immediately**. It can be configured using the **activate-file** command.
Activating file method	File activation mode used by the clients matching the group. If default mode is used, this field displays **Default**. It can be configured using the **activate-file** command.

Item	Description
Ip-address list	Clients match the group based on IP addresses, and all matching IP addresses are displayed. • If clients match the group based on ESNs, **ESN list** is displayed. • If clients match the group based on MAC addresses, **Match mac-address list** is displayed. • If clients match the group based on models, **Product model** is displayed. • If clients match the group based on types, **Device type** is displayed. The matching rule can be configured using the **match** command.

2.2.23 display easy-operation power

Function

The **display easy-operation power** command displays power consumption information of the Commander and clients.

Format

display easy-operation power [**client** *client-id* | **commander**]

Parameters

Parameter	Description	Value
client *client-id*	Indicates power consumption information of a specified client.	The value is an integer. It depends on the maximum number of clients supported by the Commander. For details, see **Maximum Number of Managed Clients** on the Commander.
commander	Indicates power consumption information of the Commander.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command used to check power consumption information differs on the Commander and clients.

- On the Commander
  - If no parameter is specified, you can check power consumption information about the Commander and all the clients in initial, upgrade, and normal operating states.
  - If only **client** *client-id* is specified, you can check power consumption information about the specified client.
  - If only **commander** is specified, you can check power consumption information about the Commander.
- On the client

  The parameters **client** *client-id* and **commander** are not supported. You can check power consumption information only about the current client.

Example

Display power consumption information of the Commander and clients.

```
<HUAWEI> display easy-operation power
--------------------------------------------------------------------------------
Role       HostName                  Interface     Usage(W)  Gauge  Mode
--------------------------------------------------------------------------------
Commander  HUAWEI                                    995.0     actual standard
Client1    HUAWEI                                    511.3     rated  standard
                                     GE0/0/1         0.7       actual
Client3    HUAWEI                                    93.0      rated  standard
Client4    HUAWEI                                    100.0     rated  standard
--------------------------------------------------------------------------------
```

Table 2-11 Description of the **display easy-operation power** command output

Item	Description
Role	Device role in the EasyDeploy service, which can be Commander or client.
HostName	Device name.
Interface	Interface name: • If this parameter is left blank, power consumption of the entire device is displayed. • If an interface name is specified, power consumption of a power device connected to the corresponding interface is displayed.
Usage(W)	Power consumption, in Watts.

Item	Description
Gauge	Power consumption type: • actual: indicates real-time power consumption. • rated: indicates rated power consumption.
Mode	Energy saving mode: • standard • basic • deep

2.2.24 display easy-operation topology

Function

The **display easy-operation topology** command displays network topology information collected by the Commander.

Format

display easy-operation topology

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view network topology information collected by the Commander. Based on the collected information, zero touch device deployment and automatic faulty device replacement can be implemented.

Example

Display network topology information collected by the Commander.

```
<HUAWEI> display easy-operation topology
<-->:normal device        <??>:lost device
Total topology node number: 3
------------------------------------------------------------------------------
```



```
[HUAWEI: xxxx-xxxx-xxxx](Commander)
|-(GE0/0/8)<-->(GE0/0/38)[HUAWEI: xxxx-xxxx-xxxx](Client 1)
| |-(GE0/0/16)<-->(GE0/0/16)[HUAWEI: xxxx-xxxx-xxxx] (Client 2)
```

Table 2-12 Description of the **display easy-operation topology** command output

Item	Description
<-->	Clients that are running properly.
<??>	Properly operating clients change to the lost state.
Total topology node number	Number of nodes (including the Commander) in the network topology.

2.2.25 display ndp

Function

The **display ndp** command displays the global NDP information or the NDP information on a specified interface.

Format

display ndp [**interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>]

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] }	Displays the NDP information on a specified interface. • *interface-type interface-number1* indicates the type and number of the first interface. • *interface-type interface-number2* indicates the type and number of the last interface. If no interface is specified when you run the **display ndp** command, NDP information about all interfaces is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you check the NDP information:

- If NDP is not globally enabled, only the current NDP status of a switch is displayed.
- If NDP is globally enabled, the global NDP information and status and the NDP information and status of interfaces on a switch are displayed.

Example

Display the global NDP information and NDP information about all the interfaces.

```
<HUAWEI> display ndp
 Neighbor discovery protocol is enabled.
 Neighbor Discovery Protocol Ver: 1, Hello Timer: 60(s), Aging Timer: 180(s)
 Interface: GigabitEthernet0/0/1
    Status: Enabled, Packets Sent: 114, Packets Received: 108, Packets Error: 0
    Neighbor 1:  Aging Time: 174(s)
       MAC Address : xxxx-xxxx-xxxx
       Port Name   : GigabitEthernet0/0/1
       Software Version: Version 5.130 V200R023C00
       Device Name : S5720
       Port Duplex : FULL
       Product Ver : S5720 V200R023C00
---- More ----
```

Table 2-13 Description of the **display ndp** command output

Item	Description
Neighbor discovery protocol is *status*	The global NDP function is in *status* state. *status* includes: • disabled: NDP is disabled globally. • enabled: NDP is enabled globally. To set this value, run the **ndp enable (system view)** command.
Neighbor Discovery Protocol Ver	Currently supported NDP versions. Version 1 is currently supported by all devices.
Hello Timer	Interval for sending NDP packets, in seconds. To set this value, run the **ndp timer hello** command.
Aging Timer	Aging time of NDP information, in seconds. To set this value, run the **ndp timer aging** command.
Interface	Interface number of a switch.

Item	Description
Status	NDP status of an interface: ● Disabled: NDP is disabled on the interface. ● Enabled: NDP is enabled on the interface. To set this value, run the **ndp enable (system view)** or **ndp enable (interface view)** command.
Packets Sent	Number of NDP packets sent from the interface.
Packets Received	Number of NDP packets received by the interface.
Packets Error	Number of incorrect NDP packets received by the interface.
Neighbor 1	Neighboring node 1.
Aging Time	Aging time of NDP information about a neighboring node connected to the interface.
MAC Address	MAC address of the neighboring node.
Port Name	Name of the interface on the neighboring node connected to the interface.
Software Version	Version of the system software on the neighboring node.
Device Name	Host name of the neighboring node.
Port Duplex	Duplex mode of the interface on the neighboring node connected to the local interface. ● FULL: full-duplex. ● Half: half-duplex.
Product Ver	Type and software version number of the neighboring node.

Display the NDP information of the switch on which NDP is not globally enabled.

```
<HUAWEI> display ndp
 Neighbor discovery protocol is disabled.
 Neighbor Discovery Protocol Ver: 1, Hello Timer: 60(s), Aging Timer: 180(s)
```


2.2.26 display ntdp

Function

The **display ntdp** command displays NTDP configuration.

Format

display ntdp

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ntdp** command to check the NTDP configuration of a switch without considering whether NTDP is enabled globally or on interfaces on the switch.

Example

Display the NTDP configuration of a switch.

```
<HUAWEI> display ntdp
Network topology discovery protocol is enabled
Hops      : 8
Timer     : 0 min
Hop Delay : 200 ms
Port Delay: 20 ms
Total time for last collection: 330 ms
```

Table 2-14 Description of the **display ntdp** command output

Item	Description
Network topology discovery protocol is *status*	The global NTDP function is in *status* state. *status* includes the following types of status: • disabled: NTDP is disabled globally. • enabled: NTDP is enabled globally. To set this value, run the **ntdp enable (system view)** command.

Item	Description
Hops	Topology collection range (the number of hops). To set this value, run the **ntdp hop** command.
Timer	Interval for collecting topology information. To set this value, run the **ntdp timer** command.
Hop Delay	Delay for the first interface to forward NTDP topology request packets. To set this value, run the **ntdp timer hop-delay** command.
Port Delay	Delay for other interfaces to forward NTDP topology request packets. To set this value, run the **ntdp timer port-delay** command.
Total time for last collection	Duration for collecting topology information last time.

2.2.27 display ntdp device-list

Function

The **display ntdp device-list** command displays the topology information collected using NTDP.

Format

display ntdp device-list [**verbose**]

Parameters

Parameter	Description	Value
verbose	Displays detailed device information. If you run the **display ntdp device-list** command without setting optional parameters, brief information about the device is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check the topology information collected using NTDP, run the **display ntdp device-list** command. The topology information can be displayed only after **ntdp explore** command is run in the user view to enable the switch to periodically collect the topology information.

When NTDP is not enabled on interfaces of the switch, only information about the switch itself is collected using NTDP.

Prerequisites

NTDP has been globally enabled on the switch.

Example

Display brief switch information collected using NTDP.

```
<HUAWEI> display ntdp device-list
The device-list of NTDP:
--------------------------------------------------------------------------------
 MAC             HOP  IP               PLATFORM
--------------------------------------------------------------------------------
 xxxx-xxxx-xxxx  0                    S5700
 xxxx-xxxx-xxxx  1    10.1.1.2/24       S5700
 xxxx-xxxx-xxxx  1    10.1.1.3/24       S5700
```

Table 2-15 Description of the **display ntdp device-list** command output

Item	Description
MAC	MAC address of the device.
HOP	Number of hops from the device to the topology collecting device.
IP	IP address of the device.
PLATFORM	Type of the device.

Display detailed device information collected using NTDP.

```
<HUAWEI> display ntdp device-list verbose
 Hostname  : HUAWEI
 MAC       : xxxx-xxxx-xxxx
 Hop       : 0
 Platform  : S5700
 IP        :
 Version   : Version 5.150 V200R023C00
 Cluster   : Administrator switch of cluster
 Peer MAC        Native Port ID Peer Port ID   N-Index    P-Index    Speed Dup
 xxxx-xxxx-xxxx  GE0/0/4        GE0/0/4        9          9          1000  FULL
 xxxx-xxxx-xxxx  GE0/0/1        GE0/0/1        6          6          1000  FULL

--------------------------------------------------------------------------------

 Hostname  : HUAWEI
 MAC       : xxxx-xxxx-xxxx
 Hop       : 1
```

```
Platform  : S5700
IP        : 10.1.1.2/24
Version   : Version 5.150 V200R023C00
Cluster   : Candidate switch

Peer MAC        Native Port ID Peer Port ID   N-Index    P-Index    Speed Dup
xxxx-xxxx-xxxx  GE0/0/4        GE0/0/4        9          9          1000   FULL

--------------------------------------------------------------------------------

Hostname  : HUAWEI
MAC       : xxxx-xxxx-xxxx
Hop       : 1
Platform  : S5700
IP        : 10.1.1.3/24
Version   : Version 5.150 V200R023C00
Cluster   : Candidate switch

Peer MAC        Native Port ID Peer Port ID   N-Index    P-Index    Speed Dup
xxxx-xxxx-xxxx  GE0/0/1        GE0/0/1        6          6          1000   FULL
```

Table 2-16 Description of the **display ntdp device-list verbose** command output

Item	Description
Hostname	Host name of the device.
MAC	MAC address of the device.
Hop	Number of hops from the device to the topology collecting device.
Platform	Model of the device.
IP	Private IP address of the device.
Version	Version of the system software running on the device.
Cluster	Role of the device in the cluster.
Peer MAC	MAC address of the neighboring node.
Native Port ID	Interface of the device connecting to the neighboring node.
Peer Port ID	Interface of the neighboring node connecting to the local device.
N-Index	Index of the local interface.
P-Index	Index of the peer interface.
Speed	Rate of the interface when the neighboring node is connected to the device.
Dup	Duplex mode of the interface when the neighboring node is connected to the local device.

2.2.28 display cluster-topology-info

Function

The **display cluster-topology-info** command displays the topology information about the cluster.

Format

display cluster-topology-info

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display cluster-topology-info** command on the Commander switch only.

NOTE

If two devices are connected through multiple interfaces, this command displays information only about the link established between a pair of interfaces.

Example

Display the topology information about the cluster.

```
<HUAWEI> display cluster-topology-info
The topology information about the cluster:
<-->:normal device        <++>:candidate device        <??>:lost device
------------------------------------------------------------------------------
Total topology node number is 5.
[HUAWEI_0.Administrator: Root-00e0-ad14-c600]
|-(GigabitEthernet0/0/2)<-->(GigabitEthernet0/0/1)[HUAWEI_3.Member-3: xxxx-xxxx-xxxx]
| |-(GigabitEthernet0/0/3)<-->(GigabitEthernet0/0/1)[HUAWEI_2.Member-2: xxxx-xxxx-xxxx]
| | |-(GigabitEthernet0/0/1)<-->(GigabitEthernet0/0/1)[HUAWEI_1.Member-1: xxxx-xxxx-xxxx]
|-(GigabitEthernet0/0/1)<-->(GigabitEthernet0/0/2)[HUAWEI_4.Member-4: xxxx-xxxx-xxxx]
```

Table 2-17 shows the description of the **display cluster-topology-info** command output.

Table 2-17 Description of the **display cluster-topology-info** command output

Item	Description
<-->	Normal link.

Item	Description
<++>	Candidate link.
<??>	Faulty link.
Total topology node number is	Specifies the number of nodes in the topology of the cluster.
[HUAWEI_0.Administrator: Root-xxxx-xxxx-xxxx]	Specifies the MAC address and host name of the switch. It varies with the name and MAC address of the device.
|-	Indicates the level-1 device that is connected to the root node.
| |-	Indicates the level-2 device which is connected to the level-1 device.
| | |-	Indicates the level-3 device which is connected to the level-2 device.
(GigabitEthernet0/0/1)<-->(GigabitEthernet0/0/2)	Specifies the names of the interfaces connecting the two devices. It varies with the interfaces of the devices. The left brackets contain information about the upper-level device. The right brackets contain information about the lower-level device.
[HUAWEI_3.Member-3: xxxx-xxxx-xxxx]	Specifies the MAC address of the member device. It varies with the name and MAC address of the device.

2.2.29 easy-operation

Function

The **easy-operation** command displays the Easy-Operation view.

Format

easy-operation

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To specify the file server, information about files to be downloaded, and file activation mode, or configure other EasyDeploy-related functions, first run the **easy-operation** command to enter the Easy-Operation view.

Prerequisites

You can enter the Easy-Operation view only on the device functions as a Commander.

After choosing a device as the Commander, run the **easy-operation commander ip-address** command on the device to configure the Commander IP address, and then run the **easy-operation commander enable** command to enable the Commander function.

Example

Enter the Easy-Operation view.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation]
```

2.2.30 easy-operation client ftp-server

Function

The **easy-operation client ftp-server** command specifies IP addresses, user names, and passwords for FTP servers on a pre-delivery device.

The **undo easy-operation client ftp-server** command deletes the specified IP addresses, user names, and passwords of FTP servers on a pre-delivery device.

By default, IP addresses, user names, and passwords of FTP servers are not specified on pre-delivery devices.

Format

easy-operation client ftp-server ip-address *ipaddress* &<1-4> [**username** *username* [**password** *password*]]

undo easy-operation client ftp-server ip-address [*ipaddress*] [**username** *username*] [**password**]

Parameters

Parameter	Description	Value
ip-address *ipaddress*	Specifies the IP address of an FTP server.	The value is in dotted decimal notation.

Parameter	Description	Value
username *username*	Specifies a user name for FTP server access.	The value is a string of 1 to 64 characters.
password *password*	Specifies a password for FTP server access.	The value is a string of 1 to 16 characters in plaintext or 48 characters in ciphertext.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a device obtains file information to be downloaded from an intermediate file, it must download the specified files from file servers. To allow the device to visit the servers, run the **easy-operation client ftp-server** command to specify IP addresses, user names, and passwords for the servers.

Precautions

- The **easy-operation client ftp-server** command is contained only in a device's pre-delivery configuration file. It is not allowed to run this command after device delivery.
- If you do not want to use the pre-configured device deployment function, run the **undo easy-operation client ftp-server** command in the system view to delete the specified IP addresses, user names, and passwords of FTP servers.
- If a user name and a password have been set on a file server, the device must have the same user name and password configured.
- FTP has security risks. Using an SFTP file server is recommended.
- A maximum of four FTP file servers' IP addresses, user names, and passwords can be specified. A device searches for and obtains the desired files from the servers in the sequence in which file servers are configured.
- Ensure that the files to be downloaded have been uploaded to the specified file servers.

Example

Delete the IP address, user name, and password of an FTP server.

```
<HUAWEI> system-view
[HUAWEI] undo easy-operation client ftp-server ip-address 10.1.1.1 username huawei password
```


2.2.31 easy-operation client ftp-server-url

Function

The **easy-operation client ftp-server-url** command specifies URLs, user names, and passwords for FTP servers on a pre-delivery device.

The **undo easy-operation client ftp-server-url** command deletes the specified URLs, user names, and passwords of FTP servers on a pre-delivery device.

By default, URLs, user names, and passwords of FTP servers are not specified on pre-delivery devices.

Format

easy-operation client ftp-server-url *url-address* [**username** *username* [**password** *password*]]

undo easy-operation client ftp-server-url [*url-address*] [**username** *username*] [**password**]

Parameters

Parameter	Description	Value
url-address	Specifies the URL of an FTP server.	The value is a string of 1 to 64 characters.
username *username*	Specifies a user name for FTP server access.	The value is a string of 1 to 64 characters.
password *password*	Specifies a password for FTP server access.	The value is a string of 1 to 16 characters in plaintext or 48 characters in ciphertext.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a device obtains file information to be downloaded from an intermediate file, it must download the specified files from file servers. To allow the device to visit the servers, run the **easy-operation client ftp-server-url** command to specify URLs, user names, and passwords for the servers.

Precautions

The **easy-operation client ftp-server-url** command is contained only in a device's pre-delivery configuration file. It is not allowed to run this command after device delivery.

If you do not want to use the pre-configured device deployment function, run the **undo easy-operation client ftp-server-url** command in the system view to delete the specified URLs, user names, and passwords of FTP servers.

You can specify an FTP server using either an IP address or URL.

Example

Delete the URL, user name, and password of an FTP server.

```
<HUAWEI> system-view
[HUAWEI] undo easy-operation client ftp-server-url www.1234.com username huawei password
```

2.2.32 easy-operation client netfile

Function

The **easy-operation client netfile** command specifies a name for an intermediate file for pre-configured device deployment.

The **undo easy-operation client netfile** command deletes the name of an intermediate file for pre-configured device deployment.

By default, devices use the intermediate file **lswnet.cfg** for pre-configured device deployment.

Format

easy-operation client netfile *filename*

undo easy-operation client netfile [*filename*]

Parameters

Parameter	Description	Value
filename	Specifies the name (*.cfg) of an intermediate file.	The value is a string of 5 to 48 characters.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A pre-configured device obtains version file information from an intermediate file placed on a file server. This information includes an SNMP host's IP address, device's MAC address, ESN or model, and names of files to be downloaded.

If you do not specify an intermediate file, the device uses the **lswnet.cfg** file by default. If you want to use another intermediate file, run the **easy-operation client netfile** command.

Precautions

The **easy-operation client netfile** command is contained only in a device's pre-delivery configuration file. It is not allowed to run this command after device delivery.

If you do not want to use pre-configured device deployment, run the **undo easy-operation client netfile** command in the system view to delete the intermediate file.

The configuration file specified in an intermediate file cannot contain any pre-configured commands.

Example

Delete the intermediate file specified for pre-configured device deployment.

```
<HUAWEI> system-view
[HUAWEI] undo easy-operation client netfile huawei.cfg
```

2.2.33 easy-operation client sftp-server

Function

The **easy-operation client sftp-server** command specifies IP addresses, user names, and passwords for SFTP servers on a pre-delivery device.

The **undo easy-operation client sftp-server** command deletes the specified IP addresses, user names, and passwords of SFTP servers on a pre-delivery device.

By default, IP addresses, user names, and passwords of SFTP servers are not specified on pre-delivery devices.

Format

easy-operation client sftp-server ip-address *ipaddress* &<1-4> [**username** *username* [**password** *password*]]

undo easy-operation client sftp-server ip-address [*ipaddress*] [**username** *username*] [**password**]

Parameters

Parameter	Description	Value
ip-address *ipaddress*	Specifies the IP address of an SFTP server.	The value is in dotted decimal notation.

Parameter	Description	Value
username *username*	Specifies a user name for SFTP server access.	The value is a string of 1 to 64 characters.
password *password*	Specifies a password for SFTP server access.	The value is a string of 1 to 16 characters in plaintext or 48 characters in ciphertext.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a device obtains file information to be downloaded from an intermediate file, it must download the specified files from file servers. To allow the device to visit the servers, run the **easy-operation client sftp-server** command to specify IP addresses, user names, and passwords for the servers.

Precautions

- The **easy-operation client sftp-server** command is contained only in a device's pre-delivery configuration file. It is not allowed to run this command after device delivery.
- If you do not want to use the pre-configured device deployment function, run the **undo easy-operation client sftp-server** command in the system view to delete the specified IP addresses, user names, and passwords of SFTP servers.
- If a user name and a password have been set on a file server, the device must have the same user name and password configured.
- A maximum of four SFTP file servers' IP addresses, user names, and passwords can be specified. A device searches for and obtains the desired files from the servers in the sequence in which file servers are configured.
- Ensure that the files to be downloaded have been uploaded to the specified file servers.

Example

Delete the IP address, user name, and password of an SFTP server.

```
<HUAWEI> system-view
[HUAWEI] undo easy-operation client sftp-server ip-address 10.1.1.1 username huawei password
```


2.2.34 easy-operation client sftp-server-url

Function

The **easy-operation client sftp-server-url** command specifies URLs, user names, and passwords for SFTP servers on a pre-delivery device.

The **undo easy-operation client sftp-server-url** command deletes the specified URLs, user names, and passwords of SFTP servers on a pre-delivery device.

By default, URLs, user names, and passwords of SFTP servers are not specified on pre-delivery devices.

Format

easy-operation client sftp-server-url *url-address* [**username** *username* [**password** *password*]]

undo easy-operation client sftp-server-url [*url-address*] [**username** *username*] [**password**]

Parameters

Parameter	Description	Value
url-address	Specifies the URL of an SFTP server.	The value is a string of 1 to 64 characters.
username *username*	Specifies a user name for SFTP server access.	The value is a string of 1 to 64 characters.
password *password*	Specifies a password for SFTP server access.	The value is a string of 1 to 16 characters in plaintext or 48 characters in ciphertext.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a device obtains file information to be downloaded from an intermediate file, it must download the specified files from file servers. To allow the device to visit the servers, run the **easy-operation client sftp-server-url** command to specify URLs, user names, and passwords for the SFTP servers on the device.

Precautions

- The **easy-operation client sftp-server-url** command is contained only in a device's pre-delivery configuration file. It is not allowed to run this command after device delivery.
- If you do not want to use the pre-configured device deployment function, run the **undo easy-operation client sftp-server-url** command in the system view to delete the specified URLs, user names, and passwords of SFTP servers.
- You can specify an SFTP server using either an IP address or URL.
- If a user name and a password have been set on a file server, the device must have the same user name and password configured.
- Ensure that the files to be downloaded have been uploaded to the specified file servers.

Example

Delete the URL, user name, and password of an SFTP server.

```
<HUAWEI> system-view
[HUAWEI] undo easy-operation client sftp-server-url www.1234.com username huawei password
```

2.2.35 easy-operation client snmp securityname

Function

The **easy-operation client snmp securityname** command configures a shared key between a pre-delivery device and an SNMP host.

The **undo easy-operation client snmp securityname** command deletes a shared key between a pre-delivery device and an SNMP host.

By default, no shared key is configured between pre-delivery devices and SNMP hosts.

Format

easy-operation client snmp securityname cipher *password*

undo easy-operation client snmp securityname

Parameters

Parameter	Description	Value
cipher *password*	Specifies a shared key.	The value is a string of 1 to 32 characters in plaintext, or 48 or 68 characters in ciphertext.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In pre-configured device deployment, a pre-delivery device sends alarms to an NMS over an SNMP module for deployment monitoring. To configure a shared key between the device and the SNMP host, run the **easy-operation client snmp securityname** command.

Precautions

The **easy-operation client snmp securityname** command is contained only in a device's pre-delivery configuration file. It is not allowed to run this command after device delivery.

If you do not want to use the pre-configured device deployment function, run the **undo easy-operation client snmp securityname** command in the system view to delete the shared key.

Example

Delete the shared key between a pre-delivery device and an SNMP host.

```
<HUAWEI> system-view
[HUAWEI] undo easy-operation client snmp securityname
```

2.2.36 easy-operation client tftp-server

Function

The **easy-operation client tftp-server** command specifies IP addresses for TFTP servers on a pre-delivery device.

The **undo easy-operation client tftp-server** command deletes the specified IP addresses of TFTP servers on a pre-delivery device.

By default, IP addresses of TFTP servers are not specified on pre-delivery devices.

Format

easy-operation client tftp-server ip-address *ipaddress* &<1-4>

undo easy-operation client tftp-server ip-address [*ipaddress*]

Parameters

Parameter	Description	Value
ip-address *ipaddress*	Specifies the IP address of a TFTP server.	The value is in dotted decimal notation.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a device obtains file information to be downloaded from an intermediate file, it must download the specified files from file servers. To allow the device to visit the servers, run the **easy-operation client ftp-server** command to specify IP addresses for the servers.

Precautions

- The **easy-operation client tftp-server** command is contained only in a device's pre-delivery configuration file. It is not allowed to run this command after device delivery.
- If you do not want to use the pre-configured device deployment function, run the **undo easy-operation client tftp-server** command in the system view to delete the specified IP addresses of TFTP servers.
- TFTP has security risks. Using an SFTP file server is recommended.
- A maximum of four TFTP file servers' IP addresses can be specified. A device searches for and obtains the desired files from the servers in the sequence in which file servers are configured.
- Ensure that the files to be downloaded have been uploaded to the specified file servers.

Example

Delete the IP address of a TFTP server.

```
<HUAWEI> system-view
[HUAWEI] undo easy-operation client tftp-server ip-address 10.1.1.1
```

2.2.37 easy-operation client tftp-server-url

Function

The **easy-operation client tftp-server-url** command specifies URLs for TFTP servers on a pre-delivery device.

The **undo easy-operation client tftp-server-url** command deletes the specified URLs of TFTP servers on a pre-delivery device.

By default, URLs of TFTP servers are not specified on pre-delivery devices.

Format

easy-operation client tftp-server-url *url-address*

undo easy-operation client tftp-server-url [*url-address*]

Parameters

Parameter	Description	Value
url-address	Specifies the URL of a TFTP server.	The value is a string of 1 to 64 characters.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a device obtains file information to be downloaded from an intermediate file, it must download the specified files from file servers. To allow the device to visit the servers, run the **easy-operation client tftp-server-url** command to specify URLs for the servers.

Precautions

The **easy-operation client tftp-server-url** command is contained only in a device's pre-delivery configuration file. It is not allowed to run this command after device delivery.

If you do not want to use the pre-configured device deployment function, run the **undo easy-operation client tftp-server-url** command in the system view to delete the specified URLs of TFTP servers.

You can specify either an IP address or URL for a TFTP server.

Example

Delete the URL of a TFTP server.

```
<HUAWEI> system-view
[HUAWEI] undo easy-operation client tftp-server-url www.1234.com
```

2.2.38 easy-operation client vlan

Function

The **easy-operation client vlan** command specifies the VLAN used in the configured device deployment procedure before device delivery.

The **undo easy-operation client vlan** command deletes the VLAN used in the configured device deployment procedure.

By default, the VLAN used in the configured device deployment procedure is VLAN 1.

Format

easy-operation client vlan *vlanid*

undo easy-operation client vlan

Parameters

Parameter	Description	Value
vlanid	Specifies the VLAN used in the configured device deployment procedure.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

You can use the default VLAN 1 or run this command to specify the VLAN used in the configured device deployment procedure to implement configured device deployment.

Precautions

- This command is an overwritten command.
- The **easy-operation client vlan** command is contained only in a device's pre-delivery configuration file. Users cannot manually run this command. The **undo easy-operation client vlan** command can be manually run.

Example

Delete the VLAN used in the configured device deployment procedure.

```
<HUAWEI> system-view
[HUAWEI] undo easy-operation client vlan
```

2.2.39 easy-operation client ztp-with-cfg enable

Function

The **easy-operation client ztp-with-cfg enable** command enables pre-configured device deployment.

The **undo easy-operation client ztp-with-cfg enable** command disables pre-configured device deployment.

By default, pre-configured device deployment is disabled.

Format

easy-operation client ztp-with-cfg enable

undo easy-operation client ztp-with-cfg enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before delivery, a device can load a configuration file that contains commands for specifying file server addresses, name of an intermediate file for site deployment, and a shared key between the device and an SNMP host. After simple login configuration, the device can then automatically obtain and load correct configurations, reducing the manual operation cost.

Precautions

The **easy-operation client ztp-with-cfg enable** command is contained only in a device's pre-delivery configuration file. It is not allowed to run this command after device delivery.

If you do not need the pre-configured device deployment function, run the **undo easy-operation client ztp-with-cfg enable** command in the system view to disable this function.

Example

Disable the pre-configured device deployment function on a device.

```
<HUAWEI> system-view
[HUAWEI] undo easy-operation client ztp-with-cfg enable
```

2.2.40 easy-operation commander enable

Function

The **easy-operation commander enable** command enables the Commander function on a device.

The **undo easy-operation commander enable** command disables the Commander function on a device.

By default, the Commander function is disabled on a device.

Format

easy-operation commander enable

undo easy-operation commander enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To specify a device as the Commander, enable the Commander function on the device. The Commander can enable devices to automatically download files in zero touch device deployment, fault device replacement, and batch upgrade scenarios. On an EasyDeploy network, the Commander manages clients and delivers required information, including file server information, system software name, and configuration file name, to clients. Clients automatically download required files according to information obtained from the Commander.

Prerequisites

The Commander IP address has been configured on the device using the **easy-operation commander ip-address** command.

Precautions

- An EasyDeploy network has only one Commander.
- This command can be used only on the device that functions as the Commander.
- After you run the **undo easy-operation commander enable** command to disable the Commander function, dynamic information in the client database is deleted, and the configuration information is saved in the memory of the device. If the Commander does not restart after the Commander function is disabled, the configuration will be recovered after the Commander function is enabled again.

Example

Enable the Commander function on a device.

```
<HUAWEI> system-view
[HUAWEI] easy-operation commander enable
```


2.2.41 easy-operation commander ip-address

Function

The **easy-operation commander ip-address** command configures the Commander IP address.

The **undo easy-operation commander ip-address** command deletes the Commander IP address.

By default, no Commander IP address is configured.

Format

easy-operation commander ip-address *ip-address* [**udp-port** *udp-port*]

undo easy-operation commander ip-address [*ip-address* [**udp-port** *udp-port*]]

Parameters

Parameter	Description	Value
ip-address	Specifies the Commander IP address.	The value is in dotted decimal notation.
udp-port *udp-port*	Specifies the UDP port number that the Commander uses to communicate with clients.	The value is an integer in the range from 1025 to 65535. The default value is 60000.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After an IP address is configured for the Commander, clients can communicate with the Commander through this IP address. To implement a batch upgrade, you need to specify the Commander IP address on clients. In zero touch provisioning (ZTP) and faulty device replacement scenarios, clients obtain the Commander IP address from the DHCP server.

Precautions

The configured Commander IP address must exist on the device that functions as the Commander.

The Commander IP address cannot be the IP address of the VLANIF interface bound to a VPN.

After the Commander function is enabled on the switch, changing the Commander IP address is not allowed on the switch. Otherwise, the Commander cannot detect and manage clients.

In batch upgrade scenarios, the Commander and clients must be configured with the same Commander IP address and UDP port number. Otherwise, clients cannot communicate with the Commander.

Example

Configure the Commander IP address.

```
<HUAWEI> system-view
[HUAWEI] easy-operation commander ip-address 10.10.10.5
Warning: The pre-shared key can be modified to improve security. Continue? [Y/N]:y
Enter the pre-shared key:******
Confirm the pre-shared key:******
```

Table 2-18 Description of the **easy-operation commander ip-address** command output

Item	Description
Warning: The pre-shared key can be modified to improve security. Continue? [Y/N]	Whether to change a pre-shared key. Regardless of whether the pre-shared key is changed, the **easy-operation commander ip-address** command can still be executed, and the Commander IP address can be changed successfully. • y: The pre-shared key will be changed. • n: The pre-shared key will not be changed.
Enter the pre-shared key	Enter the ciphertext of the pre-shared key. **NOTE** • The same pre-shared key must be configured on the Commander and clients simultaneously. • If the entered pre-shared key is invalid or the two pre-shared keys are different, the pre-shared key will not be changed. The failure to change the pre-shared key does not affect the execution of the **easy-operation commander ip-address** command. That is, the Commander IP address can still be changed successfully.
Confirm the pre-shared key	Confirm the ciphertext of the pre-shared key.

2.2.42 easy-operation dtls disable

Function

The **easy-operation dtls disable** command disables Datagram Transport Layer Security (DTLS) encryption.

The **undo easy-operation dtls disable** command enables DTLS encryption.

By default, DTLS encryption is enabled.

Format

easy-operation dtls disable

undo easy-operation dtls disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command is mainly used in the capacity expansion scenario on a live network. If the system software of a client is V200R010C00 or a later version and that of the Commander is a version earlier than V200R010C00, you need to run the **easy-operation dtls disable** command on the client to disable DTLS encryption.

Precautions

- You must enable or disable DTLS encryption on the Commander and client at the same time.
- If the system software of a switch in a version earlier than V200R010C00 is upgraded to V200R010C00 or a later version, an **easy-operation dtls disable** configuration is automatically generated.
- If a client in V200R010C00 or a later version needs to be managed by the Commander in a version earlier than V200R010C00, you need to run the **easy-operation dtls disable** command on the client to disable DTLS encryption.
- If a client in a version earlier than V200R010C00 needs to be managed by the Commander in V200R010C00 or a later version and DTLS encryption is enabled on the Commander, you must upgrade the system software of the

client to V200R010C00 or a later version. Otherwise, the client cannot join the existing network.

- After DTLS encryption is enabled, the shared key configured using the **easy-operation shared-key** command does not take effect.
- After DTLS encryption is enabled, you can run the **easy-operation dtls psk** command to configure the DTLS PSK.

Example

Disable DTLS encryption.

```
<HUAWEI> system-view
[HUAWEI] easy-operation dtls disable
```

2.2.43 easy-operation dtls psk

Function

The **easy-operation dtls psk** command configures the DTLS pre-shared key (PSK).

The **undo easy-operation dtls psk** command restores the default DTLS PSK.

The default username and password are available in *S Series Switches Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

Format

easy-operation dtls psk *psk*

undo easy-operation dtls psk

Parameters

Parameter	Description	Value
psk	Specifies the PSK.	The value is a string of 6 to 32 characters in plain text or a string of 48 or 68 characters in cipher text.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After DTLS encryption is enabled, you can run this command to change the DTLS PSK.

Precautions

The same PSK must be configured on the Commander and clients simultaneously.

Example

Set the DTLS PSK to **test12345**.

```
<HUAWEI> system-view
[HUAWEI] easy-operation dtls psk test12345
```

2.2.44 easy-operation shared-key

Function

The **easy-operation shared-key** command configures a shared key for the Commander or a client.

The **undo easy-operation shared-key** command deletes the configured shared key of the Commander or client.

By default, no shared key is configured on a Commander or client.

Format

easy-operation shared-key cipher *key-string*

undo easy-operation shared-key

Parameters

Parameter	Description	Value
cipher	Configures a shared key in cipher text.	-
key-string	Specifies a shared key.	The value is a string of case-sensitive characters without spaces. A plain text key contains 1 to 64 characters, and a cipher text key contains 48 to 108 characters.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In batch upgrade and configuration scenarios, to enhance security for communication between the Commander and clients and prevent a bogus Commander from controlling clients, run the **easy-operation shared-key** command to configure the same shared key for the Commander and clients.

Precautions

- The same shared key must be configured on the Commander and clients simultaneously.
- If a shared key has been configured on the Commander, the Commander cannot manage clients running versions earlier than V200R008C00 and clients that have no shared key configured.
- The shared key configuration does not affect zero touch device deployment.
- After DTLS encryption is enabled, the shared key configured using the **easy-operation shared-key** command does not take effect.

Example

Configure a shared key on the Commander.

```
<HUAWEI> system-view
[HUAWEI] easy-operation shared-key cipher Easy@huawei
```

2.2.45 execute to

Function

The **execute to** command enables the Commander to deliver commands to clients or client groups.

Format

execute [*script-file*] **to client** { **all** | { *client-id1* [**to** *client-id2*] }&<1-10> }

execute [*script-file*] **to group** { **all** | { **name** *group-name* }&<1-10> }

Parameters

Parameter	Description	Value
script-file	Indicates a script file name. If no script file name is specified, the script made online is delivered.	The value is a string of 5 to 64 characters, depending on the actual situation.

Parameter	Description	Value
client { *client-id1* [**to** *client-id2*] }	Indicates that commands are delivered to a specified client.	The value is an integer. It depends on the maximum number of clients supported by the Commander. For details, see **Maximum Number of Managed Clients** on the Commander.
client all	Indicates that commands are delivered to all clients.	-
group name *group-name*	Indicates that commands are delivered to a specified client group.	The value is a string of 1 to 31 case-sensitive characters without spaces. The character string must start with a letter.
group all	Indicates that commands are delivered to all client groups.	-

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To implement a batch configuration of clients on a network supporting EasyDeploy, edit commands to be run, save them as a script, and deliver the edited commands to clients through the Commander.

Example

Enable the Commander to deliver commands to all clients.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] execute to client all
Warning: This operation will start the batch command executing process to the cl
ients. Continue?[Y/N]:y
Info: This operation will take some seconds, please wait..
```

2.2.46 group build-in

Function

The **group build-in** command configures a built-in group on the Commander and displays the Easy-Operation group view.

The **undo group build-in** command deletes a built-in group.

By default, no built-in group is configured.

Format

group build-in *device-type* [**vendor** *vendorname*]

undo group build-in [*device-type* [**vendor** *vendorname*]]

NOTE

- If clients of the same type from different vendors exist on the network, you need to configure **vendor** *vendorname* to distinguish the clients.
- If **vendor** *vendorname* is specified in the **group build in** command, the device type view of the corresponding vendor is displayed.
- If **vendor** *vendorname* is not specified in the **group build in** command, the vendor type is not specified.

Parameters

Parameter	Description	Value
device-type	Specifies the device type in a group.	The value is an enumerated type and case-insensitive. The following device types are supported: ● S2730S-S ● S2750-EI ● S5700-10P-LI ● S5700-EI ● S5700-HI ● S5700-P-LI ● S5700-SI ● S5700-TP-LI ● S5700-X-LI ● S5700S-LI ● S5700S-P-LI ● S5700S-X-LI ● S5710-EI ● S5710-HI ● S5710-X-LI ● S5720-EI ● S5720-HI ● S5720-LI ● S5720-SI ● S5720S-LI ● S5730-HI ● S5730-SI ● S5730S-EI ● S5731-H ● S5731-S ● S5731S-H ● S5731S-S ● S5732-H ● S5735-L ● S5735-L1 ● S5735-L-I ● S5735S-L ● S5735S-L1 ● S5735-S

Parameter	Description	Value
		• S5735S-S • S5735S-H • S5736-S • S6700-EI • S6720-EI • S6720-HI • S6720-LI • S6720-SI • S6720S-S • S6720S-LI • S6720S-SI • S6730-H • S6730S-H • S6730-S • S6730S-S • S6735-S • S9700
vendor *vendorname*	Displays the group of the device type of the specified vendor.	The value is a character string.

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If clients on a network are devices of the same type, run the **group build-in** command to configure a built-in group based on the device type. This group enables these clients to download the same files, such as the system software package and patch file.

Precautions

- If a client matches both a customized group (configured using the **group custom** command) and a built-in group, it prefers the files specified in the customized group.

- A maximum of 256 groups (including both built-in groups and customized groups) can be configured on the Commander.
- If you run the **undo group build-in** command without specifying *device-type*, the command deletes all the built-in groups.

Example

Configure a built-in group and specify the device type as S5732-H.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] group build-in s5732-h
[HUAWEI-easyoperation-group-build-in-s5732-h]
```

2.2.47 group custom

Function

The **group custom** command configures a customized group and displays the Easy-Operation group view on the Commander.

The **undo group custom** command deletes a customized group.

By default, no customized group is configured.

Format

group custom { **mac-address** | **esn** | **ip-address** | **model** | **device-type** } *group-name*

undo group custom [{ **mac-address** | **esn** | **ip-address** | **model** | **device-type** } [*group-name*]]

Parameters

Parameter	Description	Value
group-name	Specifies the name of a customized group.	The value is a string of 1 to 31 case-sensitive characters without spaces. The character string must start with a letter.
mac-address	Configures a MAC address-based group.	-
esn	Configures an ESN-based group.	-
ip-address	Configures an IP address-based group.	-
model	Configures a device model-based group.	-

Parameter	Description	Value
device-type	Configures a device type-based group. This parameter applies when a new device type is not defined for built-in groups on the Commander.	-

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If multiple devices on a network need to download the same file, you can configure a group for the devices on the Commander to simplify device configuration. You can configure various customized groups on the Commander according to the deployment on your network devices.

Precautions

- A maximum of 256 groups (including both built-in groups and customized groups) can be configured on the Commander.
- Customized groups can have matching rules based on MAC address, ESN, IP address, device model, and device type, listed in descending order of priority.
- Running the **undo group custom** command without any parameters will delete all the customized groups.

Example

Configure a MAC address-based customized group.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] group custom mac-address test
[HUAWEI-easyoperation-group-custom-test]
```

2.2.48 license

Function

The **license** command specifies a license file to be downloaded to clients.

The **undo license** command deletes the configured license file information.

Format

license *file-name*

undo license [*file-name*]

Parameters

Parameter	Description	Value
file-name	Specifies the name of a license file to be downloaded to clients. The file name has an extension .dat and may contain a file path.	The value is a string of 5 to 64 case-insensitive characters without spaces.

Views

Easy-Operation view, Easy-Operation group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When clients need to load a license file, specify the license file on the Commander.

Precautions

You can load a license file only on modular switches. When a fixed switch serves as the client, the license file cannot be loaded even after you specify the license file information.

Information about the files to be downloaded can be set in the Easy-Operation view or Easy-Operation group view:

- The file information set in the Easy-Operation view is the default file information. If no file information is set in the group database or client database, the group or client uses the default file information.
- The files specified in the Easy-Operation group view can be downloaded by the clients that match the group.

NOTICE

The names of the files to be downloaded cannot be the same as system license files. Otherwise, the upgrade fails.

Example

Specify a default license file for clients.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] license easy/test.dat
```

Specify a license file in a MAC address-based group.


```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] group custom mac-address test
[HUAWEI-easyoperation-group-custom-test] license license.dat
```

2.2.49 match

Function

The **match** command configures a matching rule for a group on the Commander.

The **undo match** command deletes a matching rule for a group on the Commander.

By default, a group has no matching rule.

Format

match mac-address *mac-address* [*mac-mask* | *mac-mask-length*]

match esn *esn*

match ip-address *ip-address* [*ip-mask* | *ip-mask-length*]

match model *model*

match device-type *device-type*

undo match mac-address [*mac-address* [*mac-mask* | *mac-mask-length*]]

undo match esn [*esn*]

undo match ip-address [*ip-address* [*ip-mask* | *ip-mask-length*]]

undo match model [*model*]

undo match device-type [*device-type*]

Parameters

Parameter	Description	Value
mac-address *mac-address*	Configures a MAC address-based matching rule. A group can have multiple MAC addresses or MAC address ranges specified. A client matches the group as long as it matches one of MAC addresses.	The value is in the H-H-H format, where each H contains four hexadecimal digits.
mac-mask	Specifies the mask of a MAC address.	The value is in the H-H-H format, where each H contains four hexadecimal digits. By default, the mask is ffff-ffff-ffff.

Parameter	Description	Value
mac-mask-length	Specifies the mask length of a MAC address.	The value is an integer that ranges from 0 to 48. By default, the mask length is 48.
esn *esn*	Configures an ESN-based matching rule. A group can have multiple ESNs specified. A client matches the group as long as it matches one of ESNs.	The value is a string of 10 to 32 case-insensitive characters without spaces.
ip-address *ip-address*	Configures an IP address-based matching rule. A group can have multiple IP addresses or IP address ranges (for example 192.168.110.0) specified. A client matches the group as long as it matches one of IP addresses.	The value is in dotted decimal notation.
ip-mask	Specifies the mask of an IP address.	The value is in dotted decimal notation. By default, the mask is 255.255.255.255.
ip-mask-length	Specifies the mask length of an IP address.	The value is an integer that ranges from 0 to 32. By default, the mask length is 32.
model *model*	Configures a device model-based matching rule.	The value is a string of 1 to 32 case-insensitive characters without spaces.
device-type *device-type*	Configures a device type-based matching rule.	The value is a string of 1 to 32 case-insensitive characters without spaces.

Views

Easy-Operation group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After configuring a customized group on the Commander, configure matching rules for the group. A client can obtain the files specified in a group only when it matches a rule in the group.

Precautions

- A matching rule can be configured only in a customized group of the corresponding type. For example, the **match mac-address** *mac-address* command can only be used in a MAC address-based customized group.
- A MAC address-based, ESN-based, or IP address-based group each supports a maximum of 256 matching rules. The total number of group rules on the device cannot exceed 256.
- For groups created based on device models, only one matching rule can be defined for each group. The device model specified in a device model-based group must be the same as the actual device model. Otherwise, clients cannot match the group.
- For groups created based on device types, only one matching rule can be defined for each group. The device type specified in a device type-based group must be the same as the actual device type. Otherwise, clients cannot match the group.

Example

Configure two MAC address-based matching rules in a customized group.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] group custom mac-address test
[HUAWEI-easyoperation-group-custom-test] match mac-address 00e0-fc12-3456
[HUAWEI-easyoperation-group-custom-test] match mac-address 00e0-fc12-3478
```

2.2.50 mngvlanid

Function

The **mngvlanid** command sets a management VLAN for a cluster.

The **undo mngvlanid** command restores the default management VLAN of a cluster.

By default, the management VLAN is VLAN 1.

Format

mngvlanid *vlan-id*

undo mngvlanid

Parameters

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.

Views

Cluster view

Default Level

2: Configuration level

Usage Guidelines

On a Commander switch, if a management VLAN is changed or the management VLAN and its corresponding VLANIF interface are deleted, the cluster is automatically deleted.

If you change the ID of the management VLAN on a client switch, the client switch automatically withdraws from the cluster.

Use the management VLAN only on the cluster and do not use the VLAN for other services such as the Rapid Ring Protection Protocol (RRPP) and multicast services. Otherwise, service functions will be adversely affected.

Example

Change the management VLAN of the device to VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] cluster
[HUAWEI-cluster] mngvlanid 2
```

2.2.51 ndp enable (interface view)

Function

The **ndp enable** command enables NDP on an interface.

The **undo ndp enable** command disables NDP on an interface.

The **ndp disable** command disables NDP on an interface.

By default, NDP is enabled on an interface.

Format

ndp enable

undo ndp enable

ndp disable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, Eth-Trunk interface view, 100GE interface view, 40GE interface view, port group view, MultiGE interface view

Default Level

2: Configuration level

Usage Guidelines

Before you enable network topology collection, run the **ndp enable** command to enable NDP on an interface.

Example

Disable NDP in the GE0/0/1 interface view.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo ndp enable
```

2.2.52 ndp enable (system view)

Function

The **ndp enable** command enables NDP globally or on an interface.

The **undo ndp enable** command disables NDP globally or on an interface.

The **ndp disable** command disables NDP globally or on an interface.

By default, NDP is enabled globally.

Format

ndp enable [**interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>]

undo ndp enable [**interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>]

ndp disable interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>

ndp disable

Parameters

Parameter	Description	Value
interface *interface-type interface-number1* [**to** *interface-type interface-number2*]	Specifies the interface on which NDP is enabled or disabled. • *interface-type interface-number1* indicates the type and number of the first interface. • *interface-type interface-number2* indicates the type and number of the last interface. If you run the **ndp enable** command or the **undo ndp enable** command without specifying the interface, NDP is enabled or disabled globally.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before you enable network topology collection, run the **ndp enable** command to enable NDP.

Configuration Impact

If the **ndp enable** command is run more than once, all configurations take effect.

Example

Enable NDP on the GE0/0/1 interface.

```
<HUAWEI> system-view
[HUAWEI] ndp enable interface gigabitethernet 0/0/1
```

2.2.53 ndp timer aging

Function

The **ndp timer aging** command configures an aging time for NDP entries on the receiving switch.

The **undo ndp timer aging** command restores the default aging time of NDP entries on the receiving switch.

By default, the aging time of the NDP entries on the receiving switch is 180 seconds.

Format

ndp timer aging *aging-time*

undo ndp timer aging

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time of the NDP entries on the receiving switch.	The value is an integer that ranges from 6 to 255, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the receiving switch does not receive NDP packets from a local switch before the aging time of the NDP entry on the receiving switch expires, the receiving switch automatically deletes the neighbor entry corresponding to the local switch.

Prerequisites

NDP has been enabled on the receiving switch.

Precautions

The aging time of the NDP entries on the receiving switch must be greater than the interval for sending NDP packets.

Example

Set the aging time of NDP entries to 175 seconds.

```
<HUAWEI> system-view
[HUAWEI] ndp timer aging 175
```

2.2.54 ndp timer hello

Function

The **ndp timer hello** command configures the interval for sending NDP packets.

The **undo ndp timer hello** command restores the default interval for sending NDP packets.

By default, the interval for sending NDP packets is 60 seconds.

Format

ndp timer hello *interval*

undo ndp timer hello

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending NDP packets.	The value is an integer that ranges from 5 to 254, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure an interval for sending NDP packets, run the **ndp timer hello** command. The NDP interface then sends NDP packets at the specified interval.

Prerequisites

NDP has been enabled on the switch.

Precautions

The interval for sending NDP packets must be less than the aging time of NDP entries on the receiving switch.

Example

Set the interval for sending NDP packets to 55 seconds.

```
<HUAWEI> system-view
[HUAWEI] ndp timer hello 55
```

2.2.55 ndp trunk-member enable

Function

The **ndp trunk-member enable** command enables trunk member interface-based NDP.

The **undo ndp trunk-member enable** command disables trunk member interface-based NDP.

By default, trunk member interface-based NDP is disabled.

Format

ndp trunk-member enable

undo ndp trunk-member enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a local switch connects to a remote switch through a trunk link, the local switch discovers neighbors and displays NTDP topology information based on the trunk interface. To allow the local switch to obtain link information about trunk member interfaces, run the **ndp trunk-member enable** command to enable trunk member interface-based NDP. The topology information about the trunk member interfaces can then be queried on the NMS.

Prerequisites

NDP has been globally enabled using the **ndp enable** command in the system view.

Example

Enable trunk member interface-based NDP.

```
<HUAWEI> system-view
[HUAWEI] ndp enable
[HUAWEI] ndp trunk-member enable
```

2.2.56 ntdp enable (interface view)

Function

The **ntdp enable** command enables NTDP on an interface.

The **undo ntdp enable** command disables NTDP on an interface.

The **ntdp disable** command disables NTDP on an interface.

By default, NTDP is enabled on an interface.

Format

ntdp enable

undo ntdp enable

ntdp disable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 25GE interface view, Eth-Trunk interface view, 100GE interface view, 40GE interface view, port group view, MultiGE interface view

Default Level

2: Configuration level

Usage Guidelines

Before you enable network topology collection, run the **ntdp enable** command to enable NTDP on an interface.

Example

Disable NTDP in the GE0/0/1 interface view.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo ntdp enable
```

2.2.57 ntdp enable (system view)

Function

The **ntdp enable** command enables NTDP globally.

The **undo ntdp enable** command disables NTDP globally.

The **ntdp disable** command disables NTDP globally.

By default, NTDP is enabled globally.

Format

ntdp enable

undo ntdp enable

ntdp disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before you enable network topology collection, run the **ntdp enable** command to enable NTDP globally.

Example

Enable NTDP globally.

```
<HUAWEI> system-view
[HUAWEI] ntdp enable
```

2.2.58 ntdp explore

Function

The **ntdp explore** command enables you to manually collect topology information.

Format

ntdp explore

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to initiate the process of collecting topology information on an NTDP-capable device. The NTDP-capable device can then effectively manage and monitor devices on the network in real time to reflect the network topology changes.

You can also run the **ntdp timer** command to allow a switch to automatically collect topology information at a specified interval.

Example

Manually start topology information collection.

```
<HUAWEI> ntdp explore
```

2.2.59 ntdp hop

Function

The **ntdp hop** command sets the maximum number of hops for collecting topology information through NTDP.

The **undo ntdp hop** command restores the default maximum number of hops for collecting topology information through NTDP.

By default, the maximum number of hops is 8 for collecting topology information through NTDP.

Format

ntdp hop *max-hop-value*

undo ntdp hop

Parameters

Parameter	Description	Value
max-hop-value	Specifies the maximum number of hops for collecting topology information through NTDP.	The value is an integer that ranges from 1 to 8.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the maximum number of hops for collecting topology information through NTDP is configured, topology information about switches in the hop range can be collected, which avoids collection of infinite topology information. The larger the maximum number of hops is, the more the memory of the topology collection switch is consumed.

Prerequisites

NTDP has been enabled on the switch.

Example

Set the range for collecting topology information through NTDP to 5 hops.

```
<HUAWEI> system-view
[HUAWEI] ntdp hop 5
```

2.2.60 ntdp timer

Function

The **ntdp timer** command sets the interval for collecting topology information through NTDP.

The **undo ntdp timer** command restores the default interval for collecting topology information through NTDP.

By default, the interval for collecting topology information through NTDP is 0 minutes. That means that no topology information is periodically collected.

Format

ntdp timer *interval*

undo ntdp timer

Parameters

Parameter	Description	Value
interval	Specifies the interval for collecting topology information through NTDP.	The value is an integer that ranges from 0 to 65535, in minutes. **NOTE** The Commander collects network topology information at an interval of 5 minutes; therefore, you are advised to set the interval for collecting topology information through NTDP to less than 5 minutes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the interval for collecting topology information through NTDP is set, the switch collects topology information at this interval.

Prerequisites

NTDP has been enabled on the switch.

Example

Set the interval for collecting topology information to 2 minutes.

```
<HUAWEI> system-view
[HUAWEI] ntdp timer 2
```

2.2.61 ntdp timer hop-delay

Function

The **ntdp timer hop-delay** command sets a delay after which the first interface forwards NTDP topology request packets.

The **undo ntdp timer hop-delay** command restores the default delay.

By default, the first interface forwards NTDP topology request packets after a delay of 200 milliseconds.

Format

ntdp timer hop-delay *hop-delay-time*

undo ntdp timer hop-delay

Parameters

Parameter	Description	Value
hop-delay-time	Specifies the delay after which the first interface forwards NTDP topology request packets.	The value is an integer that ranges from 1 to 1000, in milliseconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command takes effect only after NTDP is enabled on the switch.

Example

Set the hop delay for forwarding NTDP topology request packets to 300 milliseconds.

```
<HUAWEI> system-view
[HUAWEI] ntdp timer hop-delay 300
```

2.2.62 ntdp timer port-delay

Function

The **ntdp timer port-delay** command sets a delay after which interfaces other than the first one forwards NTDP topology request packets.

The **undo ntdp timer port-delay** command restores the default delay.

By default, interfaces other than the first one forward NTDP topology request packets after a delay of 20 milliseconds.

Format

ntdp timer port-delay *port-delay-time*

undo ntdp timer port-delay

Parameters

Parameter	Description	Value
port-delay-time	Specifies the delay after which interfaces other than the first one forward NTDP topology request packets.	The value is an integer that ranges from 1 to 1000, in milliseconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **ntdp timer port-delay** command takes effect only after NTDP is enabled on the switch.

Example

Set the delay for interfaces other than the first one on the device to forward NTDP topology request packets to 40 milliseconds.

```
<HUAWEI> system-view
[HUAWEI] ntdp timer port-delay 40
```


2.2.63 patch

Function

The **patch** command specifies a patch file to be downloaded to clients.

The **undo patch** command deletes the configured patch file information.

Format

patch *file-name*

undo patch [*file-name*]

Parameters

Parameter	Description	Value
file-name	Specifies the name of a patch file to be downloaded to clients. The file name has an extension .pat and may contain a file path.	The value is a string of 5 to 48 case-insensitive characters without spaces.

Views

Easy-Operation view, Easy-Operation group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When clients need to load a patch file, specify the patch file on the Commander.

Precautions

Information about the files to be downloaded can be set in the Easy-Operation view or Easy-Operation group view:

- The file information set in the Easy-Operation view is the default file information. If no file information is set in the group database or client database, the group or client uses the default file information.
- The files specified in the Easy-Operation group view can be downloaded by the clients that match the group.

Example

Specify a default patch file for clients.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] patch easy/test.pat
```


Specify a patch file in a MAC address-based group.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] group custom mac-address test
[HUAWEI-easyoperation-group-custom-test] patch patch.pat
```

2.2.64 reset easy-operation client-database

Function

The **reset easy-operation client-database** command clears the client database on the Commander.

Format

reset easy-operation client-database

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The client database contains client information that is manually configured by the administrator and learned dynamically by the Commander. When the number of clients in the client database exceeds the limit, information about new clients cannot be added to the database. To release space in the client database, use this command to clear the client database after confirming that the manually configured client information can be deleted.

Precautions

This command deletes both manually configured client information and dynamically learned client information. Before running this command, confirm that manually configured client information can be deleted. If the Commander is enabled to learn client information, it continues adding learned client information to the client database after you run this command.

Example

Clear the client database on the Commander.

```
<HUAWEI> reset easy-operation client-database
Warning: All of the database information of client and relative replace in this
device will be cleared. Continue?[Y/N]:y
<HUAWEI>
```


2.2.65 reset easy-operation client-offline

Function

The **reset easy-operation client-offline** command clears lost state clients.

Format

reset easy-operation client-offline

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The maximum number of clients managed by the Commander depends on the device specifications. If the number of clients exceeds the upper limit, information about new clients cannot be configured on the Commander. Delete the clients in the lost state that occupy the database resources for a long time.

Precautions

- If the clients automatically join the management domain of the Commander, they can be deleted.
- If the clients are configured manually, they cannot be deleted but their status changes to unknown.
- If client replacement information is configured using the **client replace** command, client IDs in the client database will not be deleted.

Example

Delete clients in the lost state from the client database.

```
<HUAWEI> reset easy-operation client-offline
Warning: All of clients which are in the lost status will be deleted. Continue?[Y/N]:y
```

2.2.66 reset ndp statistics

Function

The **reset ndp statistics** command clears NDP packet statistics from one or all the interfaces of a device.

Format

reset ndp statistics [**interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>]

Parameters

Parameter	Description	Value
interface *interface-type interface-number1* [**to** *interface-type interface-number2*]	Clears NDP packet statistics from a specified interface. ● *interface-type interface-number1* specifies the type and number of the first interface. ● *interface-type interface-number2* indicates the type and number of the last interface. When optional parameters are not specified, global statistics on NDP packets are cleared.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

If you run the **reset ndp statistics** command without setting optional parameters, the NDP packet statistics of all interfaces are cleared.

Example

Delete NDP packet statistics from all the interfaces of the device.

```
<HUAWEI> reset ndp statistics
```

2.2.67 system-software

Function

The **system-software** command specifies the name and version of the system software package to be downloaded to clients.

The **undo system-software** deletes the configured software name and version.

Format

system-software *file-name* [*version*]

undo system-software [*file-name* [*version*]]

Parameters

Parameter	Description	Value
file-name	Specifies the name of a system software package to be downloaded to clients. The file name has an extension .cc and may contain a file path.	The value is a string of 4 to 48 case-insensitive characters without spaces. The string cannot contain the following characters: ~ * : ' " ? < > | [ ] % \ /.
version	Specifies the version of a system software package, for example, V200R023C00. If the specified software version is the same as the software version running on the client, a software upgrade will not be performed for the client.	The value is a string of 11 to 32 case-insensitive characters without spaces.

Views

Easy-Operation view, Easy-Operation group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When clients need to upgrade their system software, specify the required system software information on the Commander.

Precautions

Information about the files to be downloaded can be set in the Easy-Operation view or Easy-Operation group view:

- The file information set in the Easy-Operation view is the default file information. If no file information is set in the group database or client database, the group or client uses the default file information.
- The files specified in the Easy-Operation group view can be downloaded by the clients that match the group.

Example

Specify a default system software package for clients.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] system-software easy/sV200R023C00.cc
```

Specify a system software package in a MAC address-based group.


```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] group custom mac-address test
[HUAWEI-easyoperation-group-custom-test] system-software V200R023C00.cc V200R023C00
```

2.2.68 tftp-server/sftp-server/ftp-server

Function

The **tftp-server** command configures the TFTP server IP address on the Commander.

The **sftp-server** command configures the SFTP server IP address, user name, and password on the Commander.

The **ftp-server** command configures the FTP server IP address, user name, and password on the Commander.

The **undo tftp-server** command deletes the TFTP server IP address on the Commander.

The **undo sftp-server** command deletes the SFTP server IP address, user name, and password on the Commander.

The **undo ftp-server** command deletes the FTP server IP address, user name, and password on the Commander.

By default, no file server IP address, user name, or password is configured on the Commander.

Format

tftp-server *ip-address*

{ **sftp-server** | **ftp-server** } *ip-address* [**username** *username* [**password** *password*]]

undo tftp-server [*ip-address*]

undo { **sftp-server** | **ftp-server** } [*ip-address*] [**username** *username*] [**password** *password*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a file server (TFTP, SFTP, or FTP server).	The value is in dotted decimal notation.
username *username*	Specifies the user name used to log in to the SFTP or FTP server.	The value is a string of 1 to 64 case-sensitive characters.

Parameter	Description	Value
password *password*	Specifies the password used to log in to the SFTP or FTP server.	The value is a case-sensitive character string. A password in plain text contains 1 to 16 characters, and a ciphertext password contains 48 characters. In the configuration file, the password is displayed in ciphertext regardless of whether it is input in plaintext or ciphertext.

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Files that need to be downloaded by clients are saved in a file server. After clients obtain information from the Commander about the necessary files, the clients download the files from the file server specified on the Commander. Therefore, the file server information must be configured on the Commander.

Precautions

- If the file server is an SFTP or FTP server and has a user name and password configured, configure the same user name and password on the Commander.
- Using an SFTP server is recommended because FTP and TFTP have security risks.
- Information about only one file server can be configured. If you run this command multiple times, only the latest configuration takes effect.
- Ensure that the files required for clients have been saved on the specified file server.

Example

Specify the IP address, user name, and password of the SFTP server on the Commander.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] sftp-server 10.10.10.5 username easyoperation password YsHsjx_202206
```

Specify the TFTP server IP address on the Commander.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] tftp-server 10.10.10.5
```


2.2.69 topology enable

Function

The **topology enable** command enables the Commander to collect network topology information.

The **undo topology enable** command disables the Commander from collecting network topology information.

By default, the Commander is disabled from collecting network topology information.

Format

topology enable

undo topology enable

Parameters

None

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **topology enable** command to enable the Commander to collect network topology information every 5 minutes. Based on the collected information, you can implement zero touch device deployment and automatic faulty device replacement.

Prerequisites

NDP and NTDP have been enabled.

The interval for collecting topology information through NTDP has been set.

Example

Enable network topology information collection on the Commander.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] topology enable
```


2.2.70 topology save

Function

The **topology save** command saves network topology information collected by the Commander.

Format

topology save

Parameters

None

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Network topology information collected by the Commander is saved only in the device memory. If the device restarts, the saved information is lost. You can run this command to save the collected network topology information in the flash memory and name it **ezop-topo.xml**.

Prerequisites

Network topology information collection has been enabled.

Precautions

If you run this command multiple times, only the latest configuration takes effect.

Example

Save the current network topology information collected by the Commander.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] topology save
Warning: This command will record the information of topology. Continue? [Y/N]:y
```

2.2.71 undo group

Function

The **undo group** command deletes all groups.

Format

undo group

Parameters

None

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

This command deletes all the groups on a switch, including built-in groups and customized groups.

Example

Delete all groups.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] undo group
Warning: All of the group configuration will be cleared. Continue?[Y/N]:y
```

2.2.72 upgrade group

Function

The **upgrade group** command starts a batch upgrade on the Commander.

Format

upgrade group [*group-name*] &<1-15>

Parameters

Parameter	Description	Value
group-name	Specifies a group name. The Commander starts a batch upgrade for all the clients that match the specified group. A maximum of 15 groups can be specified for a batch upgraded. The group names are separated by a space.	The value is a string of 1 to 31 case-sensitive characters without spaces. The character string must start with a letter.

Views

Easy-Operation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the groups, files to be loaded, and file activation mode are specified on the Commander, you can run this command to start a batch upgrade for clients.

Precautions

- If *group-name* is not specified, a batch upgrade is performed on all clients matching all the groups on the Commander.
- Before running this command, ensure that configurations of the clients have been saved.
- If a client is a stack system, its system MAC address will change after the upgrade, because the master switch changes. In this case, the client ID of the stack system is displayed as LOST on the Commander. To avoid this problem, configure the stack system MAC address to the MAC address of a member switch.

Example

Start a batch upgrade for clients matching all the groups.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] upgrade group
Warning: This command will start the upgrade process of all groups and clients i
n these groups may reboot. Ensure that configurations of the clients have been s
aved. Continue?[Y/N]:y
```

Start a batch upgrade for clients matching specified groups.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] upgrade group test1 test2 test3
Warning: This command will start the upgrade process of the group and clients in
 this group may reboot. Ensure that configurations of the clients have been save
d. Continue?[Y/N]:y
```

2.2.73 web-file

Function

The **web-file** command specifies a web page file to be downloaded to clients.

The **undo web-file** command deletes the configured web page file information.

Format

web-file *file-name*

undo web-file [*file-name*]

Parameters

Parameter	Description	Value
file-name	Specifies the name of a web page file to be downloaded to clients. The file name has an extension .web.7z or .web.zip and may contain a file path.	The value is a string of 8 to 64 case-insensitive characters without spaces.

Views

Easy-Operation view, Easy-Operation group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When clients need to load a web page file, specify the web page file on the Commander.

Precautions

Information about the files to be downloaded can be set in the Easy-Operation view or Easy-Operation group view:

- The file information set in the Easy-Operation view is the default file information. If no file information is set in the group database or client database, the group or client uses the default file information.
- The files specified in the Easy-Operation group view can be downloaded by the clients that match the group.

Example

Specify a default web page file for clients.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] web-file easy/test.web.7z
```

Specify a web page file in a MAC address-based group.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] group custom mac-address test
[HUAWEI-easyoperation-group-custom-test] web-file test.web.7z
```

2.2.74 module

Function

The **module** command specifies a module file to be downloaded.

The **undo module** command deletes information about the module file to be downloaded.

Format

module *file-name*

undo module [*file-name*]

Parameters

Parameter	Description	Value
file-name	Specifies the name (*.mod) of a module file to be loaded to clients. The file path can be specified.	The value is a string of 5 to 48 case-insensitive characters. It cannot contain spaces.

Views

Easy-Operation view, Easy-Operation group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a client needs to load a module file, the module file needs to be specified.

Precautions

Information about the files to be downloaded can be set in the Easy-Operation view or Easy-Operation group view:

- The file information set in the Easy-Operation view is the default file information. If no file information is set in the group database or client database, the group or client uses the default file information.
- The files specified in the Easy-Operation group view can be downloaded by the clients that match the group.

Example

Specify a default module file.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] module easy/test.mod
```

Specify a module file in a MAC address-based group.

```
<HUAWEI> system-view
[HUAWEI] easy-operation
[HUAWEI-easyoperation] group custom mac-address test
[HUAWEI-easyoperation-group-custom-test] module test.mod
```


2.3 USB-based Deployment Configuration Commands

2.3.1 Command Support

Only the following switch models support USB-based deployment:

S1730S-S1, S5720-LI, S5720S-LI, S5720I-SI, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-S, S5731S-H, S5732-H, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, S5735S-S, S5735-S-I, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, S6730S-S.

2.3.2 display device usb-deployment configuration

Function

The **display device usb-deployment configuration** command displays the configuration of USB-based deployment.

Format

display device usb-deployment configuration

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

After the USB-based deployment configuration is completed, you can run this command to view related configuration information, including whether USB-based deployment is enabled, configuration file encryption password, HMAC key, and whether HMAC check is enabled.

Example

Display the configuration of USB-based deployment.

```
<HUAWEI> display device usb-deployment configuration
USB-deployment: disable
Config-file password: ******
HMAC: enable
Hmac-key: --
```


Table 2-19 Description of the **display device usb-deployment configuration** command output

Item	Description
USB-deployment	Whether USB-based deployment is enabled. • disable: indicates that USB-based deployment is disabled on an interface. • enable: indicates that USB-based deployment is enabled on an interface.
Config-file password	Configuration file encryption password. When no password is configured, "--" is displayed.
HMAC	Whether HMAC check is enabled. • disable: indicates that HMAC check is disabled on an interface. • enable: indicates that HMAC check is enabled on an interface.
Hmac-key	HMAC key for HMAC verification. When no HMAC key is configured, "--" is displayed.

2.3.3 set device usb-deployment disable

Function

The **set device usb-deployment disable** command disables the USB-based deployment function.

The **undo set device usb-deployment disable** command enables the USB-based deployment function.

By default, the USB-based deployment function is disabled.

Format

set device usb-deployment disable

undo set device usb-deployment disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

By default, the USB-based deployment function is disabled. However, if a device has no configuration, the USB-based deployment function is always enabled.

NOTE

On an unconfigured switch, both the configuration files for current startup and next startup are not specified. That is, the Startup saved-configuration file and Next startup saved-configuration file are NULL in the

display startup command output.

Example

Disable the USB-based deployment function.

```
<HUAWEI> system-view
[HUAWEI] set device usb-deployment disable
```

Enable the USB-based deployment function.

```
<HUAWEI> system-view
[HUAWEI] undo set device usb-deployment disable
Warning: The function of USB deployment in this device will be enabled. Continue
? [Y/N]:y
```

2.3.4 set device usb-deployment config-file password

Function

The **set device usb-deployment config-file password** command configures an encryption password for the configuration file used in USB-based deployment.

The **undo set device usb-deployment config-file password** command deletes the encryption password for the configuration file used in USB-based deployment.

By default, no encryption password is configured.

NOTE

If upgrade files for USB-based deployment include a configuration file, it is recommended that you run this command to configure an encryption password for the configuration file and compress the configuration file using the configured password before saving it in the USB flash drive. This configuration improves security.

Format

set device usb-deployment config-file password *password*

undo set device usb-deployment config-file password

Parameters

Parameter	Description	Value
password	Specifies the password used for encrypting the configuration file.	The value is a string of 8 to 64 characters or a string of 48 to 108 characters. • If the password is in plain text, it is a string of 8 to 64 case-sensitive characters and must be a combination of at least two of the following: letters, digits, and special characters. • If the password is in cipher text, it is a string of 48 to 108 characters. The password is displayed in cipher text in the configuration file regardless of whether you enter it in plain or cipher text.

Views

System view

Default Level

3: Management level

Usage Guidelines

If a password is configured using the **set device usb-deployment config-file password** *password* command, you need to compress and encrypt the configuration file (if any) with this password and save the compressed file to a specified directory in the USB flash drive. The device cannot compress a .zip configuration file. If such a configuration file is used, decompress the file, use the configured password to compress it, and save it in the USB flash drive.

A user with a level lower than the management level cannot query the password configured using this command. If this user query the configuration file, the password is displayed as asterisks (******).

Example

Set the encryption password for the configuration file used in USB-based deployment to **Pwd123456**.

```
<HUAWEI> system-view
[HUAWEI] set device usb-deployment config-file password Pwd123456
```

2.3.5 set device usb-deployment hmac-key

Function

The **set device usb-deployment hmac-key** command configures an HMAC key for HMAC verification during USB-based deployment.

The **undo set device usb-deployment hmac-key** command deletes the HMAC key used for HMAC verification during USB-based deployment.

By default, no HMAC key is configured for HMAC verification.

Format

set device usb-deployment hmac-key *hmac-key*

undo set device usb-deployment hmac-key

Parameters

Parameter	Description	Value
hmac-key	Specifies an HMAC key for HMAC verification during USB-based deployment.	The value is a string of 8 to 64 or 68 to 108 characters. ● A cleartext key is a string of 8 to 64 case-sensitive characters. It is recommended that the key be a combination of at least two of the following: uppercase letters A to Z, lowercase letters a to z, digits, and special characters. ● A ciphertext key is a string of 68 to 108 characters. In the configuration file, a password is displayed in cipher text regardless of whether it is entered in clear text or cipher text.

Views

System view

Default Level

3: Management level

Usage Guidelines

If upgrade files include a configuration file, you can enable HMAC verification to ensure validity of the configuration file to be loaded. After the **set device usb-deployment hmac** command is run to enable HMAC verification for the configuration file during USB-based deployment, run the **set device usb-deployment hmac-key** command to configure an HMAC key for HMAC verification so that the device calculates the HMAC value of the configuration file and then compares the value with the HMAC field value in the index file. If the two values are the same, the configuration file is valid and loaded to the device for USB-based deployment. If the two values are different, the configuration file is invalid and cannot be loaded for USB-based deployment.

A user at a level lower than the management level cannot check the HMAC key configured using this command. If this user checks the configuration file, the HMAC key is displayed as ******.

Example

Configure an HMAC key for HMAC verification during USB-based deployment.

```
<HUAWEI> system-view
[HUAWEI] set device usb-deployment hmac-key huawei@123456852369741236553424654643213
```

2.3.6 set device usb-deployment hmac

Function

The **set device usb-deployment hmac** command enables hashed message authentication code (HMAC) check for the configuration file used for USB-based deployment.

The **undo set device usb-deployment hmac** command disables HMAC check for the configuration file used for USB-based deployment.

By default, HMAC check is disabled.

NOTE

If upgrade files for USB-based deployment include a configuration file, it is recommended that you enable HMAC check to improve security of the configuration file.

Format

set device usb-deployment hmac

undo set device usb-deployment hmac

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Prerequisites

Before enabling the HMAC check function, run the **set device usb-deployment config-file password** command to configure an encryption password for the configuration file used for USB-based deployment.

Applications

If upgrade files for USB-based deployment include a configuration file, you can enable HMAC check to ensure validity of the configuration file to be loaded. After HMAC check is enabled on a device, the device uses the password configured by

the **set device usb-deployment config-file password** command to calculate the HMAC for the configuration file, and compares the calculated value with the HMAC field value in the index file. If the two values are the same, the configuration file is considered valid and loaded to the device. If not, the configuration file is considered invalid and cannot be loaded.

Example

Enable HMAC check for the configuration file used for USB-based deployment.

```
<HUAWEI> system-view
[HUAWEI] set device usb-deployment hmac
```

2.3.7 set device usb-deployment password

Function

The **set device usb-deployment password** command sets an authentication password for USB-based deployment.

The **undo set device usb-deployment password** command deletes the authentication password for USB-based deployment.

Format

set device usb-deployment password cipher *password*

set device usb-deployment password *password*

undo set device usb-deployment password

Parameters

Parameter	Description	Value
cipher *password*	Specifies the authentication password for USB-based deployment.	The value is a cipher text string of 8 to 16 or 68 characters.
password	Specifies the authentication password for USB-based deployment.	The value is a cipher text string of 8 to 16 or 68 characters.

Views

System view

Default Level

3: Management level

Usage Guidelines

A user with a level lower than the management level cannot query the password configured using this command. If this user query the configuration file, the password is displayed as asterisks (******).

Example

Delete the authentication password for USB-based deployment.

```
<HUAWEI> system-view
[HUAWEI] undo set device usb-deployment password
```

2.4 First Login Commands

2.4.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

2.4.2 clock datetime

Function

The **clock datetime** command sets the current date and time on a switch.

Format

clock datetime *HH:MM:SS YYYY-MM-DD*

Parameters

Parameter	Description	Value
HH:MM:SS	Specifies the current time on a switch.	*HH* specifies the hour, which is an integer ranging from 0 to 23. *MM* specifies the minute, which is an integer ranging from 0 to 59. *SS* specifies the second, which is an integer ranging from 0 to 59.
YYYY-MM-DD	Specifies the current date (year, month, and day) on the switch.	*YYYY* specifies the year, which is an integer ranging from 2000 to 2037. *MM* specifies the month, which is an integer ranging from 1 to 12. *DD* specifies the day, which is an integer ranging from 1 to 31.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In the scenario where accurate absolute time is required, the current date and time must be set on a switch.

Prerequisite

The time zone and daylight saving time have been configured using the **clock timezone** and **clock daylight-saving-time** commands. If the time zone and daylight saving time are not configured, the **clock datetime** command sets a UTC time.

Precautions

- The specified time must be in 24-hour format. If you do not specify *MM* and *SS*, their values are 0. You must enter at least one digit to specify *HH*. For example, when you enter 0, the time is 00:00:00.
- The specified year must be a four-digit number and the specified month and day can be a one-digit number. For example, when you enter 2012-9-1, the time is 2012-09-01.
- If the device is configured to restart at a specified time and if the system time is changed to be more than 10 minutes later than the specified restart time, the scheduled restart function will be disabled.

NOTE

The valid time range is based on the UTC, and this command sets the local time. If the DST or time zone is specified in the current environment, the system automatically converts the local time to the UTC.

For example, if you set the time zone to GMT+8 and the local date to 2000-1-1, the UTC converted equals to the local date minus eight hours, which is 1999-12-31. However, the valid date range is 2000 to 2037. As a result, the validity check fails, and date setting fails.

Example

Set the current time and date of the system to 0:1:2 2012-01-01.

```
<HUAWEI> clock datetime 0:1:2 2012-01-01
```

2.4.3 clock daylight-saving-time

Function

The **clock daylight-saving-time** command sets the name, start time, and end time of the daylight saving time (DST).

The **undo clock daylight-saving-time** command cancels the DST settings.

By default, DST is not used.

Format

clock daylight-saving-time *time-zone-name* **one-year** *start-time start-date end-time end-date offset*

clock daylight-saving-time *time-zone-name* **repeating** *start-time* { { **first** | **second** | **third** | **fourth** | **last** } *weekday month* | *start-date1* } *end-time* { { **first** | **second** | **third** | **fourth** | **last** } *weekday month* | *end-date1* } *offset* [*start-year* [*end-year*]]

undo clock daylight-saving-time

Parameters

Parameter	Description	Value
time-zone-name	Specifies the name of the DST zone.	The value is a string of 1 to 32 case-sensitive characters without spaces.
one-year	Specifies absolute DST.	-
repeating	Specifies periodic DST.	-
start-time	Specifies the DST start time.	The start time is in 24-hour format *HH:MM*. *HH* specifies the hour, which is an integer ranging from 0 to 23. *MM* specifies the minute, which is an integer ranging from 0 to 59. If *MM* is not specified, DST starts on the hour. You must enter at least one digit to specify *HH*. For example, when you enter 0, the start time is 00:00.
start-date	Specifies the DST start date.	The start date is in the format *YYYY-MM-DD*. *YYYY* specifies the year, which is an integer ranging from 2000 to 2099, *MM* specifies the month, which is an integer ranging from 1 to 12, and *DD* specifies the day, which is an integer ranging from 1 to 31.

Parameter	Description	Value
end-time	Specifies the DST end time.	The end time is in 24-hour format *HH:MM*. *HH* specifies the hour, which is an integer ranging from 0 to 23. *MM* specifies the minute, which is an integer ranging from 0 to 59. If *MM* is not specified, DST starts on the hour. You must enter at least one digit to specify *HH*. For example, when you enter 0, the start time is 00:00.
end-date	Specifies the DST end date.	The end date is in the format *YYYY-MM-DD*. *YYYY* specifies the year, which is an integer ranging from 2000 to 2099, *MM* specifies the month, which is an integer ranging from 1 to 12, and *DD* specifies the day, which is an integer ranging from 1 to 31.
first	Specifies the first workday in a month.	-
second	Specifies the second workday in a month.	-
third	Specifies the third workday in a month.	-
fourth	indicates the fourth workday in a month.	-
last	Specifies the last workday in a month.	-
weekday	Specifies a day of the week.	The value is **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat**, or **Sun**.
month	Specifies a month.	The value is **Jan**, **Feb**, **Mar**, **Apr**, **May**, **Jun**, **Jul**, **Aug**, **Sep**, **Oct**, **Nov**, or **Dec**.

Parameter	Description	Value
start-date1	Specifies the DST start date.	The start date is in the format *MM-DD*. *MM* specifies the month, which is an integer ranging from 1 to 12, and *DD* specifies the day, which is an integer ranging from 1 to 31.
end-date1	Specifies the DST end date.	The end date is in the format *MM-DD*. *MM* specifies the month, which is an integer ranging from 1 to 12, and *DD* specifies the day, which is an integer ranging from 1 to 31.
offset	Specifies the DST offset.	The offset is in 24-hour format *HH:MM*. *HH* specifies the hour, which is an integer ranging from 0 to 2. *MM* specifies the minute, which is an integer ranging from 0 to 59. If *MM* is not specified, the offset is the specified hours. You must enter at least one digit to specify *HH*. The offset should be shorter than or equal to 2 hours.
start-year	Specifies the start year.	The start year is in the format *YYYY* and ranges from 2000 to 2099.
end-year	Specifies the end year.	The end year is in the format *YYYY* and ranges from 2000 to 2099.

Views

User view, system view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

DST, also referred to as summer time, is a convention intended to save resources. In high latitude areas, sunrise time is earlier during summer than it is during winter. To reduce use of incandescent lighting in the evenings and save energy, clocks are adjusted forward one hour.

Users can customize the DST zone according to their countries' or regions' convention. In addition, users can set how far ahead clocks are adjusted forward, usually an hour. With DST enabled, when it is time to start DST, the system time is adjusted according to the user-specified DST. When it is time to end DST, the system time automatically returns to the original time.

Configuration Impact

To configure DST, note the following:

- The time in logs and debugging information uses the local time adjusted based on the time zone and the configured DST.
- The time in the output of the **display** commands uses the local time adjusted based on the time zone and the configured DST.

To remove configurations for DST, note the following:

- If DST has already taken effect when you remove the configurations, the device will adjust its clock by subtracting the value of the *offset* parameter from the current time.
- If DST has not taken effect, removing the configurations will not affect the system time.

Precautions

- The DST is configured in the summer. The DST duration ranges from one day to one year.
- You can configure the start time and end time for periodic DST in one of the following modes: date+date, week+week, date+week, and week+date.
- When you run the **clock daylight-saving-time** command in either the user or system view, the configuration files are both generated in the system view. You are advised to run this command in the system view.

Example

Set periodic DST.

```
<HUAWEI> system-view
[HUAWEI] clock daylight-saving-time bj repeating 0 first sun jan 0 first sun apr 2 2009 2009
```

Set periodic DST by day.

```
<HUAWEI> system-view
[HUAWEI] clock daylight-saving-time bj repeating 12:11 1-1 1:0 3-4 1
```

Set absolute DST.

```
<HUAWEI> system-view
[HUAWEI] clock daylight-saving-time bj one-year 12:11 2010-10-2 1:00 2010-11-4 1
```


2.4.4 clock timezone

Function

The **clock timezone** command sets the local time zone.

The **undo clock timezone** command deletes the local time zone.

By default, the system uses the Coordinated Universal Time (UTC) time zone.

Format

clock timezone *time-zone-name* { **add** | **minus** } *offset*

undo clock timezone

Parameters

Parameter	Description	Value
time-zone-name	Specifies the time zone name.	The name is a string of 1 to 32 case-sensitive characters without spaces.
add	Specifies the offset from the UTC for the time zone specified by *time-zone-name*. That is, the sum of the default UTC time zone and *offset* is equal to the time zone specified by *time-zone-name*.	-
minus	Specifies the offset from the UTC for the time zone specified by *time-zone-name*. That is, the remainder obtained by subtracting *offset* from the default UTC time zone is equal to the time zone specified by *time-zone-name*.	-

Parameter	Description	Value
offset	Specifies the offset from the UTC.	Format: HH:MM:SS ● *HH* specifies the hour. – If the local time is earlier than the UTC, the value is an integer ranging from 0 to 14. – If the local time is later than the UTC, the value is an integer ranging from 0 to 12. ● *MM* and *SS* specify the minute and second respectively, and both range from 0 to 59. ● When *HH* is set to the maximum value, the *MM* and *SS* values must be 0.

Views

User view, System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The system clock is the time indicated by the system timestamp. Because the rules governing local time differ in different regions, the system clock can be configured to comply with the rules of any given region.

System clock = UTC + Time zone offset + DST offset

To ensure normal communication between devices, set an accurate system clock. You can run the **clock timezone** and **clock daylight-saving-time** commands to set the time zone and DST offsets.

Configuration Impact

System time adjustment may affect the timing restart function. If you must adjust the system time after the timing restart function is enabled, pay attention to the impact of system time adjustment on the timing restart function:

- If the system time is changed to less than 10 minutes after the scheduled restart time, the system restarts immediately.
- If the system time is changed to 10 minutes or more after the scheduled restart time, the timing restart function is disabled.
- If the system time is changed to 720 hours earlier than the scheduled restart time, the timing restart function is disabled.

Precautions

- The specified time must be in 24-hour format. If you do not specify *MM* and *SS*, their values are 0. You must enter at least one digit to specify *HH*. For example, when you enter 0, the time is 00:00:00.
- After configuring the local time zone, run the **display clock** command to view the configuration. The time in logs and diagnostic information uses the local time adjusted based on the time zone and DST.
- When you run the **clock timezone** command in either the user or system view, the configuration files are both generated in the system view. You are advised to run this command in the system view.
- Executing the **clock timezone** command takes about 3 seconds.

Example

Set the local time zone name for Beijing China to BJ.

If the default UTC is London time 2012-12-01 00:00:00, Beijing time is London time plus 08:00 because the offset from UTC is 8 hours.

```
<HUAWEI> clock datetime 0:0:0 2012-12-01
<HUAWEI> system-view
[HUAWEI] clock timezone BJ add 08:00:00
```

2.4.5 display calendar

Function

The **display calendar** command displays the calendar of the current month or a specified month in a specified year.

Format

display calendar [*month* [*year*]]

Parameters

Parameter	Description	Value
month	Specifies the month for which the calendar is displayed.	The value is a character string. The values and their meanings are as follows: • **Jan**: January • **Feb**: February • **Mar**: March • **Apr**: April • **May**: May • **Jun**: June • **Jul**: July • **Aug**: August • **Sep**: September • **Oct**: October • **Nov**: November • **Dec**: December
year	Specifies the year for which the calendar is displayed.	The value is an integer that ranges from 2000 to 2099.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring the current date and time on the switch using the **clock datetime** command, you can run the **display calendar** command to view calendar information.

If no month or year is specified, the calendar of the current month is displayed by default. If only month but not year is specified, the calendar of the specified month in the current year is displayed.

Example

Display the calendar of the current month.

```
<HUAWEI> display calendar
    November   2012
Sun Mon Tue Wed Thu Fri Sat
                  1   2   3
  4   5   6   7   8   9  10
 11  12  13  14  15  16  17
```



```
 18  19  20  21  22  23  24
 25  26  27  28  29  30
Today is 16 November 2012.
```

Display the calendar of May 2008.

```
<HUAWEI> display calendar May 2008
      May    2008
Sun Mon Tue Wed Thu Fri Sat
                  1   2   3
  4   5   6   7   8   9  10
 11  12  13  14  15  16  17
 18  19  20  21  22  23  24
 25  26  27  28  29  30  31
Today is 16 November 2012.
```

Table 2-20 Description of the **display calendar** command output

Item	Description
Sun	Sunday
Mon	Monday
Tue	Tuesday
Wed	Wednesday
Thu	Thursday
Fri	Friday
Sat	Saturday

2.4.6 display clock

Function

The **display clock** command displays the current date and clock setting.

Format

display clock [**utc**]

Parameters

Parameter	Description	Value
utc	Indicates that the clock is adjusted to the Coordinated Universal Time (UTC).	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display clock** command to view the system date and clock setting and adjust the setting if necessary.

Precautions

The system clock is set using the **clock datetime**, **clock timezone**, and **clock daylight-saving-time** commands.

- If the three commands are not used, the original system clock is displayed after you run the **display clock** command.
- You can use any combination of the three commands to configure the system time. **Table 2-21** lists the formats of the configured time.

The table assumes that the original system time is 08:00:00 on January 1, 2010.

- 1: indicates that the **clock datetime** command is used, in which the current time and date is *date-time*.
- 2: indicates that the **clock timezone** command is used, in which the time zone parameter is set and the time offset is *zone-offset*.
- 3: indicates that the **clock daylight-saving-time** command is used, in which the DST parameters are set and the time offset is *offset*.
- [1]: indicates that the **clock datetime** command is optional.

Table 2-21 System clock setting examples

Action	System Time Configuration	Example
1	*date-time*	Command: **clock datetime 8:0:0 2011-11-12** Configured system time: 2011-11-12 08:00:06 Saturday Time Zone(DefaultZoneName) : UTC
2	Original system time ± *zone-offset*	Command: **clock timezone BJ add 8** Configured system time: 2010-01-01 16:00:30+08:00 Friday Time Zone(BJ) : UTC+08:00
1, 2	*date-time* ± *zone-offset*	Commands: **clock datetime 8:0:0 2011-11-12** and **clock timezone BJ add 8** Configured system time: 2011-11-12 16:00:10+08:00 Saturday Time Zone(BJ) : UTC+08:00

Action	System Time Configuration	Example
[1], 2, 1	*date-time*	Commands: **clock timezone NJ add 8** and **clock datetime 9:0:0 2011-11-12** Configured system time: 2011-11-12 09:00:07+08:00 Saturday Time Zone(NJ) : UTC+08:00
3	If the original system time is not in the DST segment, the original system time is displayed.	Command: **clock daylight-saving-time BJ one-year 6:0 2011-8-1 6:0 2011-10-01 1** Configured system time: 2010-01-01 08:00:16 Friday Time Zone(DefaultZoneName) : UTC Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2011 End year : 2011 Start time : 08-01 06:00:00 End time : 10-01 06:00:00 Saving time : 01:00:00
	If the original system time is in the DST segment, the configured system time is the original system time plus *offset*.	Command: **clock daylight-saving-time BJ one-year 6:0 2010-1-1 6:0 2010-9-1 2** Configured system time: 2010-01-01 10:00:26+02:00 DST Friday Time Zone(BJ) : UTC Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2010 End year : 2010 Start time : 01-01 06:00:00 End time : 09-01 06:00:00 Saving time : 02:00:00
1, 3	If *date-time* is not in the DST segment, the configured system time is *date-time*.	Commands: **clock datetime 9:0:0 2011-11-12** and **clock daylight-saving-time BJ one-year 6:0 2012-8-1 6:0 2012-10-01 1** Configured system time: 2011-11-12 09:00:26 Saturday Time Zone(DefaultZoneName) : UTC Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2012 End year : 2012 Start time : 08-01 06:00:00 End time : 10-01 06:00:00 Saving time : 01:00:00

Action	System Time Configuration	Example
	If *date-time* is in the DST segment, the configured system time is *date-time* +*offset*.	Commands: **clock datetime 9:0:0 2011-11-12** and **clock daylight-saving-time BJ one-year 9:0 2011-11-12 6:0 2011-12-01 2** Configured system time: 2011-11-12 11:02:21 DST Saturday Time Zone(BJ) : UTC Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2011 End year : 2011 Start time : 11-12 09:00:00 End time : 12-01 06:00:00 Saving time : 02:00:00
[1], 3, 1	If *date-time* is not in the DST segment, the configured system time is *date-time*.	Commands: **clock daylight-saving-time BJ one-year 6:0 2012-8-1 6:0 2012-10-01 1** and **clock datetime 9:0 2011-11-12** Configured system time: 2011-11-12 09:00:02 Saturday Time Zone(DefaultZoneName) : UTC Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2012 End year : 2012 Start time : 08-01 06:00:00 End time : 10-01 06:00:00 Saving time : 01:00:00
	If *date-time* is in the DST segment, the configured system time is *date-time*.	Commands: **clock daylight-saving-time BJ one-year 1:0 2011-1-1 1:0 2011-9-1 2** and **clock datetime 3:0 2011-1-1** Configured system time: 2011-01-01 03:00:19 DST Saturday Time Zone(BJ) : UTC Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2011 End year : 2011 Start time : 01-01 01:00:00 End time : 09-01 01:00:00 Saving time : 02:00:00

Action	System Time Configuration	Example
2, 3 or 3, 2	If the result of original system time ± *zone-offset* is not in the DST segment, the configured system time is equal to the original system time ± *zone-offset*.	Commands: **clock timezone BJ add 8** and **clock daylight-saving-time BJ one-year 6:0 2011-1-1 6:0 2011-9-1 2** Configured system time: 2010-01-01 16:01:29+08:00 Friday Time Zone(BJ) : UTC+08:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2011 End year : 2011 Start time : 01-01 06:00:00 End time : 09-01 06:00:00 Saving time : 02:00:00
	If the result of original system time ± *zone-offset* is in the DST segment, the configured system time is equal to the original system time ± *zone-offset* ± *offset*.	Commands: **clock daylight-saving-time BJ one-year 1:0 2010-1-1 1:0 2010-9-1 2** and **clock timezone BJ add 8** Configured system time: 2010-01-01 18:05:31+08:00 DST Friday Time Zone(BJ) : UTC+08:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2010 End year : 2010 Start time : 01-01 01:00:00 End time : 09-01 01:00:00 Saving time : 02:00:00
1, 2, 3 or 1, 3, 2	If the value of *date-time* ± *zone-offset* is not in the DST segment, the configured system time is equal to *date-time* ± *zone-offset*.	Commands: **clock datetime 8:0:0 2011-11-12**, **clock timezone BJ add 8**, and **clock daylight-saving-time BJ one-year 6:0 2012-1-1 6:0 2012-9-1 2** Configured system time: 2011-11-12 08:01:40+08:00 Saturday Time Zone(BJ) : UTC+08:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2012 End year : 2012 Start time : 01-01 06:00:00 End time : 09-01 06:00:00 Saving time : 02:00:00

Action	System Time Configuration	Example
	If the value of *date-time* ± *zone-offset* is in the DST segment, the configured system time is equal to *date-time* ± *zone-offset* + *offset*.	Commands: **clock datetime 8:0:0 2011-1-1**, **clock daylight-saving-time BJ one-year 6:0 2011-1-1 6:0 2011-9-1 2** and **clock timezone BJ add 8** Configured system time: 2011-01-01 10:00:43+08:00 DST Saturday Time Zone(BJ) : UTC+08:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2011 End year : 2011 Start time : 01-01 06:00:00 End time : 09-01 06:00:00 Saving time : 02:00:00
[1], 2, 3, 1 or [1], 3, 2, 1	If *date-time* is not in the DST segment, the configured system time is *date-time*.	Commands: **clock daylight-saving-time BJ one-year 6:0 2012-1-1 6:0 2012-9-1 2**, **clock timezone BJ add 8**, and **clock datetime 8:0:0 2011-11-12** Configured system time: 2011-11-12 08:00:03+08:00 Saturday Time Zone(BJ) : UTC+08:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2012 End year : 2012 Start time : 01-01 06:00:00 End time : 09-01 06:00:00 Saving time : 02:00:00
	If *date-time* is in the DST segment, the configured system time is *date-time*.	Commands: **clock timezone BJ add 8**, **clock daylight-saving-time BJ one-year 1:0 2011-1-1 1:0 2011-9-1 2**, and **clock datetime 3:0:0 2011-1-1** Configured system time: 2011-01-01 03:00:03+08:00 DST Saturday Time Zone(BJ) : UTC+08:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2011 End year : 2011 Start time : 01-01 01:00:00 End time : 09-01 01:00:00 Saving time : 02:00:00

Example

Display the current system date and time.

```
<HUAWEI> display clock
```



```
2013-02-07 15:34:02+08:00
Thursday
Time Zone(BJ) : UTC+08:00
Daylight saving time :
        Name        : BJ
        Repeat mode : one-year
        Start year  : 2013
        End year    : 2013
        Start time  : 06-01 00:00:00
        End time    : 09-01 00:00:00
        Saving time : 02:00:00
```

Display the UTC of the system.

```
<HUAWEI> display clock utc
2012-04-23 15:11:20
Monday
```

Table 2-22 Description of the **display clock** command output

Item	Description
Time Zone	Time zone.
Daylight saving time	DST.
Name	DST name.
Repeat mode	DST mode. • one-year: absolute DST • repeat: periodic DST
Start year	Year from which DST starts.
End year	Year when DST ends.
Start time	Time when DST starts.
End time	Time when DST ends.
Saving time	Storage time.

2.4.7 display sys-netid

Function

The **display sys-netid** command displays the name of a network element (NE).

Format

display sys-netid

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check the NE name. If the NE name is not set on the device, the system displays a message indicating that the NE name is not set.

Example

Display the NE name.

```
<HUAWEI> display sys-netid
Info: The NetID is: huawei-1234567890
```

2.4.8 sysname

Function

The **sysname** command sets a device host name.

The **undo sysname** command restores the default device host name.

By default, the device host name is HUAWEI.

Format

sysname *host-name*

undo sysname

Parameters

Parameter	Description	Value
host-name	Specifies a host name.	The value is a string of 1 to 246 case-sensitive characters. It can contain spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Changing the host name of a device affects the CLI prompt. For example, if the host name of the device is HUAWEI, the prompt of the user view is <HUAWEI>.

Example

Set the host name of the device to HUAWEIA.

```
<HUAWEI> system-view
[HUAWEI] sysname HUAWEIA
[HUAWEIA]
```

2.4.9 sys-netid

Function

The **sys-netid** command sets a name for a network element (NE).

The **undo sys-netid** command deletes the NE name.

By default, no NE name is set.

Format

sys-netid *netid*

undo sys-netid

Parameters

Parameter	Description	Value
netid	Specifies the NE name.	The value is a string of 16 to 240 case-sensitive characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the network management tool needs to obtain the name of an NE, you can run the **sys-netid** command to set the NE name. The NE name is the same as that obtained from the MIB object hwEntitySystemNetID.

Precautions

If you run the **sys-netid** command multiple times, only the latest configuration takes effect.

Example

Set the NE name.

```
<HUAWEI> system-view
[HUAWEI] sys-netid huawei-1234567890
Info: NetID set successfully.
Info: New NetID is: huawei-1234567890.
```

2.5 UI Configuration Commands

2.5.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

2.5.2 acl (user interface view)

Function

The **acl** command uses an ACL to restrict login rights of users on a terminal.

The **undo acl** command cancels the configuration.

By default, login rights are not restricted.

Format

acl [**ipv6**] { *acl-number* | *acl-name* } { **inbound** | **outbound** }

undo acl [**ipv6**] [*acl-number* | *acl-name*] { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
ipv6	Indicates an ACL6 number.	-
acl-number	Specifies the number of an ACL.	The value is an integer ranging from 2000 to 3999. • 2000-2999: restricts the source address using the basic ACL. • 3000-3999: restricts the source and destination addresses using the advanced ACL.

Parameter	Description	Value
acl-name	Specifies the name of an ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter. **NOTE** When the number of the ACL configured using the **acl name** command ranges from 2000 to 3999, the *acl-name* parameter can be successfully delivered using the **acl (user interface view)** command. • 2000-2999: restricts the source address using the basic ACL. • 3000-3999: restricts the source and destination addresses using the advanced ACL.
inbound	Restricts users with an address or within an address segment from logging in to a device.	-
outbound	Restricts users who have logged in to a device from logging in to other devices.	-

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command restricts the login rights of a user interface based on the source IP address, destination IP address, source port, destination port, VPN instance, or packets whose protocol type is TCP. You can use this command to permit or deny access to a destination or from a source.

Prerequisites

An ACL has been configured using the **acl (system view)** and **rule (basic ACL view)** commands or using **acl (system view)** and **rule (advanced ACL view)** commands.

If no rule is configured, login rights on the user interface are not restricted when the **acl** command is run.

Precautions

After the configurations of the ACL take effect, all users on the user interface are restricted by the ACL.

You can configure all of the following ACL types: IPv4 inbound, IPv4 outbound, IPv6 inbound, and IPv6 outbound on a user interface. Only one ACL of each type can be configured on a user interface, and only the latest configuration of an ACL takes effect.

Console interface does not support this command.

Example

Restrict the Telnet login rights on user interface VTY 0 using an ACL.

```
<HUAWEI> system-view
[HUAWEI] acl 3001
[HUAWEI-acl-adv-3001] rule deny tcp destination-port eq telnet
[HUAWEI-acl-adv-3001] quit
[HUAWEI] user-interface vty 0
[HUAWEI-ui-vty0] acl 3001 outbound
```

Remove the restriction on the Telnet login rights on user interface VTY 0.

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0
[HUAWEI-ui-vty0] undo acl outbound
```

2.5.3 authentication-mode (user interface view)

Function

The **authentication-mode** command configures an authentication mode for accessing the user interface.

The **undo authentication-mode** command deletes the authentication mode for accessing the user interface.

The default authentication mode for console port login users is password authentication. By default, the authentication mode for users using other login modes is not configured using this command. You must configure an authentication mode for accessing the user interface; otherwise, users cannot log in to the device.

Format

authentication-mode { **aaa** | **password** }

undo authentication-mode

Parameters

Parameter	Description	Value
aaa	Indicates the AAA authentication mode.	-
password	Indicates the password authentication mode.	-

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After entering the default user name and password, you must reconfigure the login password and then can log in to the device. After logging in to the device, you can run this command to reconfigure the authentication mode.

Before Telnet or SSH users log in to the device using VTY user interface, they must run the **authentication-mode** command to configure the authentication mode.

Precautions

To ensure that users can log in to the device successfully, configure an authentication mode.

Before setting the Telnet login authentication mode to password authentication, run the **protocol inbound** { **all** | **telnet** } command to configure the VTY user interface to support Telnet. Otherwise, the user authentication mode configuration will fail.

NOTICE

The **none** parameter is not contained in the command. To specify this parameter, install the empty password authentication plug-in. This parameter, however, brings security risks, and the **aaa** or **password** parameter is recommended.

You can search for **Plug-in Usage Guide** at the Huawei technical support website (**Enterprise Network** or **Carrier**), and choose the desired plug-in usage guide based on the switch model and software version. If you do not have permission to access the website, contact technical support personnel.

- After you set the authentication mode to **password**, run the **set authentication password** command to configure an authentication password. Keep the password safe. You need to enter the password when logging in to the device. The levels of commands accessible to a user depend on the level configured for the user interface to which the user logs in.
- After login, the level of the commands the user can run depends on the level of the local user specified in AAA configuration.
- When you run the **undo authentication-mode** command to delete the authentication mode, the device asks you whether to delete the authentication mode.
- In V200R009 and earlier versions, the console port uses non-authentication by default. From V200R010 to V200R019, the console port uses AAA authentication by default. In V200R020C00 and later versions, the console port uses password authentication by default.

- If a device runs a version earlier than V200R010C00 and the authentication mode for accessing the user interface is not configured using this command, the default authentication mode is still non-authentication after the system software is upgraded to V200R010C00 or a later version. The system asks you whether to change the password. To ensure the console port usage security, it is recommended that you configure the login password or set the authentication mode to AAA or password authentication after logging in to the device.
- If a device runs a version earlier than V200R010C00 and the authentication mode for accessing the user interface has been configured using this command, the default authentication mode is still the originally configured authentication mode after the system software is upgraded to V200R010C00 or a later version.

Example

Configure password authentication for users to access the user interface.

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0
[HUAWEI-ui-vty0] protocol inbound all
[HUAWEI-ui-vty0] authentication-mode password
Warning: The "password" authentication mode is not secure, and it is strongly re
commended to use "aaa" authentication mode.
[HUAWEI-ui-vty0] set authentication password cipher YsHsjx_202206
Warning: The "password" authentication mode is not secure, and it is strongly re
commended to use "aaa" authentication mode.
```

2.5.4 auto-execute command

Function

The **auto-execute command** command configures auto-run commands.

The **undo auto-execute command** command cancels auto-run commands.

By default, the auto-run function is disabled.

Format

auto-execute command *command*

undo auto-execute command

Parameters

Parameter	Description	Value
command	Specifies an auto-run command.	-

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **auto-execute command** command to make a device run a command automatically on the corresponding user interface.

You can run the **auto-execute command** command to enable automatic execution of the **Telnet** command.

Precautions

- The **auto-execute command** command applies to the VTY user interface.
- When you log in to a device, the device automatically runs the commands that are configured by the **auto-execute command** command. After command execution, the user's terminal disconnects from the device.
- Before saving the configuration of the **auto-execute command** command, ensure that you can log in to the device to cancel the command configuration.
- If you use the **auto-execute command** command, you cannot configure the device in the user interface view. Therefore, use this command with caution.

Example

Configure the **telnet 10.110.100.1** command to automatically run after a user logs in to the device using the VTY0 interface.

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0
[HUAWEI-ui-vty0] auto-execute command telnet 10.110.100.1
Warning: The system will not be configured through ui-vty0.
Continue? [Y/N]: y
```

2.5.5 databits

Function

The **databits** command sets the number of data bits of the user interface.

The **undo databits** command restores the default number of data bits.

By default, the user interface has 8 data bits.

Format

databits { **5** | **6** | **7** | **8** }

undo databits

Parameters

Parameter	Description	Value
5	Indicates that the number of data bits is 5.	-
6	Indicates that the number of data bits is 6.	-
7	Indicates that the number of data bits is 7.	-
8	Indicates that the number of data bits is 8.	-

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Use this command only when necessary. If the number of data bits of a device's user interface is changed, ensure that the same number of data bits is set on the HyperTerminal used for login.

The setting is valid only when the serial port is configured to work in asynchronous mode.

Example

Set the number of data bits to 5.

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] databits 5
```

2.5.6 display user-interface

Function

The **display user-interface** command displays information about a user interface.

Format

display user-interface [*ui-type ui-number1* | *ui-number*] [**summary**]

Parameters

Parameter	Description	Value
ui-type	Displays information about a specified user interface.	The value can be Console or VTY.

Parameter	Description	Value
ui-number1	Displays information about a user interface with a specified relative number.	The minimum value is 0. The maximum value is the number of user interfaces that the system supports minus 1.
ui-number	Displays information about a user interface with a specified absolute number.	The value is an integer ranging from 0 to 54, 67 to 83. The value varies according to the device type.
summary	Displays the summary of a user interface.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

To check detailed configuration information about all user interfaces or a specified user interface, run the **display user-interface** command.

Example

Display detailed information about the user interface with the absolute number 0.

```
<HUAWEI> display user-interface 0
  Idx  Type     Tx/Rx      Modem Privi ActualPrivi      Auth  Int
  0    CON 0    9600       -     3     -                P     -
  +    : Current UI is active.
  F    : Current UI is active and work in async mode.
  Idx  : Absolute index of UIs.
  Type : Type and relative index of UIs.
  Privi: The privilege of UIs.
  ActualPrivi: The actual privilege of user-interface.
  Auth : The authentication mode of UIs.
      A: Authenticate use AAA.       N: Current UI need not authentication.       P: Authenticate use current
UI's password.
  Int  : The physical location of UIs.
```

Display detailed information about all user interfaces.

```
<HUAWEI> display user-interface
  Idx  Type     Tx/Rx      Modem Privi ActualPrivi      Auth  Int
  0    CON 0    9600         -     3     -                P     -
+ 34   VTY 0                -     3     3                A     -
+ 35   VTY 1                -     1     2                A     -
+ 36   VTY 2                -     3     2                A     -
  37   VTY 3                -     1     -                P     -
  38   VTY 4                -     1     -                A     -
...
UI(s) not in async mode -or- with no hardware support:
```



```
1-32
  +    : Current UI is active.
  F    : Current UI is active and work in async mode.
  Idx  : Absolute index of UIs.
  Type : Type and relative index of UIs.
  Privi: The privilege of UIs.
  ActualPrivi: The actual privilege of user-interface.
  Auth : The authentication mode of UIs.
      A: Authenticate use AAA.       N: Current UI need not authentication.       P: Authenticate use current
UI's password.
  Int  : The physical location of UIs.
```

Table 2-23 Description of the **display user-interface** command output

Parameter	Description
+	Active user interface.
F	Active user interface in asynchronous mode.
Idx	Absolute number of a user interface.
Type	Type and relative number of a user interface.
Tx/Rx	Data transfer rate of the user interface.
Modem	Type of the modem.
Privi	Authority configured on a user interface.
ActualPrivi	Actual permission of a user interface. In AAA authentication mode, the level of a local user in AAA configuration is the actual permission.
Auth	Authentication mode on a user interface.
Int	User interface.
A	AAA authentication.
N	No authentication on the current user interface.
P	Password authentication.

2.5.7 display user-interface maximum-vty

Function

The **display user-interface maximum-vty** command displays the maximum number of VTY users.

Format

display user-interface maximum-vty

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

To check the maximum number of users who are allowed to log in to a device using Telnet or SSH, run the **display user-interface maximum-vty** command. By default, the maximum number of total Telnet and SSH users is five.

Example

Display the maximum number of VTY users.

```
<HUAWEI> display user-interface maximum-vty
Maximum of VTY user : 5
```

Table 2-24 Description of the **display user-interface maximum-vty** command output

Parameter	Description
Maximum of VTY user	Maximum number of VTY users. The maximum number of VTY users can be configured using the **user-interface maximum-vty** command.

2.5.8 display users

Function

The **display users** command displays login information of each user interface.

Format

display users [**all**]

Parameters

Parameter	Description	Value
all	Displays information about all users who log in to a device through user interfaces, including information about user interfaces that are not connected. If the **all** parameter is not used, the command displays information only about user interfaces that have been connected.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about users who are connected to a device. The information includes the user name, IP address, and authentication and authorization information.

NOTE

The user with a level of 0, 1, or 2 can only view related information about users of the same or a lower level. A user with a level of 3 or above can view login information of all users.

Example

Display information about users who log in to the device through user interfaces.

```
<HUAWEI> display users
  User-Intf    Delay     Type   Network Address     AuthenStatus    AuthorcmdFlag
  34 VTY 0    00:00:00  TEL    10.164.6.10           pass            no
  Username : user1
+ 35 VTY 1    00:00:00  TEL    10.164.6.15           pass            no
  Username : user2
```

Table 2-25 Description of the **display users** command output

Item	Description
+	User interface in use.
User-Intf	The number in the first column under **User-Intf** indicates the absolute number of the user interface, and the number in the second column under **User-Intf** indicates the relative number of the user interface. User Interface type. ● Console: Users who log in through the console port ● VTY: Users who log in using VTY ● LTT: User logs in stack system through the non-master switch console port ● WEB: Users who log in through Web system
Delay	Interval from the user's latest input on the login page to the current time, in seconds.

Item	Description
Type	Connection type. • Console • Telnet • SSH • Web
Network Address	IP address of the login user.
Username	User name for logging in to the device. If the user name is not specified, **Unspecified** is displayed.
AuthenStatus	Whether the authentication succeeds.
AuthorcmdFlag	Command line authorization status. • yes: Command line authentication is enabled. • no: Command line authentication is disabled.

2.5.9 display vty mode

Function

The **display vty mode** command displays the current VTY mode.

Format

display vty mode

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

VTY modes are classified into the man-to-machine mode and machine-to-machine mode.

Example

Display the VTY mode.


```
<HUAWEI> display vty mode
Current user-interface mode is Human-Machine interface.
```

2.5.10 display vty lines

Function

The **display vty lines** command displays the number of rows that are displayed on the VTY screen.

Format

display vty lines

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to view the number of rows (configured using **screen-length** command) that are displayed on the VTY screen.

Example

Display the number of rows that are displayed on the VTY screen.

```
<HUAWEI> display vty lines
Current user-interface lines is 24
```

2.5.11 display web welcome-message

Function

The **display web welcome-message** command displays greetings of the web system.

Format

display web welcome-message

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display web welcome-message** command to view greetings of the web system.

Example

Display greetings of the web system.

```
<HUAWEI> display web welcome-message
huawei
```

2.5.12 flow-control

Function

The **flow-control** command configures a flow control mode.

The **undo flow-control** command restores the default flow control mode.

The default flow control mode is **none**, that is, flow control is disabled.

Format

flow-control { **hardware** | **none** | **software** }

undo flow-control

NOTE

Currently, the flow control mode of the device cannot be set to hardware.

Parameters

Parameter	Description	Value
hardware	Specifies hardware flow control.	-
none	Specifies no flow control.	-
software	Specifies software flow control.	-

Views

User interface view

Default Level

3: Management level

Usage Guidelines

The configuration is effective only when the serial interface works in asynchronous interaction mode.

If the flow control mode cannot be configured on a device, the system prompts the message **"Error: Failed to run this command because of internal causes of system malfunctions.**"

Example

Set the flow control mode to software flow control in the user interface view.

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] flow-control software
```

2.5.13 free user-interface

Function

The **free user-interface** command disconnects a user from a specified user interface.

Format

free user-interface { *ui-number* | *ui-type ui-number1* }

Parameters

Parameter	Description	Value
ui-number	Specifies the absolute number of a user interface.	The value is an integer ranging from 0 to 54 and 67 to 83. The value varies according to the device type.
ui-type	Specifies the type of a user interface.	The value can be console or VTY.
ui-number1	Specifies the relative number of a user interface.	The minimum value is 0. The maximum value is the number of user interfaces that the system supports minus 1.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a login user does not perform any operation for a long time or needs to be prohibited from configuring the device, run the **free user-interface** command to disconnect the user from the user interface. The device then logs out the user.

Precautions

The **free user-interface** command does not take effect for the current user interface. For example, if the current user interface is VTY 2, the **free user-interface vty 2** command does not take effect, and an error message is displayed.

This command provides the same function as the **kill user-interface** command.

Example

Disconnect the user from user-interface 0.

```
<HUAWEI> free user-interface 0
Warning: User interface Console1 will be freed. Continue? [Y/N]:y
```

2.5.14 kill user-interface

Function

The **kill user-interface** command disconnects a user from a user interface.

NOTE

The **kill user-interface** command can only be executed by users at level 3 or higher. These users can clear any other users.

Format

kill user-interface { *ui-number* | *ui-type ui-number1* }

Parameters

Parameter	Description	Value
ui-number	Specifies the absolute number of a user interface.	The value is an integer ranging from 0 to 54 and 67 to 83. The value varies according to the device type.
ui-type	Specifies the type of a user interface.	The value can be console or VTY.
ui-number1	Specifies the relative number of a specified user interface.	The minimum value is 0. The maximum value is the number of user interfaces that the system supports minus 1.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a login user does not perform any operation for a long time or needs to be prohibited from configuring the device, run the **kill user-interface** command to disconnect the user from the user interface. The device then logs out the user.

Precautions

The **kill user-interface** command does not take effect for the current user interface. For example, if the current user interface is VTY 2, the **kill user-interface vty 2** command does not take effect, and an error message is displayed.

This command provides the same function as the **free user-interface** command.

Example

Disconnect user VTY3 from the device.

```
<HUAWEI> kill user-interface vty 3
Warning: User interface VTY3 will be freed. Continue? [Y/N]:y
Info: User interface VTY3 is free.
```

2.5.15 history-command max-size

Function

The **history-command max-size** command sets the size of the historical command buffer.

The **undo history-command max-size** command restores the default size of the historical command buffer.

By default, a maximum of 10 previously-used commands can be saved in the buffer.

Format

history-command max-size *size-value*

undo history-command max-size

Parameters

Parameter	Description	Value
size-value	Specifies the size of the historical command buffer.	The value is an integer ranging from 0 to 256.

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The CLI can automatically save the historical commands that you enter. This function is similar to that of Doskey. You can invoke and run the historical commands at any time.

Precautions

- If the historical command buffer is used up and a new command is entered, the command line interface deletes the earliest command in the buffer in the sequence the commands were entered.
- The formats of the saved historical commands are the same as those of the commands entered by users. If the commands entered by a user are incomplete, the saved historical commands are also incomplete.
- If a user runs the same command several times, only the earliest command is saved as a historical command. However, if the same command is entered with different formats, they are saved as different commands.

Example

Set the size of the historical command buffer to 20.

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] history-command max-size 20
```

2.5.16 idle-timeout

Function

The **idle-timeout** command sets a timeout period for users to disconnect from a user interface.

The **undo idle-timeout** command restores the default timeout period.

By default, the timeout period is 10 minutes.

Format

idle-timeout *minutes* [*seconds*]

undo idle-timeout

Parameters

Parameter	Description	Value
minutes	Specifies the idle timeout period, in minutes.	The value is an integer ranging from 0 to 35791.
seconds	Specifies the idle timeout period, in seconds.	The value is an integer ranging from 0 to 59.

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If an online user does not perform any operation, the user interface where the user logs in is wasted. To resolve this problem, run the **idle-timeout** command to set a timeout period. If the user does not perform any operation before the timeout period expires, the user is disconnected from the user interface.

Precautions

- If you set the timeout period to 0, the user connection remains alive until it is manually cut.
- If you set the timeout period to 0 or a large value, the user will remain in the login state, resulting in security risks. You are advised to run the **lock** command to lock the current connection.
- If the user interface disconnection function is not configured, other users may fail to log in to the device. You are advised to set the timeout period to 10-15 minutes.

NOTE

If AAA authentication is used, the **local-user idle-timeout** *minutes* [*seconds*] command takes precedence. If both the commands are configured, the value configured using the **local-user idle-timeout** command takes effect.

If RADIUS authentication is used, the RADIUS attribute **Idle-Timeout** takes precedence. If both the **Idle-Timeout** attribute and the **idle-timeout** command are configured, value of the RADIUS attribute **Idle-Timeout** takes effect.

Example

Set the timeout period to 1 minute and 30 seconds.


```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] idle-timeout 1 30
```

2.5.17 mmi-mode enable

Function

The **mmi-mode enable** command enters the machine-to-machine mode.

The **undo mmi-mode enable** command enters the man-to-machine mode.

By default, a VTY user is in man-to-machine mode.

Format

mmi-mode enable

undo mmi-mode enable

Parameters

None

Views

User view, system view

Default Level

0: Visit level

Usage Guidelines

The machine-to-machine mode is used on the NMS. After you enter the machine-to-machine mode using the **mmi-mode enable** command, some important commands that you need to use with caution can be used directly. Therefore, in man-to-machine mode, do not use this command unless necessary.

After you enter the machine-to-machine mode, the maximum number of lines in the screen of the current user interface is restored to the default value (512). You can run the **screen-length** command to change the default value.

Example

Enter the machine-to-machine mode.

```
<HUAWEI> system-view
[HUAWEI] mmi-mode enable
```

2.5.18 parity

Function

The **parity** command sets a parity bit for a user interface.

The **undo parity** command disables the parity check.

By default, no parity check is configured.

Format

parity { **even** | **mark** | **none** | **odd** | **space** }

undo parity

Parameters

Parameter	Description	Value
even	Specifies even parity check.	-
mark	Specifies Mark parity check.	-
none	Specifies no parity check.	-
odd	Specifies odd parity check.	-
space	Specifies Space parity check.	-

Views

User interface view

Default Level

3: Management level

Usage Guidelines

The setting is valid only when the serial port is configured to work in asynchronous mode.

If the parity bit for a user interface cannot be set on a device, the system prompts the message **"Error: Failed to run this command because of internal causes of system malfunctions.**"

Example

Set the transmission parity bit on the console port to odd parity.

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] parity odd
```


2.5.19 protocol inbound

Function

The **protocol inbound** command specifies the protocols that VTY user interfaces support.

The **undo protocol inbound** command restores the default protocols that VTY user interfaces support.

By default, VTY user interfaces support SSH.

Format

protocol inbound { **all** | **ssh** | **telnet** }

undo protocol inbound

Parameters

Parameter	Description	Value
all	Indicates that all protocols including SSH and Telnet are supported.	-
ssh	Indicates that only SSH is supported.	-
telnet	Indicates that only Telnet is supported.	-

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To manage and monitor login users, configure VTY user interfaces for login users and run the **protocol inbound** command to configure the protocols that the VTY user interfaces support.

Prerequisites

If SSH is configured for a user interface using the **protocol inbound ssh** command, you must run the **authentication-mode aaa** command to configure AAA authentication. This ensures that a user can successfully log in to the user interface. If password authentication is configured, the **protocol inbound ssh** command does not take effect.

Precautions

- The configuration takes effect at the next login.
- When SSH is specified for the VTY user interface, if the SSH server function is enabled but the RSA, DSA, or ECC key is not configured, a user cannot log in to the SSH server using SSH.
- Telnet is an insecure protocol. Using SSH is recommended.

Example

Configure SSH for user interfaces VTY0 to VTY4.

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0 4
[HUAWEI-ui-vty0-4] authentication-mode aaa
[HUAWEI-ui-vty0-4] protocol inbound ssh
```

2.5.20 screen-length

Function

The **screen-length** command sets the number of lines on each terminal screen.

The **undo screen-length** command restores the default configuration.

By default, the number of lines displayed on a terminal screen is 24.

Format

In the user interface view:

screen-length *screen-length* [**temporary**]

undo screen-length [**temporary**]

In the user view:

screen-length *screen-length* **temporary**

undo screen-length temporary

Parameters

Parameter	Description	Value
screen-length	Specifies the number of lines displayed on a terminal screen.	The value is an integer that ranges from 0 to 512. The value 0 indicates that all command output is displayed on one screen.
temporary	Specifies the number of lines temporarily displayed on a terminal screen.	-

Views

User interface view, user view

Default Level

3: Management level in the user interface view

1: Monitoring level in the user view

Usage Guidelines

If a command output is displayed in more lines than you can see on one screen, run the **screen-length** command to reduce the number of lines displayed on each screen.

In general, you do not need to change the number of lines displayed on each screen. Setting the number of lines to 0 is not recommended. The configuration takes effect after you log in to the system again.

NOTE

In the user view, the **temporary** parameter is mandatory, and this command is at the Monitoring level.

Example

Set the number of lines on each screen of the terminal to 30.

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] screen-length 30
```

2.5.21 screen-width

Function

The **screen-width** command sets the number of columns displayed on a terminal screen.

The **undo screen-width** command restores the default configuration.

By default, 80 columns are displayed on a terminal screen.

Format

screen-width *screen-width*

undo screen-width

Parameters

Parameter	Description	Value
screen-width	Specifies the width of a terminal screen.	The value is an integer ranging from 60 to 512.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you log in to the device from a console interface and run the **display interface description** [*interface-type* [*interface-number*]] command to view the interface information, output information does not automatically change to another line, resulting in wrong format of the output information.

To resolve this problem, run the **screen-width** command to adjust the information format. In general, you do not need to adjust the number of columns displayed on the terminal screen. Setting the number of columns displayed on a screen is not recommended.

Precautions

The number of columns set using the **screen-width** command is valid only for the current interface. The setting is not saved after you log out. When you log in to the device from the console interface and configure this command, the number of columns displayed on the terminal screen is valid only for the current console interface, which has no impact on other users who log in to the device from the VTY interface or other interfaces. If you log out of the console interface and log in to the device again, the default width is used for the terminal screen.

This command is valid only for information displayed by the **display interface description** [*interface-type* [*interface-number*]] command.

Example

Configure each line displayed on a terminal screen to have 60 characters.

```
<HUAWEI> screen-width 60
Warning: This command will change the default screen width. Continue? [Y/N]:y
Info: Succeeded in setting the screen width to 60.
```

2.5.22 set authentication password

Function

The **set authentication password** command configures a local authentication password.

The **undo set authentication password** command cancels the local authentication password.

By default, no local authentication password is configured for devices.

Format

set authentication password [**cipher** *password*]

undo set authentication password

Parameters

Parameter	Description	Value
cipher	Indicates a password in cipher text.	-
password	Specifies the password.	The value is a string of 8 to 16 characters or a string of 56 or 68 characters. The password can be in plain or cipher text. • The password in plain text is a string of 8 to 16 characters. The password must contain at least two types of the following characters: upper-case characters, lower-case characters, digits, and special characters. Special characters do not include the question mark (?) and space. • The password in cipher text is a string of 56 or 68 characters. The password in cipher text must start with $1a$ and end with $, or start with %^%# and end with %^%#. **NOTE** If the source version supports a ciphertext password that is a string of 24 characters, the target version also supports this type of password. The password is displayed in cipher text in the configuration file regardless of whether it is input in plain text or cipher text.

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If password authentication is configured for users, you can run the **set authentication password** command to change the password or set a password in cipher text.

If **cipher** *password* is not specified, the password is entered in interactive mode and can contain 8 to 16 characters. The requirements for the password are the same as the requirements for the password in plain text that is specified using the **cipher** parameter. The password you enter will not be displayed on the screen.

NOTE

If you enter the plain text password when specifying **cipher** *password*, security risks exist. The interactive mode is recommended when users enter the password.

Pre-configuration Tasks

Password authentication has been configured for the user interface.

Precautions

- If a password in cipher text is configured, users must obtain the password in plain text that is required for login authentication.
- You cannot run the **undo set authentication password** command to delete a password. The **undo set authentication password** command is retained for compatibility with other versions.
- If the password authentication is configured but the password is not configured for the user interface, the user cannot log in to the device.
- If the **set authentication password** command is executed multiple times, the latest configuration overrides the previous ones. You can run the **set authentication password** command to change the local authentication password. After the password is changed, a user who wants to log in to the device must enter the latest password for login authentication.
- Users can press **CTRL_C** to cancel password modification in the interaction mode.
- You are advised to change the password periodically to improve device security.

Example

Set a local authentication password for the user interfaces VTY 0-4 in interactive mode.

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0 4
[HUAWEI-ui-vty0-4] set authentication password
Warning: The "password" authentication mode is not secure, and it is strongly recommended to use "aaa" authentication mode.
Please configure the login password (8-16)
Enter Password:
Confirm Password:
[HUAWEI-ui-vty0-4]
```

Set a local authentication password for the user interfaces VTY 0-4.

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0 4
[HUAWEI-ui-vty0-4] set authentication password cipher YsHsjx_202206
Warning: The "password" authentication mode is not secure, and it is strongly recommended to use "aaa" authentication mode.
```

2.5.23 set password min-length

Function

The **set password min-length** command sets the minimum length of passwords in plain text allowed by a device.

The **undo set password min-length** command restores the default minimum length of passwords in plain text allowed by a device.

By default, the minimum length of passwords in plain text allowed by a device is 8 characters.

Format

set password min-length *length*

undo set password min-length

Parameters

Parameter	Description	Value
length	Specifies the minimum length of passwords in plain text allowed by a device.	The value is an integer ranging from 6 to 16.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command can change the limit on the password length. A longer password length makes the password more complex and improves device security.

Precautions

- The **set password min-length** command limits the length of all passwords in plain text. Only the passwords longer than or equal to the minimum length take effect. The minimum length does not take effect for the following passwords:
  - Passwords configured during configuration restoration
  - Passwords that have taken effect before the minimum length is configured
- This command limits the minimum length of only the passwords in plain text configured using the following commands:
  - **set authentication password**
  - **lock**
  - **local-user**
  - **super password**

  The **set password min-length** command does not limit the minimum length of other types of passwords.

NOTE

If password complexity check has been disabled using the **undo user-password complexity-check** command, the **set password min-length** command does not limit the minimum length of passwords in plain text of local users.

For device security purposes, do not disable the password complexity check function and change the password periodically.

Example

Set the minimum length of passwords in plain text allowed by the local device to 10 characters.

```
<HUAWEI> system-view
[HUAWEI] set password min-length 10
```

2.5.24 shell

Function

The **shell** command enables terminal services on a user interface.

The **undo shell** command disables terminal services on a user interface.

By default, terminal services are enabled on all user interfaces.

Format

shell

undo shell

Parameters

None

Views

User interface view

Default Level

3: Management level

Usage Guidelines

You can use the **shell** command on a user interface to enable terminal services. This command enables users to enter commands through this interface to query device information and configure the device.

You can use the **undo shell** command on the user interface to disable terminal services. This command does not allow users to perform any operations through this interface. After using the **undo shell** command in the VTY view, this user interface does not provide Telnet, STelnet, and SFTP access.

NOTE

The console interface does not support this command.

Example

Disable terminal services on VTY 0 to VTY 4.

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0 4
[HUAWEI-ui-vty0-4] undo shell
Warning: ui-vty0-4 will be disabled. Continue? [Y/N]:y
```

2.5.25 speed (user interface view)

Function

The **speed** command sets the data transfer rate of a user interface.

The **undo speed** command restores the default data transfer rate of a user interface.

By default, the data transfer rate is 9600 bit/s.

Format

speed *speed-value*

undo speed

Parameters

Parameter	Description	Value
speed-value	Specifies the data transfer rate of a user interface.	The value is expressed in bit/s. The asynchronous serial interface supports the following data transfer rates: • 300 bit/s • 600 bit/s • 1200 bit/s • 4800 bit/s • 9600 bit/s • 19200 bit/s • 38400 bit/s • 57600 bit/s • 115200 bit/s

Views

User interface view

Default Level

3: Management level

Usage Guidelines

The setting is valid only when the serial port is configured to work in asynchronous mode.

Example

Set the data transfer rate of a user interface to 115200 bit/s.

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] speed 115200
```

2.5.26 stopbits

Function

The **stopbits** command sets a stop bit for a user interface.

The **undo stopbits** command restores the default stop bit of a user interface.

The default stop bit is 1.

Format

stopbits { **1.5** | **1** | **2** }

undo stopbits

Parameters

Parameter	Description	Value
1.5	Sets the stop bit to 1.5.	-
1	Sets the stop bit to 1.	-
2	Sets the stop bit to 2.	-

Views

User interface view

Default Level

3: Management level

Usage Guidelines

If the stop bit is 1, the corresponding data bit is 7 or 8.

If the stop bit is 1.5, the corresponding data bit is 5.

If the stop bit is 2, the corresponding data bit is 6, 7, or 8.

The setting is valid only when the serial port is configured to work in asynchronous mode.

Example

Set the stop bit of a user interface to 2.

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] stopbits 2
```

2.5.27 user privilege

Function

The **user privilege** command configures a user privilege level.

The **undo user privilege** command restores the default user privilege level.

By default, users who log in to a device using the console interface are at level 15, and other users are at level 0.

Format

user privilege level *level*

undo user privilege level

Parameters

Parameter	Description	Value
level *level*	Specifies a user privilege level. **NOTE** A larger value indicates a higher priority.	The value is an integer ranging from 0 to 15.

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To limit users' access permissions to a device, the device manages users by level. Users of a specified level can run only commands whose levels are lower than or equal to the user privilege level.

Commands are classified into the visit level, monitoring level, configuration level, and management level that map levels 0, 1, 2, and 3, respectively. **Table 2-26** describes these command privilege levels.

Table 2-26 Command privilege levels

User Privilege Level	Command Privilege Level	Permission	Description
0	0	Visit	Diagnostic commands, such as ping and tracert commands, and commands that are used to access a remote device such as a Telnet client
1	0 and 1	Monitoring	System maintenance commands, such as display commands **NOTE** Some display commands are not at this level. For example, the **display current-configuration** and **display saved-configuration** commands are at level 3.
2	0, 1, and 2	Configuration	Service configuration commands
3-15	0, 1, 2, and 3	Management	System basic operation commands that are used to support services, including file system, FTP, TFTP, user management commands, command-level configuration commands, and debugging commands.

Precautions

If refined permission management is required, run the **command-privilege level** command to upgrade command privilege levels.

Example

Set the user privilege level on the VTY0 user interface to 2.

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 0
[HUAWEI-ui-vty0] user privilege level 2
```

Log in to the device using Telnet and view detailed information about the VTY0 user interface.

```
<HUAWEI> display user-interface vty 0
  Idx  Type     Tx/Rx      Modem Privi ActualPrivi Auth  Int
+ 34   VTY 0              -     2     15          N     -
  +    : Current UI is active.
  F    : Current UI is active and work in async mode.
  Idx  : Absolute index of UIs.
```



```
Type : Type and relative index of UIs.
Privi: The privilege of UIs.
ActualPrivi: The actual privilege of user-interface.
Auth : The authentication mode of UIs.
   A: Authenticate use AAA.
   N: Current UI need not authentication.
   P: Authenticate use current UI's password.
Int  : The physical location of UIs.
```

Table 2-27 Description of the **user privilege level** command output.

Item	Description
+	Current user interface is active.
F	Current user interface is active and is working in asynchronous mode.
Idx	Absolute index of the user interface.
Type	Type and relative index of the user interface.
Privi	Privilege of the user interface.
ActualPrivi	Actual privilege of the user interface.
Auth	Authentication mode of the user interface.
Int	Physical location of UIs.
A	AAA authentication.
N	None authentication
P	Password authentication

2.5.28 user-interface

Function

The **user-interface** command displays one or multiple user interface views.

Format

user-interface [*ui-type*] *first-ui-number* [*last-ui-number*]

Parameters

Parameter	Description	Value
ui-type	Specifies the type of a user interface. • If the user interface is specified, the relative number is used. • If the user interface is not specified, the absolute number is used.	The value can be console or VTY.
first-ui-number	Specifies the number of the first user interface.	• If *ui-type* is set to **console**, the *first-ui-number* value is **0**. • If *ui-type* is set to **vty**, the *first-ui-number* value ranges from 0 to the maximum number of VTY user interfaces.
last-ui-number	Specifies the number of the last user interface. When you select this parameter, you enter multiple user interface views at the same time. This parameter is valid only when *ui-type* is set to VTY. The *last-ui-number* value must be larger than the *first-ui-number* number. If the maximum number of VTY users has been set using the **user-interface maximum-vty** command in the system view before *ui-type* is selected, the *last-ui-number* value is smaller than or equal to the maximum number of VTY user interfaces minus one.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a network administrator logs in to a device using the console interface, Telnet, or SSH, the network administrator can set parameters, such as an

authentication more and user privilege level, on the user interface to allow the device to centrally manage user sessions.

Precautions

Only users at level 15 can use this command.

The user interface varies according to the login mode. The user interface views can be numbered using absolute numbers or relative numbers. **Table 2-28** describes absolute and relative numbers of user interfaces.

NOTE

- The relative numbering uniquely specifies a user interface or a group of user interfaces of the same type.
- The absolute numbering specifies a user interface or a group of user interfaces.

Table 2-28 Absolute and relative numbers of user interfaces

User Interface	Description	Absolute Number	Relative Number
Console user interface	Manages and controls users who log in to the device using the console interface.	0	0
VTY user interface	Manages and controls users who log in to the device using Telnet or SSH.	34 to 48 and 50 to 54	The first one is VTY 0, the second one is VTY 1, and so forth. • Absolute numbers 34 to 48 map relative numbers VTY 0 to VTY 14. • Absolute numbers 50 to 54 map relative numbers VTY 16 to VTY 20. VTY 15 is reserved for the system. VTY 16 to VTY 20 are reserved for the NMS. Only when VTY 0 to VTY 14 are all used, AAA authentication is configured for users, VTY 16 to VTY 20 can be used.

After you log in to the device, you can run the **display user-interface** command to view the supported user interfaces and the corresponding relative and absolute numbers.

Example

Enter the Console 0 user interface.

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0]
```

Enter the VTY 1 user interface.

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 1
[HUAWEI-ui-vty1]
```

Enter the VTY 1 to VTY 3 user interfaces.

```
<HUAWEI> system-view
[HUAWEI] user-interface vty 1 3
[HUAWEI-ui-vty1-3]
```

2.5.29 user-interface current

Function

The **user-interface current** command displays the current user interface view.

Format

user-interface current

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To enter the current user interface view, run the **user-interface current** command, without the need to run the **display user-interface** command to check the user interface number.

Precautions

Only users at level 15 can use this command.

The user interface varies according to the login mode. The user interface views can be numbered using absolute numbers or relative numbers. **Table 2-28** describes absolute and relative numbers of user interfaces.

NOTE

- The relative numbering uniquely specifies a user interface or a group of user interfaces of the same type.
- The absolute numbering specifies a user interface or a group of user interfaces.

Example

Enter the current user view.

```
<HUAWEI> system-view
[HUAWEI] user-interface current
[HUAWEI-ui-vty1]
```

2.5.30 user-interface maximum-vty

Function

The **user-interface maximum-vty** command configures the maximum number of login users.

The **undo user-interface maximum-vty** command restores the default maximum number of login users.

By default, the maximum number of Telnet and SSH users is 5.

Format

user-interface maximum-vty *number*

undo user-interface maximum-vty

Parameters

Parameter	Description	Value
number	Specifies the maximum number of Telnet and SSH users.	The value is an integer ranging from 0 to 15.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure the maximum number of login users, run the **user-interface maximum-vty** command.

Precautions

- If the maximum number that you set is smaller than the number of current online users, a device displays a configuration failure message.
- When the configured maximum number of VTY user interfaces is less than the number of current online users, the system disconnects the users that are not authenticated and occupy VTY channels for more than 15s and allows new users to log in to the device through VTY.
- When the configured maximum number of VTY user interfaces exceeds the maximum number of allowed access users, you need to configure the authentication mode for the excess user interfaces.
- The maximum number of login users set by the **user-interface maximum-vty** command is the total number of Telnet and SSH users.
- If the maximum number of login users is set to 0, users are not allowed to log in to the device using Telnet or SSH.
- When the number of login VTY users has reached the maximum, an NMS user can log in using the reserved VTY numbers 16-20. The NMS user is allowed to log in to the device only after passing the AAA local authentication.

Example

Set the maximum number of Telnet users to 7.

```
<HUAWEI> system-view
[HUAWEI] user-interface maximum-vty 7
```

2.5.31 user-interface password complexity-check disable

Function

The **user-interface password complexity-check disable** command disables the password complexity check function.

The **undo user-interface password complexity-check disable** command enables the password complexity check function.

By default, the password complexity check function is enabled.

Format

user-interface password complexity-check disable

undo user-interface password complexity-check disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Passwords configured in the interface view must meet the following complexity requirements:

- A password must contain at least 8 characters. If the minimum length set using the **set password min-length** command exceeds 8 characters, the command configuration takes effect.
- A password must contain at least two types of characters: uppercase characters, lowercase characters, digits, and special characters, excluding question marks (?) and spaces.

To disable the password complexity check function, run the **user-interface password complexity-check disable** command. To enable the password complexity check function, run the **undo user-interface password complexity-check disable** command.

Precautions

If the configured password does not meet complexity requirements, it is prone to attacks and cracks from unauthorized users, which affects device security. Therefore, keeping the password complexity check function enabled is recommended.

Example

Disable the password complexity check function.

```
<HUAWEI> system-view
[HUAWEI] user-interface password complexity-check disable
```

2.5.32 web welcome-message

Function

The **web welcome-message** command configures greetings for the web system.

The **undo web welcome-message** command cancels the configuration of greetings for the web system.

By defaults, greetings are not configured for the web system.

Format

web welcome-message *message*

undo web welcome-message

Parameters

Parameter	Description	Value
message	Configures greetings for the web system.	The value is a string of 1 to 242 case-sensitive characters without question mark (?). Spaces are supported.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run the **web welcome-message** command to configure greetings for the web system. After the **undo web welcome-message** command is run, no greetings will be displayed on the web system.

Example

Configure greetings of the web system to **huawei**.

```
<HUAWEI> system-view
[HUAWEI] web welcome-message huawei
```

2.6 User Login Configuration Commands

2.6.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

2.6.2 configuration exclusive

Function

The **configuration exclusive** command locks the current system configuration. When the system configuration is locked, the user who locks it can query and modify the configuration while other users can only query the configuration.

The **undo configuration exclusive** command unlocks the system configuration.

By default, the system configuration is unlocked.

Format

configuration exclusive

undo configuration exclusive

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device allows several users to log in concurrently to perform manual configurations, which may cause configuration conflicts and service exceptions. To prevent service exceptions, run the **configuration exclusive** command to lock and modify the configuration. Other users can then only query the configuration.

To unlock the configuration, do either of the following:

- Run the **undo configuration exclusive** command.
- Do not modify the configuration in the configured lock interval. The system then automatically unlocks the configuration. To configure the lock interval, run the **configuration-occupied timeout** command.

Precautions

- After you run the **configuration exclusive** command, other users cannot modify the system configuration, so confirm your action before running this command.
- Before you run the **configuration exclusive** command, run the **configuration-occupied timeout** command to configure the maximum lock interval so that the system can automatically unlock the configuration after this interval.

Example

Lock the current system configuration.

```
<HUAWEI> configuration exclusive
```

Unlock the system configuration.

```
<HUAWEI> undo configuration exclusive
```


2.6.3 configuration-occupied timeout

Function

The **configuration-occupied timeout** command sets the interval after which the system automatically unlocks the configuration.

The **undo configuration-occupied timeout** command restores the default automatic unlock interval.

By default, the value is 30 seconds.

Format

configuration-occupied timeout *timeout-value*

undo configuration-occupied timeout

Parameters

Parameter	Description	Value
timeout-value	Specifies the interval after which the system automatically unlocks the configuration if no configuration command is run.	The value is an integer that ranges from 1 to 7200, in seconds. By default, the value is 30 seconds.

Views

System view

Default Level

3: Management level

Usage Guidelines

The **configuration-occupied timeout** command configures the longest lock interval. If no configuration command is delivered within this interval, the system automatically unlocks the configuration so that other users can modify the configuration.

The usage scenarios for this command are as follows:

- If the user does not have the configuration right, the system displays an error.
- If the configuration is locked by another user, the system displays a message indicating that the modification fails.
- If the configuration is locked by the user who configures the longest lock interval, the modification is valid.

NOTE

Note the following when running the **configuration-occupied timeout** command:

- The interval cannot be too short because the device will automatically unlock the configuration if no configuration command is delivered by the user who configures the interval.
- The interval cannot be too long because other users cannot modify the configuration within this period even if the user who locks the configuration delivers no configuration command within this period.
- The command is valid for all users.

Example

Set the automatic unlock interval to 120 seconds.

```
<HUAWEI> system-view
[HUAWEI] configuration-occupied timeout 120
```

2.6.4 console0 disable

Function

The **console0 disable** command disables the console port login function.

The **undo console0 disable** command enables the console port login function.

By default, the console port login function is enabled.

Format

console0 disable

undo console0 disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Application Scenario

By default, the administrator can log in to a switch through the console port. If the console port login function is not required, you can run the **console0 disable** command to disable this function. If this function is required, you can run the **undo console0 disable** command to enable this function.

Precautions

After the **console0 disable** command is run, this command does not take effect for users who have logged in to the device through the console port and takes effect for the users only after they exit from the console port using the **quit** command.

For devices that have the PNP button, you can press and hold the PNP button to enable the function of logging in through the console port.

Example

Disable the console port login function.

```
<HUAWEI> system-view
[HUAWEI] console0 disable
```

2.6.5 display configuration-occupied user

Function

The **display configuration-occupied user** command displays information about the user who locks the configuration.

Format

display configuration-occupied user

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

You can run the **display configuration-occupied user** command to query the user who has the configuration right. If no user locks the system configuration, the system displays a corresponding message.

Example

Display the user who locks the configuration.

```
<HUAWEI> display configuration-occupied user
User Index: 34
User Session Name: VTY0
User Name:**
IP Address: 10.135.19.22
Locked Time: 2012-09-16 15:26:32+10:00 DST
Last Configuration Time: 2012-09-16 15:26:32+10:00 DST
The time out value of configuration right locked is: 30 second(s)
```


Table 2-29 Description of the **display configuration-occupied user** command output

Item	Description
User Index	User index.
User Session Name	User session name. The value is CON0 or ranges from VTY0 to VTY14. snmp-agent: session name of an NMS user.
User Name	Name of a login user. • If a login user name is **, the user logs in to a device using a serial port or the password authentication mode. • If the login user name is a community or V3 user name, the user is an NMS user.
IP Address	IP address of the user.
Locked Time	Time when the configuration was locked.
Last Configuration Time	Time when the user delivered the last configuration command.
The time out value of configuration right locked is	Duration for locking the configuration. To configure the duration, run the **configuration-occupied timeout** command.

Display the user who locks the system configuration (when no user locks the system configuration).

```
<HUAWEI> display configuration-occupied user
Info: No user locked the current configuration.
```

2.6.6 display dsa local-key-pair public

Function

The **display dsa local-key-pair public** command displays the public key in the local DSA key pair of the device.

Format

display dsa local-key-pair public

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

This command displays the public key in the local DSA key pair. You can copy the public key in the command output to the DSA public key of the SSH server to ensure that the public keys on the client and server are consistent and that the client can be authenticated by the server.

Example

Display the public key in the client DSA key pair.

```
<HUAWEI> display dsa local-key-pair public
=================================================
Time of Key pair created:2014-08-27 06:35:16+08:00
Key name    : HUAWEI_Host_DSA
Key modulus : 2048
Key type    : DSA encryption Key
Key fingerprint: b5:82:31:f1:65:0f:97:81:dc:27:95:a8:f8:26:68:c4
=================================================
Key code:
3081DC
  0240
    AE0AE467 2BF3587F 30FE81FF A14D8070 1FC2930B
    A34004C1 B37824BB D3160595 702901CD 53F0EAE0
    6CC46D2D BE78F6A4 3DC4AAEF C7228E01 9C2EF7CE
    87C63485
  0214
    94FC5624 DCEB09DA E9B88293 2AC88508 AB7C813F
  0240
    91FF0F2C 91996828 BAAD5068 CD2FE83E CEFA1CF4
    7BCA4251 9F04FD24 6CFB50A3 AD78CC0D 335DEFD2
    0B4C3530 DAA25592 DEAFA0EB 61225712 E4AF6139
    C986329F
  0240
    26D21FBE 18A9FCB3 C19A7430 A801D8A1 09CFC6E6
    ACB104F4 B398B3B7 83A059EA BE23AE04 5D7AD134
    4279637B 51AD9ADF 80B627EA 9328C95F 3DFF00EE
    84847039

 Host public key for PEM format code:
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1kc3MAAABBAK4K5Gcr81h/MP6B/6FNgHAfwpMLo0AEwbN4JLvTFgWV
cCkBzVPw6uBsxG0tvnj2pD3Equ/HIo4BnC73zofGNIUAAAAVAJT8ViTc6wna6biC
kyrIhQirfIE/AAAAQQCR/w8skZloKLqtUGjNL+g+zvoc9HvKQlGfBP0kbPtQo614
zA0zXe/SC0w1MNqiVZLer6DrYSJXEuSvYTnJhjKfAAAAQCbSH74YqfyzwZp0MKgB
2KEJz8bmrLEE9LOYs7eDoFnqviOuBF160TRCeWN7Ua2a34C2J+qTKMlfPf8A7oSE
cDk=
---- END SSH2 PUBLIC KEY ----
Public key code for pasting into OpenSSH authorized_keys file :
ssh-dss AAAAB3NzaC1kc3MAAABBAK4K5Gcr81h/MP6B/6FNgHAfwpMLo0AEwbN4JLvTFgWVcCkBzVPw
6uBsxG0tvnj2pD3Equ/HIo4BnC73zofGNIUAAAAVAJT8ViTc6wna6biCkyrIhQirfIE/AAAAQQCR/w8s
```



```
kZloKLqtUGjNL+g+zvoc9HvKQlGfBP0kbPtQo614zA0zXe/SC0w1MNqiVZLer6DrYSJXEuSvYTnJhjKf
AAAAQCbSH74YqfyzwZp0MKgB2KEJz8bmrLEE9LOYs7eDoFnqviOuBF160TRCeWN7Ua2a34C2J+qTKMlf
Pf8A7oSEcDk= dsa-key
```

Table 2-30 Description of the **display dsa local-key-pair public** command output

Item	Description
Time of Key pair created	Time when the public key was created.
Key name	Name of the public key.
Key modulus	Length of the key.
Key type	Type of the public key.
Key fingerprint	Key fingerprint.
Key code	Content of the key.
Host public key for PEM format code	PEM code of the public key.
Public key code for pasting into OpenSSH authorized_keys file	Public key format in the OpenSSH file.

2.6.7 display dsa peer-public-key

Function

The **display dsa peer-public-key** command displays the DSA public key that has been configured.

Format

display dsa peer-public-key [**brief** | **name** *key-name*]

Parameters

Parameter	Description	Value
brief	Displays the brief information.	-
name *key-name*	Displays the DSA public key with the specified name.	The value is a string of 1 to 30 case-insensitive characters without spaces. **NOTE** The string can contain spaces if it is enclosed with double quotation marks (").

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command displays the DSA public key for you to check whether the local and peer public keys are consistent.

Precautions

You must complete the DSA public key configuration before running this command.

Example

Display the DSA public key with the specified name.

```
<HUAWEI> display dsa peer-public-key name amar
=====================================
   Key name: amar
   Encoding type: DER
=====================================
Key Code:
3081DC
  0240
    AE0AE467 2BF3587F 30FE81FF A14D8070 1FC2930B A34004C1 B37824BB D3160595
    702901CD 53F0EAE0 6CC46D2D BE78F6A4 3DC4AAEF C7228E01 9C2EF7CE 87C63485
  0214
    94FC5624 DCEB09DA E9B88293 2AC88508 AB7C813F
  0240
    91FF0F2C 91996828 BAAD5068 CD2FE83E CEFA1CF4 7BCA4251 9F04FD24 6CFB50A3
    AD78CC0D 335DEFD2 0B4C3530 DAA25592 DEAFA0EB 61225712 E4AF6139 C986329F
  0240
    0E7BEFD5 594ECA9C CE574D9D 369BCD0C 19C94725 5FE8666E 73292AD6 908E4E0C
    7F0EA3AF A02F17F7 3A0B1D15 E22420CB B5EC1D2C 8BA77729 276EDEBB 8DA843C7
```

Table 2-31 Description of the **display dsa peer-public-key** command output

Item	Description
Key name	Type of the public key.
Encoding type	Type of the public key encoding format.
Key code	Code of the public key.

2.6.8 display ecc local-key-pair public

Function

The **display ecc local-key-pair public** command displays information about the public key in the local Elliptic Curves Cryptography (ECC) key pair.

Format

display ecc local-key-pair public

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **display ecc local-key-pair public** command to check information about the public key in the local ECC key pair on a client and then copy the public key to the server. The public key enables a server to authenticate users and ensures the login of authorized users.

Pre-configuration Tasks

You must run the **ecc local-key-pair create** command to generate a local ECC host key pair before using the command.

Example

Display information about the public key in the local ECC key pair on a client.

```
<HUAWEI> display ecc local-key-pair public
=================================================
Time of Key pair created:2016-10-19 11:50:20+00:00
Key name    : HUAWEI_Host_ECC
Key modulus : 521
Key type    : ECC encryption Key
Key fingerprint:
=================================================
Key code:
   0401CE1E 5EF3B843 CD917648 1D70EF8F CECE8518 5B32ED5F 529E9DC4 D16EDF1A
   5F6E6389 10AAE2D4 74FD9DA7 F05AB123 9AF3EE64 9F0BAF99 A0CBF55B E319B2D1
   8EDEBB01 7C63469B C62A2256 3EAEA0BD 486F9524 8559C7EF 24D969D1 11093BBF
   27F770E7 03E28ABA BB357E5B 28EF04CC EA931C81 C7D7EBD8 5797B1CD 05D9B497
   56D91126 E9

 Host public key for PEM format code:
---- BEGIN SSH2 PUBLIC KEY ----
```



```
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACFBAHOHl7zuEPN
kXZIHXDvj87OhRhbMu1fUp6dxNFu3xpfbmOJEKri1HT9nafwWrEjmvPuZJ8Lr5mg
y/Vb4xmy0Y7euwF8Y0abxioiVj6uoL1Ib5UkhVnH7yTZadERCTu/J/dw5wPiirq7
NX5bKO8EzOqTHIHH1+vYV5exzQXZtJdW2REm6Q==
---- END SSH2 PUBLIC KEY ----

Public key code for pasting into OpenSSH authorized_keys file :
ecdsa-sha2-nistp521 AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACFBAHOHl7z
uEPNkXZIHXDvj87OhRhbMu1fUp6dxNFu3xpfbmOJEKri1HT9nafwWrEjmvPuZJ8Lr5mgy/Vb4xmy0Y7e
uwF8Y0abxioiVj6uoL1Ib5UkhVnH7yTZadERCTu/J/dw5wPiirq7NX5bKO8EzOqTHIHH1+vYV5exzQXZ
tJdW2REm6Q== ecdsa-key
```

Table 2-32 Description of the **display ecc local-key-pair public** command output

Item	Description
Time of Key pair created	Time when the public key in the local ECC key pair is generated, in the format of YYYY-MM-DD HH:MM:SS±HH:MM.
Key Name	Name of the public key in the local ECC key pair.
Key modulus	Length of the public key in the local ECC key pair on a client.
Key Type	Type of the public key in the local ECC key pair. "ECC encryption Key" indicates an ECC public key.
Key Code	Code of the public key in the local ECC key pair configured using the **ecc local-key-pair create** command.
Host public key for PEM format code	PEM code of the public key in the local ECC key pair on a client.
Public key code for pasting into OpenSSH authorized_keys file	Public key in the local ECC key pair on a client that is used for OpenSSH authorization. This information can be used after being copied to the OpenSSH authorized_keys file.

2.6.9 display ecc peer-public-key

Function

The **display ecc peer-public-key** command displays information about the Elliptic Curves Cryptography (ECC) public key configured on the remote end.

Format

display ecc peer-public-key [**brief** | **name** *key-name*]

Parameters

Parameter	Description	Value
brief	Displays the brief information about the ECC public key configured on the remote end.	-
name *key-name*	Displays information about an ECC public key with a specified name configured on the remote end.	The value is a string of 1 to 30 case-sensitive characters, spaces not supported.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **display ecc peer-public-key** command on a client to check information about the public key configured on the remote end. The public key enables a server to authenticate users and ensures the login of authorized users.

Example

Display the information about the ECC public keys of 127.0.0.1.

```
<HUAWEI> display ecc peer-public-key
====================================
   Key name: 127.0.0.1
   Encoding type: DER
====================================
Key Code:
   04013184 A3311697 89DF558B 7F67BF9D BD95DBD5 280D659F 0E29852C AEC2FFBA
   1913AC2A 88247ADA 46BEBEBE 1829C0DA 3BABC8FC 8F6EAD28 2AE2C6A8 116BAA3A
   540E6B00 34E033D8 9D84841B 0D33DAD8 DEDD1C09 2B70B3DB 5AF0FCB2 37DF1C82
   C4C622A6 85B23698 195DA60F 06858ADB DD743937 B4A29C4C FB28B40B BCEEE036
   1DE61BD2 24
```

Display the brief information about all the ECC public keys.

```
<HUAWEI> display ecc peer-public-key brief
  Bits   Name
-----------------------
  521   127.0.0.1
  384   192.168.131.203
```


Table 2-33 Description of the **display ecc peer-public-key** command output

Item	Description
Bits	Length of the ECC public key configured on the remote end.
Name	Name of the ECC public key configured on the remote end.
Key name	Name of the ECC public key configured on the remote end.
Encoding type	Encoding type of the ECC public key configured on the remote end. • OPENSSH If OpenSSH is specified, data is Base64 encoded. OpenSSH is derived from PEM. • PEM If PEM is specified, data is Base64 encoded. • DER If DER is specified, data is Base16 encoded.
Key Code	Code of the public key in the local ECC key pair configured using the **ecc local-key-pair create** command.

2.6.10 display http server

Function

The **display http server** command displays information about the current HTTPS server.

Format

display http server

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can view the HTTPS server information, including the status of HTTPS services, port number, maximum number of users allowed to access the HTTPS server, and number of current online users.

Example

Display information about the current HTTPS server.

```
<HUAWEI> display http server
  HTTP Server Status              : enabled
  HTTP Server Port                : 80(80)
  HTTP Timeout Interval           : 20
  Current Online Users            : 3
  Maximum Users Allowed           : 5
  HTTP Secure-server Status       : enabled
  HTTP Secure-server Port         : 443(443)
  HTTP SSL Policy                 : ssl_server
  HTTP IPv6 Server Status         : disabled
  HTTP IPv6 Server Port           : 80(80)
  HTTP IPv6 Secure-server Status  : disabled
  HTTP IPv6 Secure-server Port    : 443(443)
  HTTP server source interface    : MEth0/0/1
```

Table 2-34 Description of the display http server command output

Item	Description
HTTP Server Status	Status of the HTTP IPv4 server. • Enabled: The HTTP IPv4 service is enabled. • Disabled: The HTTP IPv4 service is disabled. You can configure the HTTP IPv4 server status by running the **http server enable** command.
HTTP Server Port	Port number of the HTTP IPv4 server. The default value is 80. You can configure the port number of the HTTP IPv4 server by running the **http server port** command.
HTTP Timeout Interval	Timeout period of the HTTP/HTTPS server. The default value is 20 minutes. You can configure the timeout period of the HTTP/HTTPS server by running the **http timeout** command.
Current Online Users	Number of current online users.

Item	Description
Maximum Users Allowed	Maximum number of users allowed to access the HTTP server.
HTTP Secure-server Status	Status of the HTTPS IPv4 server. ● Enabled: The HTTPS IPv4 service is enabled. ● Disabled: The HTTPS IPv4 service is disabled. You can configure the HTTPS IPv4 server status by running the **http secure-server enable** command.
HTTP Secure-server Port	Port number of the HTTPS IPv4 server. The default value is 443. You can configure the port number of the HTTPS IPv4 server by running the **http secure-server port** command.
HTTP SSL Policy	HTTPS SSL policy. You can configure the HTTPS SSL policy by running the **ssl policy** command.
HTTP IPv6 Server Status	Status of the HTTP IPv6 server function: ● **enabled**: The HTTP IPv6 server function is enabled. ● **disabled**: The HTTP IPv6 server function is disabled. You can configure the HTTP IPv6 server status by running the **http ipv6 server enable** command.
HTTP IPv6 Server Port	Port number of the HTTP IPv6 server. The default value is 80. You can configure the port number of the HTTPS IPv6 server by running the **http ipv6 server port** command.
HTTP IPv6 Secure-server Status	Status of the HTTPS IPv6 server function: ● **enabled**: The secure HTTPS IPv6 server function is enabled. ● **disabled**: The secure HTTPS IPv6 server function is disabled. You can configure the HTTPS IPv6 server status by running the **http ipv6 secure-server enable** command.

Item	Description
HTTP IPv6 Secure-server Port	Port number of the HTTPS IPv6 server. The default value is 443. You can configure the port number of the HTTPS IPv6 server by running the **http ipv6 secure-server port** command.
HTTP server source interface	The source interface of the HTTPS server. You can configure the source interface of the HTTPS server by running the **http server-source** command.

2.6.11 display http user

Function

The **display http user** command displays information about current online users.

Format

display http user [**username** *username*]

Parameters

Parameter	Description	Value
username *username*	Specifies the name of the current online user.	The value is a string of 1 to 64 case-insensitive characters, with no space or wildcard. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

3: Management level

Usage Guidelines

If **username** is not specified, this command displays summary information about all online users.

If **username** is specified, this command displays detailed information about the specified online user.

Example

Display general information about the current online user.

```
<HUAWEI> display http user
Total online users: 1
-------------------------------------------------------
User name    IP Address          Login Date
-------------------------------------------------------
admin        192.168.0.1         2012-03-23 15:30:55+00:00
```

Display detailed information about the current online user **admin**.

```
<HUAWEI> display http user username admin
Client IP Address: 192.168.0.1
Login Date: 2012-03-19 15:30:55+00:00
User timeouts: 15 minute
```

Table 2-35 Description of the display http user command output

Item	Description
User name	User name.
Client IP Address	IP address of the HTTP client.
Login Date	Login date and time.
User timeouts	Idle timeout duration of online users.

2.6.12 display rsa local-key-pair public

Function

The **display rsa local-key-pair public** command displays the public key in the local key pair.

Format

display rsa local-key-pair public

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command on the client and configure the client public key in the command output to the SSH server, which ensures that the SSH client validity check by the SSH server is successful and enables the secure data exchange between the SSH server and client.

Example

Display the public key in the local key pair.

```
<HUAWEI> display rsa local-key-pair public
=====================================================

Time of Key pair created: 2012-08-15 06:41:55+08:00
Key name: HUAWEI_Host
Key type: RSA encryption Key
Key fingerprint: ab:ec:d7:e1:22:5f:e4:e3:6e:f0:d6:1f:99:e4:f2:f3
=====================================================

Key code:
3047
  0240
    D8D10BE8 CD41AA43 862B6C2B 637D1A53
1EBB4015
    96A70B13 72B17A16 84E02168 4061A4C2
A1CDB541
    484F71DB D7271E5F E3C75BEA AF853023
0CDCE55D
    ECCB0461
  0203
    010001

 Host public key for PEM format code:
---- BEGIN SSH2 PUBLIC KEY ----
AAAAB3NzaC1yc2EAAAADAQABAAAAQQDY0QvozUGqQ4YrbCtjfRpTHrtAFZanCxNy

sXoWhOAhaEBhpMKhzbVBSE9x29cnHl/
jx1vqr4UwIwzc5V3sywRh
---- END SSH2 PUBLIC KEY ----

Public key code for pasting into OpenSSH authorized_keys
file :
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAQQDY0QvozUGqQ4YrbCtjfRpTHrtAFZanCxNysXoWhOAhaEBhpMKhzb
VBSE9x29cnHl/jx1vqr4UwIwzc5V3sywRh rsa-key


=====================================================

Time of Key pair created: 2012-08-15 06:42:03+08:00
Key name: HUAWEI_Server
Key type: RSA encryption Key
Key fingerprint: 16:3b:43:4f:74:16:98:b3:5c:51:b5:a3:83:f8:86:19
=====================================================

Key code:
3067
  0260
    F31D5536 26C05536 6703885D E8FCDB00
07C45437
    B3D08086 9E25B7B6 CFE375B2 1AA957EE
24D2DC51
    BAA81ECD 6894F71E 20596754 35653808
C8B74ACB
    DE94C584 1E234FED 840900F0 4A4100FB
C133DFB7
```



```
  12D4B4DB EF0C3E1F E211202A
F45DD5DD
 0203
  010001
```

Table 2-36 Description of the **display rsa local-key-pair public** command output

Item	Description
Time of Key pair created	Time and date when the public key was created.
Key Name	The value can be the host or server public key. The server public key is saved only when the key type is RSA.
Key Type	Type of the public key.
Key fingerprint	Public key fingerprint.
Key Code	Code of the public key.

2.6.13 display rsa peer-public-key

Function

The **display rsa peer-public-key** command displays the peer public key saved on the local host. If no parameter is specified, the command displays detailed information about all peer public keys.

Format

display rsa peer-public-key [**brief** | **name** *key-name*]

Parameters

Parameter	Description	Value
brief	Displays the brief information about all peer public keys.	-
name *key-name*	Specifies the key name.	The value is a string of 1 to 30 case-insensitive characters without spaces. **NOTE** The string can contain spaces if it is enclosed with double quotation marks (").

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to check detailed information about the RSA public key and whether the local and peer public keys are the same.

Precautions

You must complete the RSA public key configuration before running this command.

Example

Display the brief information about all RSA public keys.

```
<HUAWEI> display rsa peer-public-key brief
Address         Bits   Name
----------------------------
                768    rsakey001
```

Table 2-37 Description of the **display rsa peer-public-key brief** command output

Item	Description
Address	Brief information about the public key.
Bits	Bits in the public key.
Name	Name of the public key.

Display the detailed information about the RSA public key named **rsakey001**.

```
<HUAWEI> display rsa peer-public-key name rsakey001
=====================================
  Key name: rsakey001
  Key address:
=====================================
Key Code:
3067
 0260
  A3158E6C F252C039 135FFC45 F1E4BA9B 4AED2D88 D99B2463 3E42E13A 92A95A37
  45CDF037 1AF1A910 AAE3601C 2EB70589 91AF1BB5 BD66E31A A9150911 859CAB0E
  1E10548C D70D000C 55A1A217 F4EA2F06 E44BD438 DA472F14 3FB7087B 45E77C05
 0203
  010001
```


Table 2-38 Description of the **display rsa peer-public-key name** command output

Item	Description
Key name	Name of the public key.
Key address	Brief information about the public key.
Key Code	Code of the public key.

2.6.14 display ssh server

Function

The **display ssh server** command displays the SSH server information.

Format

display ssh server { **status** | **session** }

Parameters

Parameter	Description	Value
status	Displays the global configuration on the SSH server.	-
session	Displays the current session connection information on the SSH server.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

After configuring the SSH attributes, you can run this command to view the configuration or session connection information on the SSH server to verify that the SSH connection has been established.

Example

Display the global configuration on the SSH server.

```
<HUAWEI> display ssh server status
 SSH version                    :2.0
 SSH connection timeout         :60 seconds
```



```
SSH server key generating interval  :0 hours
SSH authentication retries          :3 times
SFTP IPv4 server                   :Enable
SFTP IPv6 server                   :Enable
STELNET IPv4 server                  :Enable
STELNET IPv6 server                  :Enable
SCP IPv4 server                    :Enable
SCP IPv6 server                    :Enable
SSH server source                   :0.0.0.0
ACL4 number                         :0
ACL6 number                         :0
```

Table 2-39 Description of the **display ssh server status** command output

Item	Description
SSH version	Protocol version used for the SSH session connection.
SSH connection timeout	Timeout interval of SSH server authentication, in seconds. Run the **ssh server timeout** command to set this item.
SSH server key generating interval	Interval for generating an SSH server password, in hours. Run the **ssh server rekey-interval** command to set this item.
SSH authentication retries	Number of times for retrying the SSH session connection. Run the **ssh server authentication-retries** command to set this item.
SFTP IPv4 server	SFTP IPv4 service status. Run the **sftp ipv4 server enable** command to set this item.
SFTP IPv6 server	SFTP IPv6 service status. Run the **sftp ipv6 server enable** command to set this item.
STELNET IPv4 server	STelnet IPv4 service status. Run the **stelnet ipv4 server enable** command to set this item.
STELNET IPv6 server	STelnet IPv6 service status. Run the **stelnet ipv6 server enable** command to set this item.
SCP IPv4 server	SCP IPv4 service status. Run the **scp ipv4 server enable** command to set this item.
SCP IPv6 server	SCP IPv6 service status. Run the **scp ipv6 server enable** command to set this item.

Item	Description
SSH server source	Source address of the SSH server. Run the **ssh server-source** command to set this item.
ACL4 number	ACL4 number of the SSH server. Run the **ssh server acl** *acl-number* command to set this item.
ACL6 number	ACL6 number of the SSH server. Run the **ssh ipv6 server acl** *acl-number* command to set this item.

Display the current session connection information on the SSH server.

```
<HUAWEI> display ssh server session
 Session 1:
     Conn                : VTY 10
     Version             : 2.0
     State               : started
     Username            : client002
     Retry               : 1
     CTOS Cipher         : aes256-cbc
     STOC Cipher         : aes256-cbc
     CTOS Hmac           : hmac-sha2_256
     STOC Hmac           : hmac-sha2_256
     CTOS Compress       : none
     STOC Compress       : none
     Kex                 : diffie-hellman-group1-sha1
     Public Key          : rsa
     Service Type        : sftp
     Authentication Type  : password
 Session 2:
     Conn                : VTY 14
     Version             : 2.0
     State               : started
     Username            : client001
     Retry               : 1
     CTOS Cipher         : aes256-cbc
     STOC Cipher         : aes256-cbc
     CTOS Hmac           : hmac-sha2_256
     STOC Hmac           : hmac-sha2_256
     CTOS Compress       : none
     STOC Compress       : none
     Kex                 : diffie-hellman-group1-sha1
     Public Key          : dsa
     Service Type        : stelnet
     Authentication Type  : password
```

Table 2-40 Description of the **display ssh server session** command output

Item	Description
Session	SSH session ID.
Conn	Connection used by the SSH session.
Version	Protocol version used for the SSH session connection.

Item	Description
State	Status of the SSH session connection.
Username	User name for SSH session connection. Run the **ssh user** command to set this item.
Retry	Number of times for retrying the SSH session connection. Run the **ssh server authentication-retries** command to set this item.
CTOS Cipher	Encryption algorithm name from client to server.
STOC Cipher	Encryption algorithm name from server to client.
CTOS Hmac	HMAC algorithm name from client to server.
STOC Hmac	HMAC algorithm name from server to client.
CTOS Compress	Whether data is compressed for transmission from client to server, which can be specified for SCP connection.
STOC Compress	Whether data is compressed for transmission from server to client, which can be specified for SCP connection.
Kex	Exchange algorithm name.
Public Key	Public key algorithm used for server authentication, which can be RSA, DSA, or ECC.
Service Type	Service type for an SSH user. The options are as follows: ● sftp ● stelnet ● all (including SCP, SFTP and STelnet) Run the **ssh user service-type** command to set this item.

Item	Description
Authentication Type	Authentication mode for an SSH user. The options are as follows: • password • rsa • dsa • ecc • password-rsa (password and RSA) • password-dsa (password and DSA) • password-ecc (password and ECC) • all (password, ECC, DSA, or RSA) Run the **ssh user authentication-type** command to set this item.

2.6.15 display ssh server-info

Function

The **display ssh server-info** command displays the binding between SSH servers and RSA, DSA, or ECC public keys when the current device works as an SSH client.

Format

display ssh server-info

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

When the SSH client needs to authenticate the server, the server public key saved in the local host is used to authenticate the connected SSH server. If the authentication fails, you can run the **display ssh server-info** command to check that the server public key is correct.

Example

Display all bindings between the SSH servers and public keys on the SSH client.

```
<HUAWEI> display ssh server-info
Server Name(IP)              Server Public Key Type  Server public key name
_____________________________________________________________________

192.168.50.207               RSA                192.168.50.207
192.168.50.204               DSA                192.168.50.204
192.168.50.208               ECC                192.168.50.208
```

Table 2-41 Description of the **display ssh server-info** command output

Item	Description
Server Name(IP)	Host name of the SSH server.
Server Public Key Type	Type of the public key on the SSH server.
Server public key name	Name of the public key on the SSH server.

2.6.16 display ssh user-information

Function

The **display ssh user-information** command displays the configuration of all SSH users.

Format

display ssh user-information [*username*]

Parameters

Parameter	Description	Value
username	Displays the SSH user name.	The value is a string of 1 to 64 case-insensitive characters without spaces. **NOTE** The string can contain spaces if it is enclosed with double quotation marks (").

Views

All views

Default Level

3: Management level

Usage Guidelines

This command displays the SSH user name, bound RSA, DSA, or ECC public key name, and service type.

Example

Display the configuration of the SSH user named **client001**.

```
<HUAWEI> display ssh user-information client001
    User Name           : client001
    Authentication-type  : password
    User-public-key-name : -
    User-public-key-type : -
    Sftp-directory       : -
    Service-type         : stelnet
    Authorization-cmd    : No
```

Display the configuration of all SSH users.

```
<HUAWEI> display ssh user-information
 User 1:
    User Name           : client001
    Authentication-type  : password
    User-public-key-name : -
    User-public-key-type : -
    Sftp-directory       : -
    Service-type         : stelnet
    Authorization-cmd    : No
 User 2:
    User Name           : client002
    Authentication-type  : dsa
    User-public-key-name : dsakey001
    User-public-key-type : dsa
    Sftp-directory       : flash:
    Service-type         : sftp
    Authorization-cmd    : No
```

Table 2-42 Description of the **display ssh user-information** command output

Item	Description
User Name	SSH user name. Run the **ssh user** command to set this item.
Authentication-type	Authentication mode for an SSH user. The options are as follows: • password • rsa • dsa • ecc • password-rsa (password and RSA) • password-dsa (password and DSA) • password-ecc (password and ECC) • all (password, ECC, DSA, or RSA) Run the **ssh user authentication-type** command to set this item.
User-public-key-name	Peer RSA, DSA, or ECC public key assigned to an SSH user. Run the **rsa peer-public-key**, **dsa peer-public-key**, or **ecc peer-public-key** command to set this item.

Item	Description
User-public-key-type	The public key type for an SSH user can be RSA, DSA, or ECC.
Sftp-directory	SFTP service directory of an SSH user. Run the **ssh user sftp-directory** command to set this item.
Service-type	Service type for an SSH user. The options are as follows: ● sftp ● stelnet ● all: The service types are SFTP and STelnet. Run the **ssh user service-type** command to set this item.
Authorization-cmd	Command line authentication mode configured for an SSH user. Run the **ssh user authorization-cmd aaa** command to set this item.

2.6.17 display telnet server status

Function

The **display telnet server status** command displays the status and configuration of a Telnet server.

Format

display telnet server status

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

- To check whether a device functions as a Telnet server, run the **display telnet server status** command.

- If you have set a port number for the Telnet server using the **telnet server port** *port-number* command, run **display telnet server status** command to check the port number.

Example

Display the status and configuration of the Telnet server.

```
<HUAWEI> display telnet server status
 TELNET IPv4 server                :Enable
 TELNET IPv6 server                :Enable
 TELNET server port                :23
 TELNET server source address          :0.0.0.0
 ACL4 number                       :0
 ACL6 number                       :0
```

Table 2-43 Description of the **display telnet server status** command output

Item	Description
TELNET IPv4 server	IPv4 Telnet server.
TELNET IPv6 server	IPv6 Telnet server.
TELNET server port	Listening port number of the Telnet server.
TELNET Server Source address	Source address of the Telnet server
ACL4 number	ACL4 number of the Telnet server
ACL6 number	ACL6 number of the Telnet server

2.6.18 display telnet-client

Function

The **display telnet-client** command displays the source parameters when a device works as a Telnet client.

Format

display telnet-client

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

After setting source parameters of a Telnet client, you can run this command to check the setting result. If you have not run the **telnet client-source** command, the default source IP address is 0.0.0.0.

Example

Display the source parameters of the device functioning as a Telnet client.

```
<HUAWEI> display telnet-client
 The source address of telnet client is 10.1.1.1
```

Table 2-44 Description of the **display telnet-client** command output

Item	Description
The source address of telnet client is 10.1.1.1	The source IP address of the Telnet client is 10.1.1.1.

2.6.19 dsa local-key-pair create

Function

The **dsa local-key-pair create** command generates the local DSA host key pairs.

Format

dsa local-key-pair create

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Compared with RSA, Digital Signature Algorithm (DSA) has a wider application in the SSH protocol. The asymmetric encryption system generates public and private keys to implement secure key exchange, thereby ensuring secure sessions.

If a DSA key exists, when you run this command, the system prompts you to confirm whether to change the original key. If you agree, the key in the new key

pair is named ***device name*_Host_DSA**, for example, **HUAWEI_Host_DSA**. The local DSA private key is saved in PKCS#8 format to the hostkey_dsa file in the system NOR FLASH.

After you enter the command, the device prompts you to enter the number of bits in the host key. The length of a host key pair can be 2048. By default, the key length is 2048.

Precautions

This command is not saved in a configuration file and can take effect immediately after being run. After the device restarts, you do not need to run the command again.

To improve security of the device, it is recommended that you use a key pair of 2048 bits.

Example

Generate DSA key pairs on the device.

```
<HUAWEI> system-view
[HUAWEI] dsa local-key-pair create
Info: The key name will be: HUAWEI_Host_DSA.
Info: The key modulus can be any one of the following : 2048.
Info: If the key modulus is greater than 512, it may take a few minutes.
Please input the modulus [default=2048]:
Info: Generating keys...
Info: Succeeded in creating the DSA host keys.
```

2.6.20 dsa local-key-pair destroy

Function

The **dsa local-key-pair destroy** command deletes local DSA host key pairs.

Format

dsa local-key-pair destroy

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

DSA applies to SSH verification. The asymmetric encryption system generates public and private keys to implement secure key exchange, thereby ensuring secure sessions. You can run the **dsa local-key-pair create** command to generate local DSA keys. When local DSA keys are unnecessary, you can run the **dsa local-key-pair destroy** command to delete these keys.

Prerequisite

The local DSA keys have been created.

Configuration Impact

After you run this command, the ****_DSA** file that stores DSA keys on the device is cleared.

Precautions

The **dsa local-key-pair destroy** command takes effect once, and therefore will not be saved in the configuration file.

Example

Delete local DSA keys.

```
<HUAWEI> system-view
[HUAWEI] dsa local-key-pair destroy
Info: The name of the key which will be destroyed is
HUAWEI_Host_DSA.
Warning: These keys will be destroyed. Continue? [Y/N]:y
Info: Succeeded in destroying the DSA host keys.
```

2.6.21 dsa peer-public-key

Function

The **dsa peer-public-key** command configures an encoding format for a DSA public key and displays the DSA public key view.

The **undo dsa peer-public-key** command deletes a DSA public key.

By default, no encoding format is configured for a DSA public key.

Format

dsa peer-public-key *key-name* **encoding-type** { **der** | **openssh** | **pem** }

undo dsa peer-public-key *key-name*

Parameters

Parameter	Description	Value
key-name	Specifies the public key name.	The value is a string of 1 to 30 case-insensitive characters without spaces. **NOTE** The string can contain spaces if it is enclosed with double quotation marks (").
encoding-type	Specifies an encoding format for a DSA public key.	-
der	Specifies the Distinguished Encoding Rules (DER) format for a DSA public key. DER encodes data in hexadecimal format.	-
openssh	Specifies the OpenSSH format for a DSA public key. OpenSSH encodes data in base-64 format. OpenSSH is an encoding format based on PEM.	-
pem	Specifies the Privacy Enhanced Mail (PEM) format for a DSA public key. PEM encodes data in base-64 format.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you use a DSA public key for authentication, you must specify the public key of the corresponding client for an SSH user on the server. When the client logs

in to the server, the server uses the specified public key to authenticate the client. You can also save the public key generated on the server to the client. Then the client can be successfully authenticated by the server when it logs in to the server for the first time.

Huawei data communications devices support the DER, OpenSSH and PEM formats for DSA keys. If you use a DSA key in non-DER/OpenSSH/PEM format, use a third-party tool to convert the key into a key in DER, OpenSSH or PEM format.

Because a third-party tool is not released with Huawei system software, DSA usability is unsatisfactory. In addition to DER and PEM, DSA keys need to support the OpenSSH format to improve DSA usability.

Third-party software, such as PuTTY, OpenSSH, and OpenSSL, can be used to generate DSA keys in different formats. The details are as follows:

- The PuTTY generate DSA keys in PEM format.
- The OpenSSH generates DSA keys in OpenSSH format.
- The OpenSSL generates DSA keys in DER format.

OpenSSL is an open source software. You can download related documents at the OpenSSL official website.

After you configure an encoding format for a DSA public key, Huawei data communications device automatically generates a DSA public key in the configured encoding format and enters the DSA public key view. Then, you can run the **public-key-code begin** command and manually copy the DSA public key generated on the peer device to the local device.

Follow-up Procedure

After you copy the DSA public key generated on the peer device to the local device, perform the following operations to exit the DSA public key view:

1. Run the **public-key-code end** command to return to the DSA public key view.
2. Run the **peer-public-key end** command to exit the DSA public key view and return to the system view.

Precautions

When you run the **undo dsa peer-public-key** command to delete a DSA public key:

- If the public key has been assigned to an SSH client, run the **undo ssh user** *user-name* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } command to release the binding between the public key and the SSH client. If you do not release the binding between them, the **undo dsa peer-public-key** command will fail to delete the public key.
- If the name of the host public key of the SSH server to be connected is specified on the SSH client, you need to run the **undo ssh client** *servername* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } command to delete the host public key of the SSH server. Otherwise, the DSA public key cannot be deleted.

The peer public key supports only PKCS#1. Other PKCS versions are not supported.

Example

Configure an encoding format for a DSA public key and enter the DSA public key view.

```
<HUAWEI> system-view
[HUAWEI] dsa peer-public-key 23 encoding-type der
[HUAWEI-dsa-public-key]
```

2.6.22 ecc local-key-pair create

Function

The **ecc local-key-pair create** command generates a local Elliptic Curves Cryptography (ECC) host key pair.

Format

ecc local-key-pair create

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A local key pair is a prerequisite to a successful SSH login. Compared with the RSA algorithm used by the **rsa local-key-pair create** command, the ECC algorithm shortens the key length, accelerates the encryption, and improves the security. The length of the server key pair and the host key pair can be 256 bits, 384 bits and 521 bits. By default, the length of the key pair is 521 bits.

Precautions

- The generated ECC host key pair is named in the format of switch name_Host_ECC, such as HUAWEI_Host_ECC. The local DSA private key is saved in PKCS#8 format to the hostkey_ecc file in the system NOR FLASH.
- The **ecc local-key-pair create** and **ecc local-key-pair destroy** commands are not saved in the configuration file. They only need to be run once and take effect even after the switch restarts.
- Do not delete the ECC key file from the switch. If the ECC key file is deleted, the ECC key pair cannot be restored after the switch is restarted.

Example

Generate a local ECC host key pair.

```
<HUAWEI> system-view
[HUAWEI] ecc local-key-pair create
Info: The key name will be: HUAWEI_Host_ECC.
Info: The ECC host key named HUAWEI_Host_ECC already exists.
Warning: Do you want to replace it ? [Y/N]: Y
Info: The key modulus can be any one of the following : 256, 384, 521.
Info: If the key modulus is greater than 512, it may take a few minutes.
Please input the modulus [default=521]:521
Info: Generating keys...
Info: Succeeded in creating the ECC host keys.
```

Enter a key with incorrect length and re-enter the key with incorrect length for five times, which is the maximum number of retry attempts.

```
<HUAWEI> system-view
[HUAWEI] ecc local-key-pair create
Info: The key name will be: HUAWEI_Host_ECC.
Info: The ECC host key named HUAWEI_Host_ECC already exists.
Warning: Do you want to replace it ?[Y/N]: Y
Info: The key modulus can be any one of the following : 256, 384, 521.
Info: If the key modulus is greater than 512, it may take a few minutes.
Please input the modulus [default=521]:123
Error: Invalid ECC key modulus.
Please input the modulus [default=521]:1024
Error: Invalid ECC key modulus.
Please input the modulus [default=521]:512
Error: Invalid ECC key modulus.
Please input the modulus [default=521]:2048
Error: Invalid ECC key modulus.
Please input the modulus [default=521]:4096
Error: Invalid ECC key modulus.
Error: The maximum number of retries has reached, and the command has already been canceled.
```

2.6.23 ecc local-key-pair destroy

Function

The **ecc local-key-pair destroy** command deletes the local Elliptic Curves Cryptography (ECC) keys.

Format

ecc local-key-pair destroy

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If you no longer need the local ECC key pairs, run the **ecc local-key-pair destroy** command to delete them.

Configuration Impact

After the **ecc local-key-pair destroy** command is run, the ECC key files on the device are cleared. Exercise caution when running the command.

Precautions

- The **ecc local-key-pair create** and **ecc local-key-pair destroy** commands are not saved in the configuration file. They only need to be run once and take effect even after the switch restarts.
- Do not delete the ECC key file from the switch. If the ECC key file is deleted, the ECC key pair cannot be restored after the switch is restarted.

Example

Delete the local ECC host key pair and server key pair.

```
<HUAWEI> system-view
[HUAWEI] ecc local-key-pair destroy
Info: The name of the key which will be destroyed is HUAWEI_Host_ECC.
Warning: These keys will be destroyed. Continue? [Y/N]:Y
Info: Succeeded in destroying the ECC host keys.
```

2.6.24 ecc peer-public-key

Function

The **ecc peer-public-key** command creates an ECC public key and enters the Elliptic Curves Cryptography (ECC) public key view.

The **undo ecc peer-public-key** command deletes an ECC public key.

By default, no ECC public key is created.

Format

ecc peer-public-key *key-name* **encoding-type** { **der** | **pem** | **openssh** }

undo ecc peer-public-key *key-name*

Parameters

Parameter	Description	Value
key-name	Specifies an ECC public key name.	The value is a string of 1 to 30 case-sensitive characters, spaces not supported.

Parameter	Description	Value
encoding-type	Indicates the encoding type of an ECC public key.	-
der	Specifies DER as the encoding type of an ECC public key. If DER is specified, data is encoded in hexadecimal notation.	-
pem	Specifies PEM as the encoding type of an ECC public key. If PEM is specified, data is Base64 encoded.	-
openssh	Specifies OpenSSH as the encoding type of an ECC public key. If OpenSSH is specified, data is Base64 encoded. OpenSSH is derived from PEM.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When ECC public key authentication is used, a client's public key must be specified on the server for an SSH user. When the client logs in to the server, the server performs authentication on the client based on the public key of the SSH user.

After an ECC public key is created and the ECC public key view is displayed, run the **public-key-code begin** command, then you can manually copy the client's public key to the server.

The client's public key is randomly generated by the client software.

Follow-up Procedure

After copying the client's ECC public key to the server, run the following commands to quit the ECC public key view:

1. Run the **public-key-code end** command to return to the ECC public key view.
2. Run the **peer-public-key end** command to exit the ECC public key view and return to the system view.

Precautions

A maximum of 20 ECC public keys can be created.

When you run the **undo ecc peer-public-key** command to delete an ECC public key:

- If the public key has been assigned to an SSH client, run the **undo ssh user** *user-name* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } command to release the binding between the public key and the SSH client. If you do not release the binding between them, the **undo dsa peer-public-key** command will fail to delete the public key.
- If the name of the host public key of the SSH server to be connected is specified on the SSH client, you need to run the **undo ssh client** *servername* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } command to delete the host public key of the SSH server. Otherwise, the DSA public key cannot be deleted.

The peer public key supports only PKCS#1. Other PKCS versions are not supported.

Example

Create an ECC public key and enter the ECC public key view.

```
<HUAWEI> system-view
[HUAWEI] ecc peer-public-key ecc-peer-key encoding-type pem
Info: Enter "ECC public key" view, return system view with "peer-public-key end".
[HUAWEI-ecc-public-key] public-key-code begin
Info: Enter "ECC key code" view, return the last view with "public-key-code end".
[HUAWEI-ecc-key-code] ---- BEGIN SSH2 PUBLIC KEY ----
[HUAWEI-ecc-key-code]
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACDBL5J4v3pqi5S
[HUAWEI-ecc-key-code] ALI9lvLw4cdvtpD2AC6sEJXg9GDCD5vGBnkXlKmnOy6d1TyrXx57ZPNnrSdqVkHC
[HUAWEI-ecc-key-code] sMBa63vSwg1XsVW2qZgx8H57+FJiTPY61b1Vfst9GUif1ymfpB7XrbdYZDownoh0
[HUAWEI-ecc-key-code] FZNadZtIf2CRc0OeiKXbCSPP25dfoT/DTcc=
[HUAWEI-ecc-key-code] ---- END SSH2 PUBLIC KEY ----
[HUAWEI-ecc-key-code] public-key-code end
[HUAWEI-ecc-public-key] peer-public-key end
```

Delete an ECC public key.

```
<HUAWEI> system-view
[HUAWEI] undo ecc peer-public-key ecc-peer-key
Warning: The public key named ecc-peer-key will be deleted. Continue? [Y/N]:Y
```

2.6.25 free http user-id

Function

The **free http user-id** command configures a device to release web users.

Format

free http user-id *user-id*

Parameters

Parameter	Description	Value
user-id	Specifies the VTY ID of a web user to be released. You can run the **display users** command to query the VTY ID.	The value is an integer that ranges from 1 to 256.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A maximum of five web users are supported at present. If one of the five web users is logged out unexpectedly, the user's client keeps connection with the FTP server before the connection expires. During this period, other users cannot log in to the FTP server. To manually release the web user, run the **free http user-id** command.

Precautions

The **free http user-id** command is used only to release web users. **user-id** of web users ranges from 89 to 93, and a maximum of five users are allowed to stay online concurrently. If you set **user-id** to a value smaller than 89 or greater than 93, the message "Error: The specified user does not exist or is not an HTTP user." is displayed.

Example

Release the web user whose VTY ID is 89.

```
<HUAWEI> system-view
[HUAWEI] free http user-id 89
```

2.6.26 http acl

Function

The **http acl** command configures an ACL/ACL6 on the HTTP or HTTPS server.

The **undo http acl** command deletes the ACL/ACL6 on the HTTP or HTTPS server.

By default, no ACL/ACL6 is configured on the HTTP or HTTPS server.

Format

HTTP or HTTPS IPv4:

http acl *acl-number*

undo http acl

HTTP or HTTPS IPv6:

http ipv6 acl *acl6-number*

undo http ipv6 acl

Parameters

Parameter	Description	Value
acl-number	Specifies the ACL number for an HTTP or HTTPS IPv4 server.	The value is an integer that ranges from 2000 to 3999.
acl6-number	Specifies the ACL6 number for an HTTP or HTTPS IPv6 server.	The value is an integer that ranges from 2000 to 3999.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To ensure the security of an HTTP or HTTPS server, you need to configure an ACL/ACL6 for it to specify clients that can log in to the current HTTP or HTTPS server.

Precautions

- The **http acl** command takes effect only after you run the **rule** command to configure the ACL/ACL6 rule.
- After an ACL/ACL6 rule is modified, the HTTP or HTTPS server does not forcibly log out an online user who matches the ACL/ACL6 rule until the user sends the next login request.
- If the **http acl** command is configured several times, only the latest configuration takes effect.

Example

Set the ACL number to 2000 for the HTTP or HTTPS IPv4 server.

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule 1 permit source 10.1.1.1 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] http acl 2000
```

Set the ACL6 number to 2000 for the HTTP or HTTPS IPv6 server.


```
<HUAWEI> system-view
[HUAWEI] acl ipv6 2000
[HUAWEI-acl6-basic-2000] rule 1 permit source fc00:1::1 128
[HUAWEI-acl6-basic-2000] quit
[HUAWEI] http ipv6 acl 2000
```

2.6.27 http secure-server enable

Function

The **http secure-server enable** command enables the HTTPS service function.

The **undo http secure-server enable** command disables the HTTPS service function.

The **http secure-server disable** command disables the HTTPS service function.

By default, the HTTPS IPv4 service function is enabled, and the HTTPS IPv6 service function is disabled.

Format

http [**ipv6**] **secure-server enable**

undo http [**ipv6**] **secure-server enable**

http [**ipv6**] **secure-server disable**

Parameters

Parameter	Description	Value
ipv6	Enables or disables the HTTPS IPv6 service function. If this parameter is not specified, the HTTPS IPv4 service function is enabled or disabled.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After an SSL policy is loaded to an HTTPS server, the HTTPS server provides HTTPS service using SSL. The client and HTTPS server establish an SSL connection to protect user information from theft.

Prerequisites

The web page file has been loaded to the device.

Precautions

- After the HTTPS service is enabled, only authenticated users can use the web browser to access the web network management system to manage devices.
- After the HTTPS service is enabled, the SSL handshake negotiation is triggered.
- After the **http secure-server enable** command is run, the HTTPS server accepts only login requests from MEth0/0/1 or VLANIF1 by default. To allow authorized users to log in to the HTTPS server from other interfaces, you should run the **http server-source** command to specify the source interface of the HTTPS server.
- After the **http ipv6 secure-server enable** command is run, the HTTPS server does not accept login requests from any IPv6 address by default, you should run the **http ipv6 server-source** command to specify the IPv6 source address for the HTTPS server.

Example

Enable the HTTPS IPv4 service.

```
<HUAWEI> system-view
[HUAWEI] http secure-server enable
```

Enable the HTTPS IPv6 service.

```
<HUAWEI> system-view
[HUAWEI] http ipv6 secure-server enable
```

2.6.28 http secure-server port

Function

The **http secure-server port** command sets a port number for an HTTPS server.

The **undo http secure-server port** command restores the default port number of an HTTPS server.

By default, the port number of an HTTPS server is 443.

Format

http [**ipv6**] **secure-server port** *port-number*

undo http [**ipv6**] **secure-server port**

Parameters

Parameter	Description	Value
ipv6	Specifies the port number for an HTTPS IPv6 server. If this parameter is not specified, the command sets the port number for an HTTPS IPv4 server.	-

Parameter	Description	Value
port-number	Specifies the port number of an HTTPS server.	The value is 443 or an integer that ranges from 1025 to 55535.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, the port number of an HTTPS server is 443. Attackers may frequently access an HTTPS server through the default port, consuming bandwidth, deteriorating server performance, and causing authorized users unable to access the server. You can run the **http secure-server port** command to specify another port number to prevent attackers from accessing the default port.

Precautions

If the **http secure-server port** command is configured several times, only the latest configuration takes effect.

Example

Set the port number of an HTTPS IPv4 server to 8080.

```
<HUAWEI> system-view
[HUAWEI] http secure-server port 8080
```

Set the port number of an HTTPS IPv6 server to 8080.

```
<HUAWEI> system-view
[HUAWEI] http ipv6 secure-server port 8080
```

2.6.29 http secure-server ssl-policy

Function

The **http secure-server ssl-policy** command configures an SSL policy for the HTTP server.

The **undo http secure-server ssl-policy** command restores the default SSL policy for the HTTP server.

A default SSL policy is available on an HTTP server.

Format

http secure-server ssl-policy *policy-name*

undo http secure-server ssl-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an SSL policy.	The value is a string of 1 to 23 case-insensitive characters without spaces. The value can contain digits, letters, and underscores (_).

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Traditional HTTP service transmits data in plain text, which can be intercepted and tampered with. User identity cannot be authenticated, and the HTTP server cannot ensure online data security of applications such as the e-commerce and online banks. You can run the **http secure-server ssl-policy** command to configure an SSL policy for the HTTP server to encrypt data, authenticate user identity, and check message integrity to ensure data security during the web access.

Prerequisites

Before running the **http secure-server ssl-policy** command, you must first run the **ssl policy** command to create an SSL policy on the HTTP server.

Precautions

- The device provides a default SSL policy named **Default**. After the web page file is loaded to the device, the default SSL policy is loaded automatically, and you do not need to configure an SSL policy. To enhance device security, it is recommended that you obtain a new digital certificate from the CA and manually configure an SSL policy
- Only one SSL policy can be configured for the HTTP server, and the latest configured SSL policy takes effect.

Example

Configure an SSL policy for the HTTP server.

```
<HUAWEI> system-view
[HUAWEI] http secure-server ssl-policy http_server
```


2.6.30 http server enable

Function

The **http server enable** command enables the HTTP server function.

The **undo http server enable** command disables the HTTP server function.

The **http server disable** command disables the HTTP server function.

By default, the HTTP IPv4 server function is enabled, and the HTTP IPv6 server function is disabled.

Format

http [**ipv6**] **server enable**

undo http [**ipv6**] **server enable**

http [**ipv6**] **server disable**

Parameters

Parameter	Description	Value
ipv6	Enables or disables the HTTP IPv6 server function. If this parameter is not specified, the HTTP IPv4 server function is enabled or disabled.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After running the **http server enable** command to enable the HTTP server, you can use the browser to access the web NMS to manage devices.

If the web page to load does not exist, the HTTP service cannot be enabled.

Prerequisites

The HTTPS service has been enabled using the **http secure-server enable** command.

Precautions

- After the **http server enable** command is run, the HTTPS server accepts only login requests from MEth0/0/1 or VLANIF1 by default. To allow authorized

users to log in to the HTTPS server from other interfaces, you should run the **http server-source** command to specify the source interface of the HTTP server.

- After the **http ipv6 server enable** command is run, the HTTP server does not accept login requests from any IPv6 address by default, you should run the **http ipv6 server-source** command to specify the IPv6 source address for the HTTP server.

Example

Enable the HTTP IPv4 server.

```
<HUAWEI> system-view
[HUAWEI] http secure-server enable
[HUAWEI] http server enable
Warning: HTTP is not a secure protocol, and it is recommended to use HTTPS.
Info: Succeeded in starting the HTTP server.
```

Enable the HTTP IPv6 server.

```
<HUAWEI> system-view
[HUAWEI] http ipv6 secure-server enable
[HUAWEI] http ipv6 server enable
Warning: HTTP is not a secure protocol, and it is recommended to use HTTPS.
Info: Succeeded in starting the HTTP IPv6 server.
```

2.6.31 http server load

Function

The **http server load** command loads a web page file.

The **undo http server load** command cancels loading of a specified web page file.

By default, the web page file in the system software has been loaded to the devices.

Format

http server load { *file-name* | **default** }

undo http server load

Parameters

Parameter	Description	Settings
file-name	Specifies the name of the web page file to load. The web page file must be stored in the root directory of the storage device.	The value is a string of 4 to 64 characters without spaces. The file name is in the *.web.7z format.

Parameter	Description	Settings
default	Specifies the web page file in the current system software that is to be loaded.	–

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If you need to manage and maintain devices on the graphical user interface (GUI), configure the Web network management function. When you need to update web page file when using the Web network management function, run this command to load web page file.

Prerequisites

Before loading the web page file using the **http server load** command, ensure that the web page file has been stored to the root directory of the storage device on the device; otherwise, file loading will fail.

Precautions

- If the system software is upgraded from V200R006 or an earlier version to V200R007 or a later version, but the target software version conflicts with the configuration file for next startup, the device will cancel the configuration of loading the web page file in the original system software after the upgrade, and loads the web page file integrated in the new system software by default.
- The web page file contains the SSL certificate, which is used to authenticate the HTTP server during login to ensure information security. When a user attempts to log in to the device through HTTP, the HTTPS login page is pushed to the user. After the user is authenticated, the system returns to the HTTP page. The SSL certificate is also used in the HTTPS login mode to ensure security of user information and data exchanged between the client and server. You can load a new digital certificate to the device.
- If the loaded web page file does not exist, the HTTP service cannot be enabled when the device restarts.
- To disable a loaded web page file, you must load another file.

Example

Load the web page file **web_1.web.7z**.


```
<HUAWEI> system-view
[HUAWEI] http server load web_1.web.7z
```

2.6.32 http server port

Function

The **http server port** command sets the listening port number of the HTTP server.

The **undo http server port** command restores the default listening port number of the HTTP server.

By default, the listening port number of the HTTP server is 80.

Format

http [**ipv6**] **server port** *port-number*

undo http [**ipv6**] **server port**

Parameters

Parameter	Description	Value
ipv6	Specifies a listening port number for an HTTP IPv6 server. If this parameter is not specified, the command configures a listening port number for an HTTP IPv4 server.	-
port-number	Specifies the listening port number of the HTTP server.	The value is 80, or an integer that ranges from 1025 to 55535. The default value is 80.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, the listening port number of the security HTTP server is 80. Attackers may frequently access the default listening port, which wastes bandwidth, deteriorates server performance, and prevents authorized users from accessing the HTTP server through the listening port. You can run the **http server port** command to specify another listening port number to prevent attackers from accessing the listening port.

Precautions

If the **http server port** command is configured several times, only the latest configuration takes effect.

Example

Set the listening port number of the HTTP IPv4 server to 1025.

```
<HUAWEI> system-view
[HUAWEI] http server port 1025
```

Set the listening port number of the HTTP IPv6 server to 1500.

```
<HUAWEI> system-view
[HUAWEI] http ipv6 server port 1500
```

2.6.33 http server-source

Function

The **http server-source** command specifies a source interface for an HTTP or HTTPS server.

The **undo http server-source** command cancels the source interface specified for an HTTP or HTTPS server.

By default, the source interface of an HTTP or HTTPS server is MEth0/0/1 or VLANIF 1. The web login is supported after the device enters the initial configuration mode. The source interface of an HTTP or HTTPS server is MEth0/0/1 or VLANIF 1..

Format

http server-source -i *interface-type interface-number*

undo http server-source

http server-source all-interface

Parameters

Parameter	Description	Value
-i *interface-type interface-number*	Specifies the source interface of an HTTP or HTTPS server.	-
all-interface	Indicates that any interface that has an IPv4 address configured can be used as the source interface of an HTTP or HTTPS server.	-

NOTE

In V200R020C00 and later versions, to allow authorized users to log in to the HTTP server through a non-management network port, run a command to specify the source interface of the HTTP server. For details about the command, see "Usage Scenario" in "Usage Guidelines" in this section.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In versions earlier than V200R020C00, an HTTP or HTTPS server receives connection requests from all interfaces by default, incurring security risks. For details, see the product documentation of the corresponding version.

In V200R020C00 and later versions, an HTTP or HTTPS server accepts only login requests from MEth0/0/1 or VLANIF1 by default. To allow authorized users to log in to the HTTP or HTTPS server, run either of the following commands to specify the source interface of the HTTP or HTTPS server.

- Run the **http server-source -i** *interface-type interface-number* command to configure a specified interface as the source interface of the HTTP or HTTPS server.
- Run the **http server-source all-interface** command to configure all interfaces configured with IPv4 addresses as the source interfaces of the HTTP or HTTPS server.

Prerequisites

Before you specify a logical interface as the source interface, ensure that the interface to be specified is created and has an IP address configured. Before you specify a physical interface as the source interface, ensure that the interface has an IPv4 address configured. Otherwise, the **http server-source** command cannot be successfully executed.

Configuration Impact

Users can log in to an HTTP or HTTPS server only from the specified source interface.

After you run **http server-source** command, the HTTP IPv4 user that has logged in to the server will be forcibly logged out and needs to log in again.

Precautions

After the source interface of an HTTP or HTTPS server is specified using the **http server-source** command, ensure that HTTP or HTTPS users can access the source interface at Layer 3. Otherwise, the HTTP or HTTPS users will fail to log in to the HTTP or HTTPS server.

After the **http server-source all-interface** command is run, the system allows HTTP or HTTPS users to log in to the HTTP or HTTPS server through all interfaces with IPv4 addresses configured. This increases system security risks. Therefore, you are not advised to run this command.

Example

Specify loopback 0 as the source interface of an HTTP or HTTPS server.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 0
[HUAWEI-LoopBack0] quit
[HUAWEI] http server-source -i loopback 0
Warning: The operation will reboot the HTTP server. Continue? [Y/N]:y
Info: Succeeded in setting the source interface of the HTTP server to
LoopBack0.
Info: Succeeded in starting the HTTP secure server.
Warning: HTTP is not a secure protocol, and it is recommended to use
HTTPS.
Info: Succeeded in starting the HTTP server.
```

2.6.34 http ipv6 server-source

Function

The **http ipv6 server-source** command specifies an IPv6 source address for an HTTP or HTTPS server.

The **undo http ipv6 server-source** command cancels the IPv6 source address specified for an HTTP or HTTPS server.

By default, the IPv6 source address of an HTTP or HTTPS server is not specified.

Format

http ipv6 server-source -a *ipv6_address* [**-vpn-instance** *vpn_name*]

undo http ipv6 server-source

http ipv6 server-source all-interface

Parameters

Parameter	Description	Value
-a *ipv6_address*	Specifies the IPv6 source address for an HTTP or HTTPS server.	The total length of an IPv6 address is 128 bits, which are divided into eight groups. Each group contains four hexadecimal digits. The value is in the format X:X:X:X:X:X:X:X.

Parameter	Description	Value
-vpn-instance *vpn_name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain spaces. The VPN instance name cannot be **_public_**. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
all-interface	Indicates that any interface IPv6 address on the device can be used as the IPv6 source address of the HTTP or HTTPS server.	-

NOTE

In V200R020C00 and later versions, to allow authorized users to log in to the HTTP server through a non-management network port, run a command to specify the source interface of the HTTP server. For details about the command, see "Usage Scenario" in "Usage Guidelines" in this section.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In versions earlier than V200R020C00, an HTTP or HTTPS server receives connection requests from all interfaces by default, incurring security risks. For details, see the product documentation of the corresponding version.

In V200R020C00 and later versions, an HTTP or HTTPS server does not accept login requests from any interface by default. To allow authorized users to log in to the HTTP or HTTPS server, run either of the following commands to specify the source interface of the HTTP or HTTPS server.

- Run the **http ipv6 server-source -a** *ipv6_address* [**-vpn-instance** *vpn_name*] command to configure the specified IPv6 address as the IPv6 source address of the HTTP or HTTPS server.
- Run the **http ipv6 server-source all-interface** command to configure all interface IPv6 addresses on the device as the IPv6 source addresses of the HTTP or HTTPS server.

Prerequisites

A VPN instance has been created before you specify it for an HTTP or HTTPS server. Otherwise, the **http ipv6 server-source** command cannot be executed.

Configuration Impact

After an IPv6 source address is specified for an HTTP or HTTPS server, HTTP or HTTPS users can log in to the HTTP or HTTPS server only using this IPv6 address. This configuration applies to the HTTP or HTTPS users who attempt to log in to the server, not to the HTTP or HTTPS users who have logged in to the server.

Precautions

After an IPv6 source address is specified for an HTTP or HTTPS server using this command, ensure that HTTP or HTTPS users can access this IPv6 address at Layer 3. Otherwise, HTTP or HTTPS users will fail to log in to the HTTP or HTTPS server.

If the specified IPv6 source address is bound to a VPN instance, the HTTP or HTTPS server is also bound to the VPN instance.

After the **http ipv6 server-source all-interface** command is run, the system allows HTTP or HTTPS users to log in to the HTTP or HTTPS server through all interfaces with IPv6 addresses configured. This increases system security risks. Therefore, running this command is not recommended.

Example

Specify the IPv6 source address 2001:DB8:: for an HTTP or HTTPS server.

```
<HUAWEI> system-view
[HUAWEI] http ipv6 server-source -a 2001:DB8::
```

2.6.35 http timeout

Function

The **http timeout** command sets the idle timeout duration of the web server.

The **undo http timeout** command restores the default idle timeout duration of the web server.

By default, the idle timeout duration of the web server is 20 minutes.

Format

http timeout *timeout*

undo http timeout

Parameters

Parameter	Description	Value
timeout	Specifies the idle timeout duration of the web server for online users.	The value is an integer that ranges from 1 to 60, in minutes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A maximum of five web users are supported at present. When the fifth web user logs in to the web server, any other user cannot log in to the web server even if any of the five users does not perform operations for a long time. The idle timeout duration is configured to release web resources in time. To occupy web channels for a long time, you must set the idle timeout duration to the maximum value.

Precautions

- After you run the **http timeout** command, the idle timeout durations are the same for all web users who log in to the web server. If the idle timeout duration expires, a user is disconnected from the web server and the web server notifies the user only after the user sends the next login request.
- If the **http timeout** command is configured several times, only the latest configuration takes effect.

Example

Set the idle timeout duration of the web server to 6 minutes.

```
<HUAWEI> system-view
[HUAWEI] http timeout 6
```

2.6.36 lock

Function

The **lock** command locks the current user interface to prevent unauthorized users from operating the interface.

By default, the system does not automatically lock the current user interface.

Format

lock

Parameters

None

Views

User view

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

Lock the current user interface using this command to prevent other users from operating the interface. The user interface can be console or VTY.

After running the **lock** command, you are prompted to enter a password twice. If you enter the correct password twice, the user interface is locked.

Precautions

- The passwords must meet the following requirements:
  - The password must be a string of 8 to 16 case-sensitive characters.
  - The password must contain at least two types of the following characters: upper-case characters, lower-case characters, digits, and special characters.

    Special characters do not include the question mark (?) and space.
- The password entered in interactive mode is not displayed on the screen.
- You can press **CTRL_C** to cancel the password-based locking operation.
- To unlock the user interface, press **Enter**, and then enter the correct password as prompted.

Example

Lock the current user interface after logging in through the console port.

```
<HUAWEI> lock
Please configure the login password (8-16)
Enter Password:
Confirm Password:
Info: The terminal is locked.
```

To log in to the system again, press **Enter**. The following information is displayed:

```
Enter Password:
```

Enter the correct password and return to the user view.

```
<HUAWEI>
```

2.6.37 matched upper-view

Function

The **matched upper-view** command allows a device to search for the **undo** command in the upper view, and returns to the upper view.

The **undo matched upper-view** command prohibits a device from searching for the **undo** command in the upper view.

By default, a device does not search for the **undo** command in the upper view.

Format

matched upper-view

undo matched upper-view

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

If the **matched upper-view** command is run, when you run an **undo** command that is not registered in the current view, a device searches for the **undo** in the upper view. If the device finds the same **undo** command, it executes this command in the upper view. If the device does not find the same **undo** command in the upper view, it continues to search for this command in more upper views till the system view.

Running this command brings security risks. For example, if you run the **undo ftp server** command in the interface view, while this command is not registered in the interface view, the device automatically searches for it in the upper view, that is, the system view, and disables the FTP function.

The **matched upper-view** command is valid only for current login users who run this command.

Example

Allow a device to search for the **undo** command in the upper view.

```
<HUAWEI> system-view
[HUAWEI] matched upper-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo ftp server
Info: Succeeded in closing the FTP server.
```

Prohibit a device from searching for the **undo** command in the upper view.

```
<HUAWEI> system-view
[HUAWEI] undo matched upper-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo ftp server
                              ^
Error: Unrecognized command found at '^' position.
```


2.6.38 peer-public-key end

Function

The **peer-public-key end** command returns to the system view from the public key view and saves the configured public keys.

Format

peer-public-key end

Parameters

None

Views

Public key view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You must save the public key generated on the remote host to the local host, which ensures that the validity check on the remote end is successful. After editing a public key in the public key view, you can run this command to return to the system view.

Prerequisites

Before you run this command, the **rsa peer-public-key** command has been run to enter the RSA public key view, the **dsa peer-public-key** command has been run to enter the DSA public key view, or the **ecc peer-public-key** command has been run to enter the ECC public key view.

Example

Return to the system view from the public key view.

```
<HUAWEI> system-view
[HUAWEI] dsa peer-public-key dsakey001 encoding-type der
[HUAWEI-dsa-public-key] public-key-code begin
[HUAWEI-dsa-key-code] 308188
[HUAWEI-dsa-key-code] 028180
[HUAWEI-dsa-key-code] B21315DD 859AD7E4 A6D0D9B8 121F23F0 006BB1BB
[HUAWEI-dsa-key-code] A443130F 7CDB95D8 4A4AE2F3 D94A73D7 36FDFD5F
[HUAWEI-dsa-key-code] 411B8B73 3CDD494A 236F35AB 9BBFE19A 7336150B
[HUAWEI-dsa-key-code] 40A35DE6 2C6A82D7 5C5F2C36 67FBC275 2DF7E4C5
[HUAWEI-dsa-key-code] 1987178B 8C364D57 DD0AA24A A0C2F87F 474C7931
[HUAWEI-dsa-key-code] A9F7E8FE E0D5A1B5 092F7112 660BD153 7FB7D5B2
[HUAWEI-dsa-key-code] 171896FB 1FFC38CD
[HUAWEI-dsa-key-code] 0203
[HUAWEI-dsa-key-code] 010001
```



```
[HUAWEI-dsa-key-code] public-key-code end
[HUAWEI-dsa-public-key] peer-public-key end
[HUAWEI]
```

2.6.39 public-key-code begin

Function

The **public-key-code begin** command displays the public key editing view.

Format

public-key-code begin

Parameters

None

Views

Public key view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To ensure that the remote host passes the validity check performed by the local host, the public key generated on the remote host must be saved to the local host. To save the public key, run the **public-key-code begin** command to enter the public key editing view and then enter the key. The key characters can contain spaces. You can also press **Enter** to enter data in another line.

Prerequisite

A key name has been specified using the **rsa peer-public-key**, **dsa peer-public-key**, or **ecc peer-public-key** command.

Precautions

- The public key must be a hexadecimal character string in the public key encoding format, and generated by the client or server that supports SSH.
- The public key displayed using the **display rsa local-key-pair public**, **display dsa local-key-pair public**, or **display ecc local-key-pair public** command can be used as the key data to enter.
- The last line of the key cannot contain only spaces and dsa-key; otherwise, the spaces at the beginning of the lines that are entered will be automatically deleted, and an error will be reported after the **public-key-code end** command is run.

Example

Display the DSA public key editing view and enter the key data.

```
<HUAWEI> system-view
[HUAWEI] dsa peer-public-key dsakey001 encoding-type der
[HUAWEI-dsa-public-key] public-key-code begin
[HUAWEI-dsa-key-code] 308188
[HUAWEI-dsa-key-code] 028180
[HUAWEI-dsa-key-code] B21315DD 859AD7E4 A6D0D9B8 121F23F0 006BB1BB
[HUAWEI-dsa-key-code] A443130F 7CDB95D8 4A4AE2F3 D94A73D7 36FDFD5F
[HUAWEI-dsa-key-code] 411B8B73 3CDD494A 236F35AB 9BBFE19A 7336150B
[HUAWEI-dsa-key-code] 40A35DE6 2C6A82D7 5C5F2C36 67FBC275 2DF7E4C5
[HUAWEI-dsa-key-code] 1987178B 8C364D57 DD0AA24A A0C2F87F 474C7931
[HUAWEI-dsa-key-code] A9F7E8FE E0D5A1B5 092F7112 660BD153 7FB7D5B2
[HUAWEI-dsa-key-code] 171896FB 1FFC38CD
[HUAWEI-dsa-key-code] 0203
[HUAWEI-dsa-key-code] 010001
[HUAWEI-dsa-key-code] public-key-code end
[HUAWEI-dsa-public-key] peer-public-key end
[HUAWEI]
```

2.6.40 public-key-code end

Function

The **public-key-code end** command returns to the public key view from the public key editing view and saves the configured public key.

Format

public-key-code end

Parameters

None

Views

Public key editing view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After this command is run, editing the public key ends. Before saving the public key, the system will check the validity of the key.

- If there are illegal characters in the public key configured by the user, the system displays an error prompt. The public key is then discarded, and the configuration fails.
- If the public key configured is valid, it is saved in the public key chain table of the host.

Prerequisites

Before you run this command, the **public-key-code begin** command has been run to enter the public key edit view.

Precautions

- Generally, in the public key view, only the **public-key-code end** command can be used to exit. The **quit** command cannot be used.
- If no valid key coding is input, the key cannot be generated after the **public-key-code end** command is used. The system prompts that key generation fails.
- If the key has been deleted in another window, when you run the **public-key-code end** command, the system prompts that the key does not exist and returns to the system view.

Example

Exit the DSA public key editing view and saves the DSA key configuration.

```
<HUAWEI> system-view
[HUAWEI] dsa peer-public-key dsakey001 encoding-type der
[HUAWEI-dsa-public-key] public-key-code begin
[HUAWEI-dsa-key-code] 308188
[HUAWEI-dsa-key-code] 028180
[HUAWEI-dsa-key-code] B21315DD 859AD7E4 A6D0D9B8 121F23F0 006BB1BB
[HUAWEI-dsa-key-code] A443130F 7CDB95D8 4A4AE2F3 D94A73D7 36FDFD5F
[HUAWEI-dsa-key-code] 411B8B73 3CDD494A 236F35AB 9BBFE19A 7336150B
[HUAWEI-dsa-key-code] 40A35DE6 2C6A82D7 5C5F2C36 67FBC275 2DF7E4C5
[HUAWEI-dsa-key-code] 1987178B 8C364D57 DD0AA24A A0C2F87F 474C7931
[HUAWEI-dsa-key-code] A9F7E8FE E0D5A1B5 092F7112 660BD153 7FB7D5B2
[HUAWEI-dsa-key-code] 171896FB 1FFC38CD
[HUAWEI-dsa-key-code] 0203
[HUAWEI-dsa-key-code] 010001
[HUAWEI-dsa-key-code] public-key-code end
[HUAWEI-dsa-public-key] peer-public-key end
[HUAWEI]
```

2.6.41 rsa local-key-pair create

Function

The **rsa local-key-pair create** command generates the local RSA host and server key pairs.

By default, the local RSA host and server key pairs are not configured.

Format

rsa local-key-pair create

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To implement secure data exchange between the server and client, run the **rsa local-key-pair create** command to generate a local key pair.

Precautions

If the RSA key pair exists, the system prompts you to confirm whether to replace the original key pair. The keys in the new key pair are named **device name_Server** and **device name_Host**, for example, HUAWEI_Host and HUAWEI_Server. After being encrypted by AES256, the local RSA private key is saved to the hostkey and serverkey files in the system NOR FLASH.

After you run this command, the system prompts you to enter the number of bits in the host key. The difference between the bits in the server and host key pairs must be at least 128 bits. The length of the server or host key pair is 2048 ~ 4096 bits.

After you run this command, the generated key pair is saved in the device and will not be lost after the device restarts.

To improve security of the device, it is recommended that you use a key pair of 4096 bits.

This command is not saved in a configuration file.

Example

Generate the local RSA host and server key pairs.

```
<HUAWEI> system-view
[HUAWEI] rsa local-key-pair create
The key name will be: HUAWEI_Host
The range of public key size is (2048 ~ 4096).
NOTES: If the key modulus is greater than 512,
       it will take a few minutes.
Input the bits in the modulus[default = 2048]:
Generating keys...
.....++++++++
.....++++++++
.....+++++++++
.....+++++++++
```

2.6.42 rsa local-key-pair destroy

Function

The **rsa local-key-pair destroy** command deletes all local RSA host and server key pairs.

Format

rsa local-key-pair destroy

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To delete the local key pairs, run **rsa local-key-pair destroy** command. If the host key pair and server key pair of an SSH server are deleted, run the **rsa local-key-pair create** command to create a new host key pair and server key pair for the SSH server.

After you run this command, verify that all local RSA keys are deleted. This command is not saved in a configuration file.

Prerequisite

The local RSA key pairs that can be deleted exist.

Example

Delete all RSA server key pairs.

```
<HUAWEI> system-view
[HUAWEI] rsa local-key-pair destroy
% The name for the keys which will be destroyed is HUAWEI_Host.
% Confirm to destroy these keys? [y/n]:y
Destroying keys.............Succeeded.
```

2.6.43 rsa peer-public-key

Function

The **rsa peer-public-key** command configures an encoding format for an RSA public key and displays the RSA public key view.

The **undo rsa peer-public-key** command deletes an RSA public key.

By default, the encoding format is distinguished encoding rules (DER) for an RSA public key.

Format

rsa peer-public-key *key-name* [**encoding-type** { **der** | **openssh** | **pem** }]

undo rsa peer-public-key *key-name*

Parameters

Parameter	Description	Value
key-name	Specifies the RSA public key name.	The value is a string of 1 to 30 case-insensitive characters without spaces. **NOTE** The string can contain spaces if it is enclosed with double quotation marks (").
encoding-type	Specifies the encoding format of an RSA public key.	-
der	Specifies the DER format of an RSA public key. DER encodes data in hexadecimal format.	-
openssh	Specifies the OpenSSH format of an RSA public key. OpenSSH encodes data in base-64 format. OpenSSH is an encoding format based on PEM.	-
pem	Specifies the PEM format of an RSA public key. PEM encodes data in base-64 format.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you use an RSA public key for authentication, you must specify the public key of the corresponding client for an SSH user on the server. When the client logs in to the server, the server uses the specified public key to authenticate the client. You can also save the public key generated on the server to the client. Then the

client can be successfully authenticated by the server when it logs in to the server for the first time.

Huawei data communications devices support the DER, OpenSSH and PEM formats for RSA keys. If you use an RSA key in non-DER/OpenSSH/PEM format, use a third-party tool to convert the key into a key in DER, OpenSSH or PEM format.

Because a third-party tool is not released with Huawei system software, RSA usability is unsatisfactory. In addition to DER, RSA keys need to support the privacy-enhanced mail (PEM) and OpenSSH formats to improve RSA usability.

Third-party software, such as PuTTY, OpenSSH, and OpenSSL, can be used to generate RSA keys in different formats. The details are as follows:

- The PuTTY generate RSA keys in PEM format.
- The OpenSSH generates RSA keys in OpenSSH format.
- The OpenSSL generates RSA keys in DER format.

OpenSSL is an open source software. You can download related documents at the OpenSSL official website.

After you configure an encoding format for an RSA public key, Huawei data communications device automatically generates an RSA public key in the configured encoding format and enters the RSA public key view. Then you can run the **public-key-code begin** command and manually copy the RSA public key generated on the peer device to the local device.

Prerequisite

The RSA public key in hexadecimal notation on the remote host has been obtained and recorded.

Follow-up Procedure

After you copy the RSA public key generated on the peer device to the local device, perform the following operations to exit the RSA public key view:

1. Run the **public-key-code end** command to return to the RSA public key view.
2. Run the **peer-public-key end** command to exit the RSA public key view and return to the system view.

Precautions

When you run the **undo rsa peer-public-key** command to delete a public key:

- If the public key has been assigned to an SSH client, run the **undo ssh user** *user-name* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } command to release the binding between the public key and the SSH client. If you do not release the binding between them, the **undo dsa peer-public-key** command will fail to delete the public key.
- If the name of the host public key of the SSH server to be connected is specified on the SSH client, you need to run the **undo ssh client** *servername* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } command to delete the host public key of the SSH server. Otherwise, the DSA public key cannot be deleted.

The peer public key supports only PKCS#1. Other PKCS versions are not supported.

Example

Display the RSA public key view.

```
<HUAWEI> system-view
[HUAWEI] rsa peer-public-key rsakey001
[HUAWEI-rsa-public-key]
```

Configure an encoding format for an RSA public key and enter the RSA public key view.

```
<HUAWEI> system-view
[HUAWEI] rsa peer-public-key RsaKey001 encoding-type openssh
[HUAWEI-rsa-public-key]
```

2.6.44 run

Function

The **run** command runs a user view command in the system view.

By default, a user view command cannot be run in the system view.

Format

run *command-line*

Parameters

Parameter	Description	Value
command-line	Specifies a command to be run.	-

Views

All views except the user view

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Some commands can be run only in the user view. To run these commands, you must return to the user view first. To facilitate command execution, the device allows you to run the **run** command to run such commands in the other views without returning to the user view.

Precautions

- The command specified in the **run** command can be run in the user view.
- When you run the **run** command, the association help function is unavailable.
- When you check the command history on the device using the **display history-command** command, only the commands that you enter are recorded. The command format is **run** *command-line*.

- When you check log information using the **SHELL/5/CMDRECORD** command, only the commands that are actually run are recorded in logs. The command format is **run** *command-line*.

Example

Run the **dir *.cfg** command to check the .cfg file in the system view.

```
<HUAWEI> system-view
[HUAWEI] run dir *.cfg
Directory of flash:/
  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-         11,970  Mar 14 2012 19:11:22   31.cfg
    1  -rw-         12,033  Apr 22 2012 17:10:30   31_new.cfg
509,256 KB total (118,784 KB free)
```

2.6.45 send

Function

The **send** command configures a device to send messages to all user interfaces.

Format

send { **all** | *ui-number* | *ui-type ui-number1* }

Parameters

Parameter	Description	Value
all	Specifies that the device sends messages to all user interfaces.	-
ui-number	Specifies the absolute number of a user interface.	The minimum value is 0. The maximum value is the number of the user interfaces that the device supports minus 1.
ui-type	Specifies the type of a user interface.	-
ui-number1	Specifies the relative number of a user interface.	-

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

After you run the **send** command on a device, the device prompts you to enter a message to send. After you confirm to send this message, the user who logs in to the device from a specified user interface can receive this message.

Example

Send a message to the user interface VTY 0.

```
<HUAWEI> send vty 0
Enter message, end with CTRL+Z or Enter; abort with CTRL+C:
Hello, good morning!
Warning: Send the message? [Y/N]: y
```

After you confirm to send the message, the user who logs in to the HUAWEI from VTY 0 can receive this message.

```
<HUAWEI>
Info: Receive a message from VTY2:Hello, good morning!
```

2.6.46 ssh authentication-type default password

Function

The **ssh authentication-type default password** command configures password authentication as the default authentication mode for SSH users.

The **undo ssh authentication-type default password** command cancels the default password authentication mode for SSH users.

By default, the default authentication mode of SSH users is password authentication.

Format

ssh authentication-type default password

undo ssh authentication-type default password

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When there are multiple SSH users, the default password authentication mode simplifies the configuration.

When a TACACS server is used to authenticate a user who uses SSH to log in to a device, the network administrator must specify the SSH user on the TACACS server. In most cases, the SSH server cannot obtain the user information from the TACACS server. In this situation, you can set the authentication mode to **password**. SSH users can then directly log in to the device without additional SSH user configurations on the device.

Precautions

To configure password authentication for a specific SSH user, you can also run the **ssh user** *user-name* **authentication-type password** command.

Example

Configure password authentication as the default authentication mode for SSH users.

```
<HUAWEI> system-view
[HUAWEI] ssh authentication-type default password
```

2.6.47 ssh authorization-type default aaa

Function

The **ssh authorization-type default aaa** command configures the AAA authorization function for the SSH public key authentication user.

The **undo ssh authorization-type default aaa** command cancels the AAA authorization function configured for the SSH public key authentication user.

By default, the AAA authorization function is not configured for the SSH public key authentication user.

Format

ssh authorization-type default aaa

undo ssh authorization-type default aaa

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The SSH public key authentication user is an SSH user that uses the elliptic curve cryptography (ECC), Rivest-Shamir-Adleman (RSA), or digital signature algorithm (DSA) authentication mode.

If the AAA authorization function is not configured for the SSH public key authentication user, the SSH public key authentication user uses the level of the involved VTY channel. After the AAA authorization function is configured for the SSH public key authentication user, if the authorization succeeds, the SSH public key authentication user uses the level returned by the AAA. If the authorization fails, the user still uses the level of the involved VTY channel.

Precautions

AAA authorization configuration succeeds for the SSH public key authentication user if the following conditions are met:

- A local authorization scheme is configured for the default domain of the AAA management user.
- A local user exists, and the SSH access type is configured.

Example

Configure the AAA authorization function for the SSH public key authentication user.

```
<HUAWEI> system-view
[HUAWEI] ssh authorization-type default aaa
```

2.6.48 ssh client assign

Function

The **ssh client assign** command specifies the host public key of an SSH server on an SSH client.

The **undo ssh client assign** command cancels the specified host public key of the SSH server on the SSH client.

By default, the host public key of a server is not specified on clients.

Format

ssh client *servername* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } *keyname*

undo ssh client *servername* **assign** { **rsa-key** | **dsa-key** | **ecc-key** }

Parameters

Parameter	Description	Value
servername	Specifies the host name or IP address of an SSH server.	The value is a string of 1 to 255 characters without spaces.

Parameter	Description	Value
rsa-key	Specifies the RSA public key.	-
dsa-key	Specifies the DSA public key.	-
ecc-key	Specifies the ECC public key.	-
keyname	Specifies the SSH server public key name that has been configured on an SSH client.	The value is a string of 1 to 30 case-insensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If an SSH client connects to an SSH server for the first time and first authentication is not enabled on the SSH client using the **ssh client first-time enable** command, the SSH client must determine whether the server is reliable. To do so, run the **ssh client assign** command to specify the host public key of the SSH server and the mapping between the key and SSH server on the SSH client. The client then uses the correct public key to determine whether the server is reliable based on the mapping.

Precautions

The name of the RSA, DSA, or ECC public key to be assigned to the SSH server must be the same as that configured on the SSH client. This public key must have been configured on the SSH server using the **rsa peer-public-key**, **dsa peer-public-key**, or **ecc peer-public-key** command. If either of the preceding conditions is not met, RSA, DSA, or ECC public key authentication of the SSH server fails on the SSH client.

To improve security, it is not recommended that you use RSA or DSA as the authentication algorithm.

Example

Assign the DSA public key to the SSH server.

```
<HUAWEI> system-view
[HUAWEI] ssh client 10.164.39.120 assign dsa-key sshdsakey01
```

Delete the DSA public key of the SSH server.

```
<HUAWEI> system-view
[HUAWEI] undo ssh client 10.164.39.120 assign dsa-key
```


2.6.49 ssh client cipher

Function

The **ssh client cipher** command configures an encryption algorithm list for an SSH client.

By default, the WEAKEA plug-in is not installed; the SSH client supports only the **aes128_ctr** and **aes256_ctr** algorithms; the **undo ssh client cipher** command cannot be used. After the WEAKEA plug-in is installed, the **aes256_cbc**, **aes128_cbc**, **3des_cbc**, and **des_cbc** algorithms are supported, and the **undo ssh client cipher** command can be used.

Format

ssh client cipher { **aes128_ctr** | **aes256_ctr** } *

Parameters

Parameter	Description	Value
aes128_ctr	Specifies the CTR AES128 encryption algorithm.	-
aes256_ctr	Specifies the CTR AES256 encryption algorithm.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An SSH server and a client need to negotiate an encryption algorithm for the packets exchanged between them. You can run the **ssh client cipher** command to configure an encryption algorithm list for the SSH client. After the SSH server receives a packet from the client, the server matches the encryption algorithm list of the client against its local list and selects the first matched encryption algorithm. If no encryption algorithm matches, the negotiation fails.

Precautions

The following encryption algorithms are listed in descending order of security level: **aes256_ctr** and **aes128_ctr**.

The system software does not support the **aes256_cbc**, **aes128_cbc**, **3des_cbc,** and **des_cbc** parameters. To use these parameters, you need to install the

WEAKEA plug-in. To ensure high security, you are advised to configure the **aes256_ctr** or **aes128_ctr** parameter. For details about how to install the WEAKEA plug-in, see WEAKEA Configuration.

In V200R019C00 and later versions, when the device starts with the default configurations, it automatically performs the following configurations and saves the configurations to the configuration file:

- Run the **ssh server dh-exchange min-len 2048** command to set the minimum key length supported during Diffie-hellman-group-exchange key exchange between the SSH server and client to 2048 bytes.
- Run the **ssh server cipher aes256_ctr aes128_ctr** command to configure CTR encryption algorithms for an SSH server.
- Run the **ssh server hmac sha2_256** command to configure the HMAC SHA2_256 algorithm for an SSH server.
- Run the **ssh client cipher aes256_ctr aes128_ctr** command to configure CTR encryption algorithms for an SSH client.
- Run the **ssh client hmac sha2_256** command to configure the HMAC SHA2_256 algorithm for an SSH client.

Example

Configure CTR encryption algorithms for an SSH client.

```
<HUAWEI> system-view
[HUAWEI] ssh client cipher aes128_ctr aes256_ctr
```

2.6.50 ssh client first-time enable

Function

The **ssh client first-time enable** command enables the first authentication function on an SSH client.

The **undo ssh client first-time enable** command disables the first authentication function on the SSH client.

By default, the first authentication function is disabled on the SSH client.

Format

ssh client first-time enable

undo ssh client first-time enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an SSH client accesses an SSH server for the first time and the public host key of the SSH server is not configured on the SSH client, run the **ssh client first-time enable** command to enable the first authentication function. The SSH client then can access the SSH server and save the public host key on the SSH client. When the SSH client accesses the SSH server next time, the saved public host key is used to authenticate the SSH server.

Precautions

To log in to the SSH server successfully at the first time, you can also run the **ssh client assign** command to pre-assign a public host key to the SSH server. When you use STelnet or SFTP to connect to the server, you need to specify the public key authentication algorithm for server authentication as the ECC, RSA, or DSA key algorithm.

Example

Enable the first authentication function on the SSH client.

```
<HUAWEI> system-view
[HUAWEI] ssh client first-time enable
```

2.6.51 ssh client hmac

Function

The **ssh client hmac** command configures an HMAC algorithm list for an SSH client.

By default, the WEAKEA plug-in is not installed, an SSH client supports only the **sha2_256** algorithm, and the **undo ssh client hmac** command is unavailable. When the WEAKEA plug-in is installed, an SSH client also supports the **sha2_256_96**, **sha1**, **sha1_96**, **md5** and **md5_96** algorithms, and the **undo ssh client hmac** command is available.

Format

ssh client hmac { **sha2_256** }

Parameters

Parameter	Description	Value
sha2_256	Specifies the SHA2_256 algorithm.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An SSH server and a client need to negotiate an HMAC algorithm for the packets exchanged between them. You can run the **ssh client hmac** command to configure an HMAC algorithm list for the SSH client. After the SSH server receives a packet from the client, the server matches the list of the client against its local list and selects the first matched HMAC algorithm. If no matched HMAC algorithms, the negotiation fails.

Precautions

The system software does not support the **sha2_256_96**, **sha1**, **sha1_96**, **md5**, and **md5_96** parameters. To use these parameters, you need to install the WEAKEA plug-in. For higher security purposes, you are advised to specify the **sha2_256** parameter. For details about how to install the WEAKEA plug-in, see WEAKEA Configuration.

In V200R019C00 and later versions, when the device starts with the default configurations, it automatically performs the following configurations and saves the configurations to the configuration file:

- Run the **ssh server dh-exchange min-len 2048** command to set the minimum key length supported during Diffie-hellman-group-exchange key exchange between the SSH server and client to 2048 bytes.
- Run the **ssh server cipher aes256_ctr aes128_ctr** command to configure CTR encryption algorithms for an SSH server.
- Run the **ssh server hmac sha2_256** command to configure the HMAC SHA2_256 algorithm for an SSH server.
- Run the **ssh client cipher aes256_ctr aes128_ctr** command to configure CTR encryption algorithms for an SSH client.
- Run the **ssh client hmac sha2_256** command to configure the HMAC SHA2_256 algorithm for an SSH client.

Example

Configure the **SHA2_256** algorithm for an SSH client.

```
<HUAWEI> system-view
[HUAWEI] ssh client hmac sha2_256
```


2.6.52 ssh client key-exchange

Function

The **ssh client key-exchange** command configures a key exchange algorithm list for an SSH client.

By default, the WEAKEA plug-in is not installed, an SSH client supports only the **dh_group14_sha256**, **dh_group15_sha512**, **dh_group16_sha512**, **dh_group_exchange_sha256**, **ecdh_sha2_nistp256**, **ecdh_sha2_nistp384**, and **ecdh_sha2_nistp521** algorithm, and the **undo ssh client key-exchange** command is unavailable. When the WEAKEA plug-in is installed, an SSH client also supports the **dh_group14_sha1**, **dh_group1_sha1**, and **dh_group_exchange_sha1** algorithms, and the **undo ssh client key-exchange** command is available.

Format

ssh client key-exchange { **dh_group14_sha256** | **dh_group15_sha512** | **dh_group16_sha512** | **dh_group_exchange_sha256** | **ecdh_sha2_nistp256**| **ecdh_sha2_nistp384**| **ecdh_sha2_nistp521** }*

Parameters

Parameter	Description	Value
dh_group14_sha256	Adds the diffie-hellman-group14_sha256 algorithm to the key exchange algorithm list of an SSH client.	-
dh_group15_sha512	Adds the diffie-hellman-group15_sha512 algorithm to the key exchange algorithm list of an SSH client.	-
dh_group16_sha512	Adds the diffie-hellman-group16_sha512 algorithm to the key exchange algorithm list of an SSH client.	-
dh_group_exchange_sha256	Adds the diffie-hellman-group_exchange_sha256 algorithm to the key exchange algorithm list of an SSH client.	-
ecdh_sha2_nistp256	Adds the ecdh_sha2_nistp256 algorithm to the key exchange algorithm list of an SSH client.	-
ecdh_sha2_nistp384	Adds the ecdh_sha2_nistp384 algorithm to the key exchange algorithm list of an SSH client.	-

Parameter	Description	Value
ecdh_sha2_nistp521	Adds the ecdh_sha2_nistp521 algorithm to the key exchange algorithm list of an SSH client.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An SSH server and a client need to negotiate a key exchange algorithm for the packets exchanged between them. You can run the **ssh client key-exchange** command to configure a key exchange algorithm list for the SSH client. The server compares the key exchange algorithm list sent by the client with its own key exchange algorithm list, and selects the first key exchange algorithm on the client's list that matches a key exchange algorithm on its own list as the key exchange algorithm for packet transmission. If no algorithm on the client's list matches an algorithm on the server's list, the negotiation fails.

Precautions

The following key exchange algorithms are listed in descending order of security level: **dh_group_exchange_sha256**, **ecdh_sha2_nistp521**, **ecdh_sha2_nistp384**, **ecdh_sha2_nistp256**, **dh_group16_sha512**, **dh_group15_sha512**, and **dh_group14_sha256**.

The system software does not contain the **dh_group_exchange_sha1**, **dh_group14_sha1**, and **dh_group1_sha1** parameters. To use these parameters, you need to install the WEAKEA plug-in. However, the algorithms specified by these parameters are less secure. For higher security purposes, you are advised to use other parameters. For details about how to install the WEAKEA plug-in, see WEAKEA Configuration.

NOTICE

The higher the security level of a key exchange algorithm, the longer the time required by the device to calculate the key.

Example

Add two key exchange algorithms **dh_group_exchange_sha256** and **dh_group14_sha256** to the key exchange algorithm list of the SSH client.


```
<HUAWEI> system-view
[HUAWEI] ssh client key-exchange dh_group_exchange_sha256 dh_group14_sha256
```

2.6.53 ssh client rekey

Function

The **ssh client rekey** command configures key renegotiation parameters for an SSH client.

The **undo ssh client rekey** command restores the default key renegotiation parameter settings of the SSH client.

By default, the interval at which an SSH client triggers key renegotiation is 60 minutes, the maximum size of data sent and received by an SSH client during key renegotiation is 1000 MB, and a maximum of 268435456 (2^28) packets can be sent and received by an SSH client during key renegotiation.

Format

ssh client rekey { **time** *rekey-time* | **data-limit** *data-limit* | **max-packet** *max-packet* } *

undo ssh client rekey { **time** | **data-limit** | **max-packet** } *

Parameters

Parameter	Description	Value
time *rekey-time*	Specifies an interval at which key renegotiation is triggered.	The value is an integer ranging from 30 to 1440, in minutes.
data-limit *data-limit*	Specifies the maximum size of data sent and received during key renegotiation.	The value is an integer ranging from 100 to 10000, in MB.
max-packet *max-packet*	Specifies the maximum number of packets sent and received during key renegotiation.	The value is an integer ranging from 268435456 to 2147483648.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the SSH session duration reaches the specified interval at which key renegotiation is triggered, the system renegotiates a key and uses the new key to establish SSH session connections, improving system security.

If the **time** parameter is configured for an SSH client, the client sends a key renegotiation packet to the server to renegotiate an encryption key when the SSH session duration reaches the specified interval.

If the **data-limit** parameter is configured for an SSH client, the client sends a key renegotiation packet to the server to renegotiate an encryption key when the size of sent and received data exceeds the maximum value.

If the **max-packet** parameter is configured for an SSH client, the client sends a key renegotiation packet to the server to renegotiate an encryption key when the number of sent and received packets exceeds the maximum value.

Precautions

A key renegotiation request is initiated when either an SSH client or server meets the key renegotiation criteria. After one party initiates such a request, the other party responds.

Example

Set the maximum size of data sent and received by the SSH client during key renegotiation to 2000 MB.

```
<HUAWEI> system-view
[HUAWEI] ssh client rekey data-limit 2000
```

2.6.54 ssh server acl

Function

The **ssh server acl** command configures an ACL that the SSH server uses to control the access permission of SSH clients.

The **undo ssh server acl** command cancels the configured ACL of the SSH server.

By default, no ACL is configured for SSH servers.

Format

ssh [**ipv6**] **server acl** *acl-number*

undo ssh [**ipv6**] **server acl**

Parameters

Parameter	Description	Value
acl-number	Specifies an ACL number.	The value is an integer that ranges from 2000 to 3999.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Configure the ACL for the following servers for access control:

- STelnet server: controls which clients can log in to this server through STelnet.
- SFTP server: controls which clients can log in to this server through SFTP.
- SCP server: controls which clients can log in to this server through SCP.

Prerequisites

An ACL has been configured using the **acl (system view)** command in the system view, and an ACL rule has been configured using the **rule (basic ACL view)** or **rule (advanced ACL view)** command.

Precautions

A basic ACL can be configured to restrict source addresses. An advanced ACL can be configured to restrict source and destination addresses.

Example

Configure ACL 2000 on an SSH server.

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule permit source 10.10.10.10 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] ssh server acl 2000
```

2.6.55 ssh server authentication-retries

Function

The **ssh server authentication-retries** command sets the maximum number of authentication retries for an SSH connection.

The **undo ssh server authentication-retries** command restores the default maximum number of authentication retries for an SSH connection.

The default maximum number of authentication retries for an SSH connection is 3.

Format

ssh server authentication-retries *times*

undo ssh server authentication-retries

Parameters

Parameter	Description	Value
times	Specifies the maximum number of authentication retries for an SSH connection.	The value is an integer that ranges from 1 to 5.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure the maximum number of authentication retries for an SSH connection, run the **ssh server authentication-retries** command. This prevents server overload due to numerous malicious access requests.

Precautions

The configured number of retries takes effect upon the next login.

Example

Set the maximum number of authentication retries to 4.

```
<HUAWEI> system-view
[HUAWEI] ssh server authentication-retries 4
```

2.6.56 ssh server authentication-type keyboard-interactive enable

Function

The **ssh server authentication-type keyboard-interactive enable** command enables keyboard interactive authentication on an SSH server.

The **undo ssh server authentication-type keyboard-interactive enable** command disables keyboard interactive authentication on an SSH server.

By default, keyboard interactive authentication is enabled on SSH servers.

Format

ssh server authentication-type keyboard-interactive enable

undo ssh server authentication-type keyboard-interactive enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To log in to the SSH server in keyboard interactive authentication mode, run the **ssh server authentication-type keyboard-interactive enable** command.

To log in to the SSH server in password authentication mode, run the **undo ssh server authentication-type keyboard-interactive enable** command to disable keyboard interactive authentication.

Example

Enable keyboard interactive authentication on an SSH server.

```
<HUAWEI> system-view
[HUAWEI] ssh server authentication-type keyboard-interactive enable
```

2.6.57 ssh server cipher

Function

The **ssh server cipher** command configures an encryption algorithm list for an SSH server.

By default, the WEAKEA plug-in is not installed; the SSH server supports only the **aes128_ctr** and **aes256_ctr** algorithms; the **undo ssh server cipher** command cannot be used. After the WEAKEA plug-in is installed, the **aes256_cbc**, **aes128_cbc**, **3des_cbc**, and **des_cbc** algorithms are supported, and the **undo ssh server cipher** command can be used.

Format

ssh server cipher { **aes128_ctr** | **aes256_ctr** } *

Parameters

Parameter	Description	Value
aes128_ctr	Specifies the CTR AES128 encryption algorithm.	-
aes256_ctr	Specifies the CTR AES256 encryption algorithm.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An SSH server and a client need to negotiate an encryption algorithm for the packets exchanged between them. You can run the **ssh server cipher** command to configure an encryption algorithm list for the SSH server. After the SSH server receives a packet from the client, the server matches the encryption algorithm list of the client against its local list and selects the first matched encryption algorithm. If no encryption algorithm matches, the negotiation fails.

Precautions

The following encryption algorithms are listed in descending order of security level: **aes256_ctr** and **aes128_ctr**.

The system software does not support the **aes256_cbc**, **aes128_cbc**, **3des_cbc,** and **des_cbc** parameters. To use these parameters, you need to install the WEAKEA plug-in. To ensure high security, you are advised to configure the **aes256_ctr** or **aes128_ctr** parameter. For details about how to install the WEAKEA plug-in, see WEAKEA Configuration.

In V200R019C00 and later versions, when the device starts with the default configurations, it automatically performs the following configurations and saves the configurations to the configuration file:

- Run the **ssh server dh-exchange min-len 2048** command to set the minimum key length supported during Diffie-hellman-group-exchange key exchange between the SSH server and client to 2048 bytes.
- Run the **ssh server cipher aes256_ctr aes128_ctr** command to configure CTR encryption algorithms for an SSH server.
- Run the **ssh server hmac sha2_256** command to configure the HMAC SHA2_256 algorithm for an SSH server.
- Run the **ssh client cipher aes256_ctr aes128_ctr** command to configure CTR encryption algorithms for an SSH client.

- Run the **ssh client hmac sha2_256** command to configure the HMAC SHA2_256 algorithm for an SSH client.

Example

Configure CTR encryption algorithms for an SSH server.

```
<HUAWEI> system-view
[HUAWEI] ssh server cipher aes256_ctr aes128_ctr
```

2.6.58 ssh server dh-exchange min-len

Function

The **ssh server dh-exchange min-len** command configures the minimum key length supported during Diffie-hellman-group-exchange key exchange between the SSH server and client.

The **undo ssh server dh-exchange min-len** command restores the default minimum key length supported during Diffie-hellman-group-exchange key exchange between the SSH server and client.

By default, the minimum key length supported is 1024 bytes.

Format

ssh server dh-exchange min-len *min-len*

undo ssh server dh-exchange min-len

Parameters

Parameter	Description	Value
min-len	Specifies the minimum Diffie-hellman-group-exchange key length supported on the SSH server.	The value can be either 1024, 2048 or 3072, in bytes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The Diffie-hellman-group-exchange key of 1024 bytes poses security risks. If the SSH client supports the Diffie-hellman-group-exchange key of more than 1024 bytes, run the **ssh server dh-exchange min-len** command to set the minimum key length to 2048 bytes to improve security.

Precautions

Security risks exist if the minimum Diffie-hellman-group-exchange key length is less than 2048 bytes. You are advised to set the minimum key length to 2048 bytes.

In V200R019C00 and later versions, when the device starts with the default configurations, it automatically performs the following configurations and saves the configurations to the configuration file:

- Run the **ssh server dh-exchange min-len 2048** command to set the minimum key length supported during Diffie-hellman-group-exchange key exchange between the SSH server and client to 2048 bytes.
- Run the **ssh server cipher aes256_ctr aes128_ctr** command to configure CTR encryption algorithms for an SSH server.
- Run the **ssh server hmac sha2_256** command to configure the HMAC SHA2_256 algorithm for an SSH server.
- Run the **ssh client cipher aes256_ctr aes128_ctr** command to configure CTR encryption algorithms for an SSH client.
- Run the **ssh client hmac sha2_256** command to configure the HMAC SHA2_256 algorithm for an SSH client.

Example

Set the minimum key length supported during Diffie-hellman-group-exchange key exchange between the SSH server and client to 2048 bytes.

```
<HUAWEI> system-view
[HUAWEI] ssh server dh-exchange min-len 2048
```

2.6.59 ssh server hmac

Function

The **ssh server hmac** command configures an HMAC algorithm list for an SSH server.

By default, the WEAKEA plug-in is not installed, an SSH server supports only the **sha2_256** algorithm, and the **undo ssh server hmac** command is unavailable. When the WEAKEA plug-in is installed, an SSH server also supports the **sha2_256_96**, **sha1**, **sha1_96**, **md5** and **md5_96** algorithms, and the **undo ssh server hmac** command is available.

Format

ssh server hmac {**sha2_256** }

Parameters

Parameter	Description	Value
sha2_256	Specifies the SHA2_256 algorithm.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An SSH server and a client need to negotiate an HMAC algorithm for the packets exchanged between them. You can run the **ssh server hmac** command to configure an HMAC algorithm list for the SSH server. After the server receives a packet from the client, the server matches the list of the client against its local list and selects the first matched HMAC algorithm. If no matched HMAC algorithms, the negotiation fails.

Precautions

The system software does not support the **sha2_256_96**, **sha1**, **sha1_96**, **md5**, and **md5_96** parameters. To use these parameters, you need to install the WEAKEA plug-in. For higher security purposes, you are advised to specify the **sha2_256** parameter. For details about how to install the WEAKEA plug-in, see WEAKEA Configuration.

In V200R019C00 and later versions, when the device starts with the default configurations, it automatically performs the following configurations and saves the configurations to the configuration file:

- Run the **ssh server dh-exchange min-len 2048** command to set the minimum key length supported during Diffie-hellman-group-exchange key exchange between the SSH server and client to 2048 bytes.
- Run the **ssh server cipher aes256_ctr aes128_ctr** command to configure CTR encryption algorithms for an SSH server.
- Run the **ssh server hmac sha2_256** command to configure the HMAC SHA2_256 algorithm for an SSH server.
- Run the **ssh client cipher aes256_ctr aes128_ctr** command to configure CTR encryption algorithms for an SSH client.
- Run the **ssh client hmac sha2_256** command to configure the HMAC SHA2_256 algorithm for an SSH client.

Example

Configure the **SHA2_256** algorithm for an SSH server.

```
<HUAWEI> system-view
[HUAWEI] ssh server hmac sha2_256
```


2.6.60 ssh server key-exchange

Function

The **ssh server key-exchange** command configures a key exchange algorithm list for an SSH server.

By default, the WEAKEA plug-in is not installed, an SSH server supports only the **dh_group14_sha256**, **dh_group15_sha512**, **dh_group16_sha512**, **dh_group_exchange_sha256**, **ecdh_sha2_nistp256**, **ecdh_sha2_nistp384**, and **ecdh_sha2_nistp521** algorithm, and the **undo ssh server key-exchange** command is unavailable. When the WEAKEA plug-in is installed, an SSH server also supports the **dh_group14_sha1**, **dh_group1_sha1**, and **dh_group_exchange_sha1** algorithms, and the **undo ssh server key-exchange** command is available.

Format

ssh server key-exchange { **dh_group14_sha256** | **dh_group15_sha512** | **dh_group16_sha512** | **dh_group_exchange_sha256** | **ecdh_sha2_nistp256**| **ecdh_sha2_nistp384**| **ecdh_sha2_nistp521** }*

Parameters

Parameter	Description	Value
dh_group14_sha256	Adds the diffie-hellman-group14_sha256 algorithm to the key exchange algorithm list of an SSH server.	-
dh_group15_sha512	Adds the diffie-hellman-group15_sha512 algorithm to the key exchange algorithm list of an SSH server.	-
dh_group16_sha512	Adds the diffie-hellman-group16_sha512 algorithm to the key exchange algorithm list of an SSH server.	-
dh_group_exchange_sha256	Adds the diffie-hellman-group_exchange_sha256 algorithm to the key exchange algorithm list of an SSH server.	-
ecdh_sha2_nistp256	Adds the ecdh_sha2_nistp256 algorithm to the key exchange algorithm list of an SSH server.	-
ecdh_sha2_nistp384	Adds the ecdh_sha2_nistp384 algorithm to the key exchange algorithm list of an SSH server.	-

Parameter	Description	Value
ecdh_sha2_nistp521	Adds the ecdh_sha2_nistp521 algorithm to the key exchange algorithm list of an SSH server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An SSH server and a client need to negotiate a key exchange algorithm for the packets exchanged between them. You can run the **ssh server key-exchange** command to configure a key exchange algorithm list for the SSH server. The server compares the key exchange algorithm list sent by the client with its own key exchange algorithm list, and selects the first key exchange algorithm on the client's list that matches a key exchange algorithm on its own list as the key exchange algorithm for packet transmission. If no algorithm on the client's list matches an algorithm on the server's list, the negotiation fails.

Precautions

The following key exchange algorithms are listed in descending order of security level: **dh_group_exchange_sha256**, **ecdh_sha2_nistp521**, **ecdh_sha2_nistp384**, **ecdh_sha2_nistp256**, **dh_group16_sha512**, **dh_group15_sha512**, and **dh_group14_sha256**.

The system software does not contain the **dh_group_exchange_sha1**, **dh_group14_sha1**, and **dh_group1_sha1** parameters. To use these parameters, you need to install the WEAKEA plug-in. However, the algorithms specified by these parameters are less secure. For higher security purposes, you are advised to use other parameters. For details about how to install the WEAKEA plug-in, see WEAKEA Configuration.

Example

Add the **dh_group14_sha256** algorithm to the key exchange algorithm list of the SSH server.

```
<HUAWEI> system-view
[HUAWEI] ssh server key-exchange dh_group14_sha256
```


2.6.61 ssh server port

Function

The **ssh server port** command configures a listening port number for an SSH server.

The **undo ssh server port** command restores the default listening port number of an SSH server.

The default listening port number of the SSH server is 22.

Format

ssh [**ipv4** | **ipv6**] **server port** *port-number*

undo ssh [**ipv4** | **ipv6**] **server port**

Parameters

Parameter	Description	Value
port-number	Specifies the listening port number of the SSH server.	The value is 22 or an integer ranging from 1025 to 55535.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To prevent attackers from attacking the standard SSH listening port number, run the **ssh server port** command to configure a new listening port. This improves security.

Precautions

If the server is listening on port 22, the SSH client can log in successfully with no port specified. If the server is listening on another port, the port number must be specified.

Before changing the current port number, disconnect all devices from the port. After the port number is changed, the server starts to listen on the new port.

After the **ssh server port** *port-number* command is run, the numbers of IPv4 port and IPv6 port are both changed. To change the number of IPv4 port or IPv6 port separately, run the **ssh** { **ipv4** | **ipv6** } **server port** *port-number* command.

Example

Set the listening port number of the SSH server to 1025.

```
<HUAWEI> system-view
[HUAWEI] ssh server port 1025
```

Set the IPv4 port number of the SSH server to 1025.

```
<HUAWEI> system-view
[HUAWEI] ssh ipv4 server port 1025
```

2.6.62 ssh server publickey

Function

The **ssh server publickey** command specifies a public key algorithm for an SSH server.

The **undo ssh server publickey** command restores all the public key algorithms of an SSH server to default settings.

By default, the DSA, ECC, RSA, RSA_SHA2_256, and RSA_SHA2_512 algorithms are enabled.

Format

ssh server publickey { **dsa** | **ecc** | **rsa** | **rsa_sha2_256** | **rsa_sha2_512** } *

undo ssh server publickey

Parameters

Parameter	Description	Value
dsa	Specifies the DSA algorithm for an SSH server.	-
ecc	Specifies the ECC algorithm for an SSH server.	-
rsa	Specifies the RSA algorithm for an SSH server.	-
rsa_sha2_256	Specifies the RSA_SHA2_256 algorithm for an SSH server.	-
rsa_sha2_512	Specifies the RSA_SHA2_512 algorithm for an SSH server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to specify a public key algorithm for an SSH server. In this case, the SSH server cannot use other public key algorithms, improving device security. The ECC public key algorithm is recommended.

If a public key algorithm is specified in the **ssh server publickey** command, the SSH server can use the specified public key algorithm and cannot use other public key algorithms. For example, if the **ssh server publickey dsa** command is run, the SSH server can use the DSA algorithm and cannot use the ECC and RSA algorithms.

Precautions

A client can log in to an SSH server using a public key algorithm only if the server also uses this public key algorithm.

For security purposes, you are not advised to use the RSA algorithm with the key of less than 2048 bits to authenticate SSH users. Instead, you are advised to use the more secure ECC, RSA_SHA2_256, or RSA_SHA2_512 authentication algorithm.

If this command has been run for multiple times, the latest configuration takes effect.

Example

Configure an SSH server to use the ECC algorithm.

```
<HUAWEI> system-view
[HUAWEI] ssh server publickey ecc
```

2.6.63 ssh server rekey

Function

The **ssh server rekey** command sets key renegotiation parameters for an SSH server.

The **undo ssh server rekey** command restores the default key renegotiation parameter settings of the SSH server.

By default, the interval at which an SSH server triggers key renegotiation is 60 minutes, the maximum size of data sent and received by an SSH server during key renegotiation is 1000 MB, and a maximum of 268435456 (2^28) packets can be sent and received by an SSH server during key renegotiation.

Format

ssh server rekey { **time** *rekey-time* | **data-limit** *data-limit* | **max-packet** *max-packet* } *

undo ssh server rekey { **time** | **data-limit** | **max-packet** } *

Parameters

Parameter	Description	Value
time *rekey-time*	Specifies an interval at which key renegotiation is triggered.	The value is an integer ranging from 30 to 1440, in minutes.
data-limit *data-limit*	Specifies the maximum size of data sent and received during key renegotiation.	The value is an integer ranging from 100 to 10000, in MB.
max-packet *max-packet*	Specifies the maximum number of packets sent and received during key renegotiation.	The value is an integer ranging from 268435456 to 2147483648.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the SSH session duration reaches the specified interval at which key renegotiation is triggered, the system renegotiates a key and uses the new key to establish SSH session connections, improving system security.

After the **time** parameter is configured for an SSH server, the SSH server checks each SSH session. If the session duration reaches the interval, the SSH server sends a key renegotiation packet to the client to renegotiate an encryption key.

After the **data-limit** parameter is configured for an SSH server, the SSH server checks each SSH session. If the size of data sent and received by the SSH server through a session exceeds the maximum value, the SSH server sends a key renegotiation packet to the client to renegotiate an encryption key.

After the **max-packet** parameter is configured for an SSH server, the SSH server checks each SSH session. If the number of packets sent and received by the SSH server through a session exceeds the maximum value, the SSH server sends a key renegotiation packet to the client to renegotiate an encryption key.

Precautions

A key renegotiation request is initiated when either an SSH client or server meets the key renegotiation criteria. After one party initiates such a request, the other party responds.

Example

Set the maximum size of data sent and received by the SSH server during key renegotiation to 2000 MB.

```
<HUAWEI> system-view
[HUAWEI] ssh server rekey data-limit 2000
```

2.6.64 ssh server rekey-interval

Function

The **ssh server rekey-interval** command sets the interval for updating the SSH server key pair.

The **undo ssh server rekey-interval** command restores the default interval for updating the SSH server key pair.

The default interval for updating the SSH server key pair is 0, indicating that the key pair is never updated.

Format

ssh server rekey-interval *hours*

undo ssh server rekey-interval

Parameters

Parameter	Description	Value
hours	Specifies the interval for updating the server key pair.	The value is an integer that ranges from 0 to 24, in hours.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the server key pair is not updated for a long time, the key is easy to decrypt, and the server is insecure. After the interval for updating the SSH server key pair is set using the **ssh server rekey-interval** command, the device will automatically update the key pair at the specified interval.

Precautions

If the client is connected to the server, the server public key on the client is not updated immediately. This key is updated only when the client is reconnected to the server.

This command takes effect only for SSH1.X. However, SSH1.X provides poor security and is therefore not recommended.

Example

Set the interval for updating the SSH server key pair to 2 hours.

```
<HUAWEI> system-view
[HUAWEI] ssh server rekey-interval 2
```

2.6.65 ssh server timeout

Function

The **ssh server timeout** command sets the timeout period for SSH connection authentication.

The **undo ssh server timeout** restores the default timeout period for SSH connection authentication.

The default timeout period for SSH connection authentication is 60 seconds.

Format

ssh server timeout *seconds*

undo ssh server timeout

Parameters

Parameter	Description	Value
seconds	Specifies the timeout period for SSH connection authentication.	The value is an integer ranging from 1 to 120, in seconds.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a user has not logged in successfully before the timeout period for SSH connection authentication expires, the current connection is terminated to ensure

security. To query the current timeout period, run the **display ssh server** command.

Precautions

The timeout period setting takes effect upon next login.

NOTE

If a very short timeout period is configured for SSH connection authentication, user login may fail due to a connection timeout. Using the default timeout period is recommended.

Example

Set the timeout period for SSH connection authentication to 90 seconds.

```
<HUAWEI> system-view
[HUAWEI] ssh server timeout 90
```

2.6.66 ssh server-source

Function

The **ssh server-source** command specifies a source interface for an SSH server.

The **undo ssh server-source** command restores the default setting.

By default, no source interface is specified for an SSH server.

Format

ssh server-source -i *interface-type interface-number*

undo ssh server-source

ssh server-source all-interface

Parameters

Parameter	Description	Value
-i *interface-type interface-number*	Specifies the source interface for an SSH server.	-
all-interface	Specifies any interface that has an IPv4 address configured as the source interface of an SSH server.	-

NOTE

In V200R020C00 and later versions, an SSH server does not accept login connection requests from any interface by default. To allow authorized users to log in to the server, run a command to specify the source interface or source address of the server. For details about the command, see "Usage Scenario" in "Usage Guidelines" in this section.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In versions earlier than V200R020C00, an SSH server accepts login connection requests from all interfaces by default, leading to low system security. For details, see the product documentation of the corresponding version.

In V200R020C00 and later versions, an SSH server does not accept login connection requests from any interface by default. To authorize users to log in to the server, run either of the following commands to specify the source interface of the SSH server:

- Run the **ssh server-source -i** *interface-type interface-number* command to configure a specified interface as the source interface of the SSH server.
- Run the **ssh server-source all-interface** command to specify any interface with an IPv4 address configured on the device as the source interface of the SSH server.

Prerequisites

Before specifying a logical interface as the source interface, ensure that the source interface has been created and has an IPv4 address configured. Otherwise, this command cannot be executed successfully.

Precautions

After this command is run, the new configuration takes effect upon the next login.

After the source interface is specified, the system allows users to log in to the SSH server only using the specified source interface. This configuration applies to the SSH users who attempt to log in to the SSH server, but not to the SSH users who have logged in to the server.

After the source interface of an SSH server is specified using this command, ensure that authorized SSH users can access the source interface at Layer 3. Otherwise, the SSH users will fail to log in to the SSH server.

If the source address or source interface is not specified, there are security risks.

When the **ssh server-source -i** command is run, if a VLANIF interface is specified as the source interface and has a secondary address configured, SSH login using the secondary address is not supported.

After the **ssh server-source all-interface** command is run, the system allows SSH users to log in to the SSH server through all interfaces with IPv4 addresses configured. This increases system security risks. Therefore, you are not advised to run this command.

Example

Specify Loopback0 as the source interface of an SSH server.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 0
[HUAWEI-LoopBack0] ip address 10.1.1.1 24
[HUAWEI-LoopBack0] quit
[HUAWEI] ssh server-source -i loopback 0
```

2.6.67 ssh ipv6 server-source

Function

The **ssh ipv6 server-source** command specifies an IPv6 source address for an SSH server.

The **undo ssh ipv6 server-source** command cancels the IPv6 source address specified for an SSH server.

By default, the IPv6 source address of an SSH server is not specified.

Format

ssh ipv6 server-source -a *ipv6_address* [**-vpn-instance** *vpn_name*]

undo ssh ipv6 server-source

ssh ipv6 server-source all-interface

Parameters

Parameter	Description	Value
-a *ipv6_address*	Specifies the IPv6 source address for an SSH server.	The total length of an IPv6 address is 128 bits, which are divided into eight groups. Each group contains four hexadecimal digits. The value is in the format X:X:X:X:X:X:X:X.
-vpn-instance *vpn_name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain spaces. The VPN instance name cannot be **_public_**. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
all-interface	Indicates that any interface IPv6 address on the device can be used as the IPv6 source address of the SSH server.	-

NOTE

In V200R020C00 and later versions, an SSH server does not accept login connection requests from any interface by default. To allow authorized users to log in to the server, run a command to specify the source interface or source address of the server. For details about the command, see "Usage Scenario" in "Usage Guidelines" in this section.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In versions earlier than V200R020C00, an SSH server accepts connection requests from all IPv6 addresses by default, incurring security risks. For details, see the product documentation of the corresponding version.

In V200R020C00 and later versions, an SSH server does not accept login requests from any IPv6 address by default. To allow authorized users to log in to the SSH server, run either of the following commands to specify an IPv6 source address for the SSH server.

- Run the **ssh ipv6 server-source -a** *ipv6_address* [**-vpn-instance** *vpn_name*] command to configure the specified IPv6 address as the IPv6 source address of the SSH server.
- Run the **ssh ipv6 server-source all-interface** command to configure all interface IPv6 addresses on the device as the IPv6 source addresses of the SSH server.

Prerequisites

A VPN instance has been created before you specify it for an SSH server. Otherwise, the **ssh ipv6 server-source** command cannot be executed.

Configuration Impact

After an IPv6 source address is specified for an SSH server, SSH users can log in to the SSH server only using this IPv6 address. This configuration applies to the SSH users who attempt to log in to the SSH server, not to the SSH users who have logged in to the server.

Precautions

After this command is run, the new configuration takes effect upon the next login.

After an IPv6 source address is specified for an SSH server using this command, ensure that SFTP or SSH users can access this IPv6 address at Layer 3. Otherwise, SFTP or SSH users will fail to log in to the SSH server.

If the specified IPv6 source address is bound to a VPN instance, the SSH server is also bound to the VPN instance.

After the **ssh ipv6 server-source all-interface** command is run, the system allows SSH users to log in to the SSH server through all interfaces with IPv6 addresses configured. This increases system security risks. Therefore, running this command is not recommended.

Example

Specify the IPv6 source address 2001:DB8:: for an SSH server.

```
<HUAWEI> system-view
[HUAWEI] ssh ipv6 server-source -a 2001:DB8::
```

2.6.68 ssh user

Function

The **ssh user** command creates an SSH user.

The **undo ssh user** command deletes an SSH user.

By default, no SSH user is created.

Format

ssh user *user-name*

undo ssh user [*user-name*]

Parameters

Parameter	Description	Value
user-name	Specifies the SSH user name.	The value is a string of 1 to 64 case-insensitive characters without spaces. **NOTE** The string can contain spaces if it is enclosed with double quotation marks (").

Views

System view

Default Level

3: Management level

Usage Guidelines

You can create an SSH user in either of the following ways:

- Run the **ssh user** command.
- Run the **ssh user authentication-type**, **ssh user service-type**, or **ssh user sftp-directory** command with the user name you want to create. If the device

cannot find the user with the name you specified, it automatically creates the user.

Example

Create an SSH user named **testuser**.

```
<HUAWEI> system-view
[HUAWEI] ssh user testuser
```

2.6.69 ssh user assign

Function

The **ssh user assign** command assigns an existing public key to a user.

The **undo ssh user assign** command deletes the mapping between the user and public key.

By default, no public key is assigned to a user.

Format

ssh user *user-name* **assign** { **rsa-key** | **dsa-key** | **ecc-key** } *key-name*

undo ssh user *user-name* **assign** { **rsa-key** | **dsa-key** | **ecc-key** }

Parameters

Parameter	Description	Value
user-name	Specifies the SSH user name.	The value is a string of 1 to 64 case-insensitive characters without spaces. **NOTE** The string can contain spaces if it is enclosed with double quotation marks (").
rsa-key	Specifies an RSA public key.	-
dsa-key	Specifies a DSA public key.	-
ecc-key	Specifies an ECC public key.	-
key-name	Specifies the client public key name.	The value is a string of 1 to 30 characters.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an SSH client needs to log in to the SSH server in RSA, DSA, or ECC mode, run the **ssh user assign** command to assign a public key to the client. If the client has been assigned keys, the latest assigned key takes effect.

Precautions

The newly configured public key takes effect upon next login.

If the user named *user-name* to whom a public key is assigned does not exist, the device automatically creates an SSH user named *user-name* and performs the configured authentication for the SSH user.

To improve security, it is not recommended that you use RSA or DSA as the authentication algorithm.

Example

Assign key1 to the user named John.

```
<HUAWEI> system-view
[HUAWEI] ssh user john assign rsa-key key1
```

2.6.70 ssh user authorization-cmd aaa

Function

The **ssh user authorization-cmd aaa** command enables command line authorization for an SSH user.

The **undo ssh user authorization-cmd aaa** command restores the default authorization mode.

By default, command line authorization is disabled for an SSH user.

Format

ssh user *user-name* **authorization-cmd aaa**

undo ssh user *user-name* **authorization-cmd aaa**

Parameters

Parameter	Description	Value
user-name	Specifies the name of a valid SSH user defined by the AAA.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

The new setting for command line authorization takes effect upon next login.

This command is valid only for SSH users. The AAA configuration determines whether to configure an authorization mode for the users who log in using passwords.

Example

Enable command line authorization for the user named John.

```
<HUAWEI> system-view
[HUAWEI] ssh user john authorization-cmd aaa
Info: Please make sure that the command line authorization method has been set for the user.
```

2.6.71 ssh user authentication-type

Function

The **ssh user authentication-type** command configures an authentication mode for an SSH user.

The **undo ssh user authentication-type** command restores the default authentication mode for an SSH user.

By default, no authentication mode is configured for an SSH user.

Format

ssh user *user-name* **authentication-type** { **password** | **rsa** | **password-rsa** | **dsa** | **password-dsa** | **ecc** | **password-ecc** | **all** }

undo ssh user *user-name* **authentication-type**

Parameters

Parameter	Description	Value
user-name	Specifies an SSH user name.	The value is a string of 1 to 64 case-insensitive characters without spaces. **NOTE** The string can contain spaces if it is enclosed with double quotation marks (").
password	Specifies the password authentication mode.	-
rsa	Specifies the RSA authentication mode.	-
password-rsa	Specifies the password and RSA authentication modes.	-
dsa	Specifies the DSA authentication mode.	-
password-dsa	Specifies the password and DSA authentication modes.	-
ecc	Specifies the ECC authentication mode.	-
password-ecc	Specifies the password and ECC authentication modes.	-

Parameter	Description	Value
all	Specifies the password, ECC, DSA, or RSA authentication mode. **NOTE** In all authentication mode, the user priority depends on the authentication mode that the user selected. • If password authentication is selected, the user priority is the same as that specified on the AAA module. • If RSA/DSA/ECC authentication is selected, the user priority depends on the priority of the VTY interface used during user access. If all authentication is selected and an AAA user with the same name as the SSH user exists, user priorities may be different in password authentication and RSA, DSA, or ECC authentication modes. Set relevant parameters as needed.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you configure an authentication mode for an SSH user, if the user does not exist, a device automatically creates an SSH user named *user-name*.

Table 2-45 describes the usage scenarios for different authentication modes.

Table 2-45 Usage scenarios for authentication modes

Authentication Mode	Usage Scenario
RSA	It is a public key encryption architecture and an asymmetric encryption algorithm. RSA is mainly used to transmit the keys of the symmetric encryption algorithm, which improves encryption efficiency and simplify key management. The server checks whether the SSH user, public key, and digital user signature are valid. If all of them are valid, the user is permitted to access the server. If any of them is invalid, the authentication fails, and the user is denied to access the server.
DSA	It is same as RSA authentication in implementation. The server checks whether the SSH user, public key, and digital user signature are valid. If all of them are valid, the user is permitted to access the server. If any of them is invalid, the authentication fails, and the user is denied to access the server. Compared with RSA authentication, DSA authentication uses the digital signature algorithm for encryption and has a wider application scope. • Many SSH tools only support DSA authentication for servers and clients. • Based on the latest RFC recommendation for SSH, DSA authentication takes precedence over RSA authentication.

Authentication Mode	Usage Scenario
ECC	Like RSA authentication, the server first checks the validity of the SSH user and whether the public key and the numeric signature are valid. If all of them are consistent with those configured on the server, user authentication succeeds. If any of the three cannot pass authentication, the user access is denied. Compared with the RSA algorithm, the ECC authentication has the following advantages: ● Provides the same security with shorter key length. ● Features a shorter computing process and higher processing speed. ● Requires less storage space. ● Requires lower bandwidth.
password	On the server, the AAA module assigns each authorized user a password for login. The server has the mapping between user names and passwords. When a user requests to access the server, the server authenticates the user name and password. If either of them fails to be authenticated, the access request of the user is denied. The account information of users who are configured with the password authentication mode can be configured on devices or remote authentication servers (for example, RADIUS servers).
password-rsa, password-dsa, and password-ecc	The SSH server authenticates a client by checking both the public key and password. The client can be authenticated only when both the public key and password meet the requirement.
all	The SSH server authenticates a client by checking the public key or password. The client can be authenticated when either the public key or password meets the requirement.

Precautions

A new SSH user cannot log in to the SSH server unless being configured with an authentication mode. The newly configured authentication mode takes effect upon next login.

To improve security, it is not recommended that you use RSA or DSA as the authentication algorithm.

Example

Configure password authentication for the SSH user John.

```
<HUAWEI> system-view
[HUAWEI] ssh user john authentication-type password
```

2.6.72 ssh user service-type

Function

The **ssh user service-type** command configures a service type for an SSH user.

The **undo ssh user service-type** command restores the default service type for an SSH user.

By default, no service type is configured for an SSH user.

Format

ssh user *user-name* **service-type** { **sftp** | **stelnet** | **all** }

undo ssh user *user-name* **service-type**

Parameters

Parameter	Description	Value
user-name	Specifies the SSH user name.	The value is a string of 1 to 64 case-insensitive characters without spaces. **NOTE** The string can contain spaces if it is enclosed with double quotation marks (").
sftp	Specifies the SFTP service type.	-
stelnet	Specifies the STelnet service type.	-
all	Specifies the SFTP and STelnet service types.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure a service type for an SSH user, run the **ssh user service-type** command on a device. If the specified user does not exist, the device creates an SSH user who has the same name as the specified user and uses the configured service type for the SSH user.

Precautions

If the SFTP service type is configured for an SSH user, you need to run the **ssh user sftp-directory** command to set an authorized directory for the user. By default, the SFTP service authorized directory is flash: for the SSH user.

Example

Configure the **all** service type for an SSH user John.

```
<HUAWEI> system-view
[HUAWEI] ssh user john service-type all
```

2.6.73 stelnet

Function

The **stelnet** command enables a user to use the STelnet protocol to log in to another device from the current device.

Format

IPv4 address

stelnet [**-a** *source-address* | **-i** *interface-type interface-number*] *host-ip* [*port-number*] [[**-vpn-instance** *vpn-instance-name*] | [**identity-key** { **dsa** | **rsa** | **ecc** | **rsa_sha2_256** | **rsa_sha2_512** }] | [**user-identity-key** { **rsa** | **dsa** | **ecc** }] | [**prefer_kex** *prefer_key-exchange*] | [**prefer_ctos_cipher** *prefer_ctos_cipher*] | [**prefer_stoc_cipher** *prefer_stoc_cipher*] | [**prefer_ctos_hmac** *prefer_ctos_hmac*] | [**prefer_stoc_hmac** *prefer_stoc_hmac*] | [**-ki** *aliveinterval*] | [**-kc** *alivecountmax*]] *

IPv6 address

stelnet ipv6 [**-a** *source-address*] *host-ipv6* [**-oi** *interface-type interface-number*] [*port-number*] [[**identity-key** { **dsa** | **rsa** | **ecc** | **rsa_sha2_256** | **rsa_sha2_512** }] | [**user-identity-key** { **rsa** | **dsa** | **ecc** }] | [**prefer_kex** *prefer_key-exchange*] | [**prefer_ctos_cipher** *prefer_ctos_cipher*] | [**prefer_stoc_cipher** *prefer_stoc_cipher*] | [**prefer_ctos_hmac** *prefer_ctos_hmac*]

| [**prefer_stoc_hmac** *prefer_stoc_hmac*] | [**-ki** *aliveinterval*] | [**-kc** *alivecountmax*]] *

NOTE

Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6730-H, S6730S-H, S6730-S, and S6730S-S support **-a** *source-address* and **-i** *interface-type interface-number* parameter in the command.

Parameters

Parameter	Description	Value
-a *source-address*	Specifies the STelnet source IP address.	-
-i *interface-type interface-number*	Specifies the STelnet source interface. If the source interface is specified using **-i** *interface-type interface-number*, the **-vpn-instance** *vpn-instance-name* parameter is not supported.	-
host-ip	Specifies the IP address or host name of the remote IPv4 STelnet server.	The value is a string of 1 to 255 case-insensitive characters without spaces.
host-ipv6	Specifies the IPv6 address or host name of the remote IPv6 STelnet server.	The value is a string of 1 to 255 case-insensitive characters without spaces.
-oi *interface-type interface-number*	Specifies the outbound interface on the local device.	If the IPv6 address of the remote host is linked to a local address, the outbound interface must be specified.
port-number	Specifies the port number that the SSH server is listening on.	The value is an integer that ranges from 1 to 65535. The default value 22 is the standard port number.

Parameter	Description	Value
identity-key	Specifies the public key for server authentication.	The public key algorithm includes dsa, rsa, rsa_sha2_256, rsa_sha2_512 and ecc. By default, the server authentication uses the ECC public key. **NOTE** To improve security, it is not recommended that you use RSA or DSA as the authentication algorithm.
user-identity-key	Specifies the public key algorithm for the client authentication.	The public key algorithm includes dsa, rsa, and ecc. By default, the client authentication uses the RSA public key. **NOTE** To improve security, it is not recommended that you use RSA or DSA as the authentication algorithm.
prefer_kex *prefer_key-exchange*	Indicates the preferred key exchange algorithm.	Specifies the preferred key exchange algorithm. The **dh_exchange_group**, **dh_exchange_group_sha256**, **dh_group14_sha1**, **dh_group14_sha256**, **dh_group15_sha512**, and **dh_group16_sha512** algorithms are supported currently. The default key exchange algorithm is dh_group14_sha1.

Parameter	Description	Value
prefer_ctos_cipher *prefer_ctos_cipher*	Specifies the preferred encryption algorithm from the client to the server. The 3des, aes128, aes256, aes128_ctr, and aes256_ctr algorithms are supported currently.	The default algorithm is aes256_ctr. To improve security, it is recommended that you use aes128_ctr and aes256_ctr algorithms. **NOTE** • If an encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select an encryption algorithm from the list. • If no encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select one from **3des**, **aes128**, **aes256**, **aes128_ctr**, and **aes256_ctr**.
prefer_stoc_cipher *prefer_stoc_cipher*	Specifies the preferred encryption algorithm from the server to the client. The 3des, aes128, aes256, aes128_ctr, and aes256_ctr algorithms are supported currently.	The default algorithm is aes256_ctr. To improve security, it is recommended that you use aes128_ctr and aes256_ctr algorithms. **NOTE** • If an encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select an encryption algorithm from the list. • If no encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select one from **3des**, **aes128**, **aes256**, **aes128_ctr**, and **aes256_ctr**.

Parameter	Description	Value
prefer_ctos_hmac *prefer_ctos_hmac*	Specifies the preferred HMAC algorithm from the client to the server. The sha1, sha1_96, md5, md5_96, sha2_256, and sha2_256_96 algorithms are supported currently.	The default algorithm is sha2_256. To improve security, it is recommended that you use sha2_256 algorithms.
prefer_stoc_hmac *prefer_stoc_hmac*	Specifies the preferred HMAC algorithm from the server to the client. The sha1, sha1_96, md5, md5_96, sha2_256, and sha2_256_96 algorithms are supported currently.	The default algorithm is sha2_256. To improve security, it is recommended that you use sha2_256 algorithms.
-vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the server belongs.	The value must be an existing VPN instance name.
-ki *aliveinterval*	Specifies the interval for sending keepalive packets when no packet is received.	The value is an integer that ranges from 1 to 3600, in seconds.
-kc *alivecountmax*	Specifies the number of times for no reply of keepalive packets.	The value is an integer that ranges from 3 to 10. The default value is 5.

Views

System view

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

Logins through Telnet bring security risks because Telnet does not provide any authentication mechanism and data is transmitted using TCP in plain text. Compared with Telnet, SSH guarantees secure file transfer on a traditional insecure network by authenticating clients and encrypting data in bidirectional mode. The SSH protocol supports STelnet. You can run this command to use STelnet to log in to another device from the current device.

STelnet is a secure Telnet service. SSH users can use the STelnet service in the same way as the Telnet service.

When a fault occurs in the connection between the client and server, the client needs to detect the fault in real time and proactively release the connection. You

need to set the interval for sending keepalive packets and the maximum number of times on the client that logs in to the server through STelnet.

- Interval for sending keepalive packets: If a client does not receive any packet within the specified interval, the client sends a keepalive packet to the server.
- Maximum number of times the server has no response: If the number of times that the server does not respond exceeds the specified value, the client proactively releases the connection.

Precautions

- Before connecting the SSH server using the **STelnet** command, run the **stelnet server enable** command to enable the STelnet service on the SSH server.
- If the server is listening on port 22, the SSH client can log in to the SSH server with no port specified. If the server is listening on another port, the port number must be specified upon login.

Example

Set keepalive parameters when a client logs in to a server through STelnet.

```
<HUAWEI> system-view
[HUAWEI] stelnet 10.164.39.209 -ki 10 -kc 4
```

Remotely connect to the STelnet server that uses an IPv6 address.

```
<HUAWEI> system-view
[HUAWEI] stelnet ipv6 fc00:2001:db8::1 prefer_ctos_cipher aes128
```

2.6.74 stelnet server enable

Function

The **stelnet server enable** command enables the STelnet service on an SSH server.

The **undo stelnet server enable** command disables the STelnet service on an SSH server.

By default, the STelnet service is disabled on SSH servers.

Format

stelnet [**ipv4** | **ipv6**] **server enable**

undo stelnet [**ipv4** | **ipv6**] **server enable**

Parameters

Parameter	Description	Value
ipv4	Configures a device as the STelnet IPv4 server.	-
ipv6	Configure a device as the STelnet IPv6 server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To connect a client to an SSH server through STelnet, you must enable the STelnet service on the SSH server.

Prerequisites

Before enabling the STelnet service, run either of the following commands as required:

- Run the **ssh server-source -i** *interface-type interface-number* command to configure a specified interface as the source interface of the SSH server or run the **ssh server-source all-interface** command to specify any interface with an IPv4 address configured on the device as the source interface of the SSH server.
- Run the **ssh ipv6 server-source -a** *ipv6_address* [**-vpn-instance** *vpn_name*] command to configure a specified IPv6 address as the IPv6 source address of the SSH server or run the **ssh ipv6 server-source all-interface** command to specify any interface IPv6 address on the device as the IPv6 source address of the SSH server.

Precautions

After you disable the STelnet service on the SSH server, all clients that have logged in through STelnet are disconnected.

After the **stelnet server enable** command is run, the numbers of IPv4 port and IPv6 port are both changed. To change the IPv4 or IPv6 port number separately, run the **stelnet** { **ipv4** | **ipv6** } **server enable** command.

Example

Enable the STelnet service.

```
<HUAWEI> system-view
[HUAWEI] stelnet server enable
```

Enable the STelnet IPv4 service.

```
<HUAWEI> system-view
[HUAWEI] stelnet ipv4 server enable
```

2.6.75 super

Function

The **super** command changes the user's current privilege level.

User privilege level indicates the type of the login user. There are 16 user privilege levels. Different from the use of command privilege level, a login user can only use the commands with the levels no higher than the user privilege level.

Format

super [*level*]

Parameters

Parameter	Description	Value
level	Specifies the user privilege level.	The value is an integer ranging from 0 to 15. By default, the level is 3.

Views

User view

Default Level

0: Visit level

Usage Guidelines

User privilege level indicates the type of the login user. There are 16 user privilege levels. Different from the use of command privilege level, a login user can only use the commands with the privilege levels no higher than the user privilege level.

In order to prevent unauthorized users from illegal intrusion, user ID authentication is performed when users at a lower level switch to users at a higher level. In other word, the password of the higher level is needed. You can run the **super password** command to set the password for changing the user from a lower level to a higher level.

For the sake of confidentiality, the password the user inputs is not shown on the screen. The user can switch to the higher level only when inputting the correct password within three times. Otherwise, the original user privilege level remains unchanged.

The passwords must meet the following requirements:

- The password is a string of 8 to 16 case-sensitive characters.
- The password must contain at least two of the following characters: upper-case character, lower-case character, digit, and special character. Special character except the question mark (?) and space.

NOTICE

Huawei switches use the combination of user name, password, and level to control users' operation rights. If you use the super command to switch user privilege levels, this right control method will become invalid. Moreover, any user can use the super password of a higher level to obtain high-level operation rights. Therefore, you are not advised to use the super command to switch user privilege levels.

Example

Enable the user to switch to level 3.

```
<HUAWEI> super 3
Password:
Now user privilege is 3 level, and only those commands whose level is equal to or less than this level can be used.
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
```

2.6.76 super password

Function

The **super password** command sets the password for switching a user from a lower level to a higher level.

The **undo super password** command deletes the password for switching a user from a lower level to a higher level.

By default, no password is configured for switching a user from a lower level to a higher level. A password must be configured for switching a user from a lower level to a higher level. Otherwise, the switching fails.

Format

super password [**level** *user-level*] [**cipher** *password*]

undo super password [**level** *user-level*]

Parameters

Parameter	Description	Value
level *user-level*	Specifies the user privilege level that needs to be changed.	The value is an integer that ranges from 1 to 15. By default, the system sets a password for a user that switches to level 3.

Parameter	Description	Value
cipher *password*	Specifies the password for changing a level.	• When **cipher** is not entered, password input is in man-machine interaction mode, and the system does not display the entered password. The password is a string of 8 to 16 case-sensitive characters. The password must contain at least two of the following characters: upper-case character, lower-case character, digit, and special character. Question mark (?) and space characters are not supported. • When **cipher** is entered, the password is displayed in either simple or ciphertext mode during input. – When being input in simple mode, the password requirements are the same as those when **cipher** is not entered. – When being input in ciphertext, the password must be a string of 56 consecutive characters. **NOTE** If the source version supports a ciphertext password which is a string of 24 or 32 characters, the target version also supports this type of password. When setting the password for switching the user privilege level, if the current user privilege level is higher than the specified user privilege level and the password exists, the old password does not need to be verified. If the current user privilege level is lower than the specified user privilege level, enter the correct old password; otherwise, the configuration will fail. The password is displayed in ciphertext in the configuration file regardless of whether it is input in simple or ciphertext mode.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If users' rights are redefined, users need to run the **super** command to change their levels from low to high. For safety, users need to be authenticated when they

change their levels. Users can run the **super password** command to set the password of changing their levels from low to high for authentication.

Precautions

- The password entered by a user is saved in ciphertext, irrespective of whether **cipher** is specified. Therefore, if the password is lost, you cannot get it back.
- Users can press **Ctrl+C** to cancel the operation when they run the **super password**.
- When a user with a level lower than the level configured using this command queries the password configured using the **display this** or **display current-configuration** command, the password is displayed as asterisks (******).

Example

Set the password **Abcd@123** for switching a user from a lower level to level 3, with **cipher** configured for the password.

```
<HUAWEI> system-view
[HUAWEI] super password level 3 cipher Abcd@123
Info: The password will be changed, please verify the old password.
Please enter old password:
Info: The password is changed successfully.
```

Set the password **Abcd@123** for switching a user from a lower level to level 3, with **cipher** not configured for the password.

```
<HUAWEI> system-view
[HUAWEI] super password level 3
Please configure the login password (8-16)
Enter Password:
Confirm Password:
Info: The password will be changed, please verify the old password.
Please enter old password:
Info: The password is changed successfully.
```

2.6.77 super password complexity-check disable

Function

The **super password complexity-check disable** command disables password complexity check when a low-level user is switched to a high-level user.

The **undo super password complexity-check disable** command enables password complexity check when a low-level user is switched to a high-level user.

By default, password complexity check is enabled when a low-level user is switched to a high-level user.

Format

super password complexity-check disable

undo super password complexity-check disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device has the following requirements for the password for switching a low-level user to a high-level user:

- By default, the minimum password length is eight characters. If the password length set by the **set password min-length** command exceeds eight characters, the value set by this command is the minimum password length.
- A password must contain two or more types of characters, such as upper-case letters, lower-case letters, digits, and special characters.

  The special characters exclude question marks (?) and spaces.

To ensure security of the password for switching a low-level user to a high-level user, run the **undo super password complexity-check disable** command to enable password complexity check. In this case, if a specified password fails the password complexity check, the configuration does not take effect. In a scenario where high security is not required, run the **super password complexity-check disable** command to disable password complexity check.

Precautions

If password complexity check is disabled when a low-level user is switched to a high-level user, a simple password will bring security risks.

Example

Disable password complexity check when a low-level user is switched to a high-level user.

```
<HUAWEI> system-view
[HUAWEI] super password complexity-check disable
```

2.6.78 telnet

Function

The **telnet** command enables a user to use the Telnet protocol to log in to another device from the current device.

Format

Log in to another device through Telnet based on IPv4.

telnet [**vpn-instance** *vpn-instance-name*] [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *host-ip* [*port-number*]

Log in to another device through Telnet based on IPv6.

telnet ipv6 [**-a** *source-ip-address*] [**vpn6-instance** *vpn6-instance-name*] *host-ipv6* [**-oi** *interface-type interface-number*] [*port-number*]

(Only S5720I-SI, S5720-LI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support **vpn6-instance** *vpn6-instance-name*.)

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the VPN4 instance name of the device to log in through Telnet.	The value must be an existing VPN instance name.
-a *source-ip-address*	Specifies a source IP address through which a server communicates with the device. This improves security. If no source address is specified, a device will use the IP address of the local outbound interface to initiate a Telnet connection.	-
-i *interface-type interface-number*	Specifies the source interface type and number on the local device.	-
vpn6-instance *vpn6-instance-name*	Specifies the name of the VPN6 instance to which the login device belongs.	The value must be an existing VPN instance name.
host-ip	Specifies the IPv4 address or host name of the remote device.	The value is a string of 1 to 255 case-insensitive characters without spaces. **NOTE** The string can contain spaces if it is enclosed with double quotation marks (").

Parameter	Description	Value
host-ipv6	Specifies the IPv6 address or host name of the remote device.	The value is a string of 1 to 255 case-insensitive characters without spaces. **NOTE** The string can contain spaces if it is enclosed with double quotation marks (").
-oi *interface-type interface-number*	Specifies the outbound interface on the local device.	If the IPv6 address of the remote host is linked to a local address, the outbound interface must be specified.
port-number	Specifies the number of the TCP port that is used by the remote device to provide the Telnet service.	The value is an integer that ranges from 1 to 65535. The default value is 23.

Views

User view

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

If multiple devices on a network need to be configured and managed, run the **telnet** command to log in to these devices from your terminal for remote device configuration, facilitating device management.

You can press **Ctrl+K** to terminate an active connection between the local and remote devices.

Precautions

- Before you run the **telnet** command to connect to the Telnet server, the Telnet client and server must be able to communicate at Layer 3 and the Telnet service must be enabled on the Telnet server.
- Logins through Telnet bring security risks because Telnet does not provide any authentication mechanism and data is transmitted using TCP in plain text. The STelnet mode is recommended for networks that have high security requirements.

Example

Connect to a remote device through Telnet.

```
<HUAWEI> telnet 192.168.1.6
```

Use the IPv6 address to connect to a remote device through Telnet.

```
<HUAWEI> telnet ipv6 fc00:0:0:11::158
```

2.6.79 telnet client-source

Function

The **telnet client-source** command specifies a source IP address or source interface for a Telnet client.

The **undo telnet client-source** command restores the default settings.

The default source IP address of a Telnet client is 0.0.0.0, and there is no default source interface.

Format

telnet client-source { **-a** *source-ip-address* | **-i** *interface-type interface-number* }

undo telnet client-source

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the IPv4 address of the local switch.	-
-i *interface-type interface-number*	Specifies the source interface of the local switch.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the source IP address is not specified in the **telnet** command, the source IP address specified using the **telnet client-source** is used. If a source IP address is specified in the **telnet** command, the specified setting is used. Check the current Telnet connection on the server. The IP address displayed is the specified source IP address or the primary IP address of the specified interface.

Prerequisites

The source interface specified using the command must exist and have an IP address configured.

Example

Set the source IP address of the Telnet client to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] telnet client-source -a 10.1.1.1
```

2.6.80 telnet server acl

Function

The **telnet server acl** command configures an ACL to control the access of clients to the Telnet server.

The **undo telnet server acl** command cancels the configuration of the ACL.

By default, no ACL is configured for Telnet servers.

Format

telnet [**ipv6**] **server acl** *acl-number*

undo telnet [**ipv6**] **server acl**

Parameters

Parameter	Description	Value
ipv6	Specifies a Telnet IPv6 server.	-
acl-number	Specifies an ACL number.	The value is an integer that ranges from 2000 to 3999.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a device functions as a Telnet server, configure an ACL on the device to control the login of the clients to the device.

Prerequisites

An ACL has been configured using the **acl (system view)** command in the system view, and an ACL rule has been configured using the **rule (basic ACL view)** or **rule (advanced ACL view)** command.

Precautions

None.

Example

Configure ACL 2000 on a Telnet server.

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule permit source 10.1.1.1 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] telnet server acl 2000
```

2.6.81 telnet server-source

Function

The **telnet server-source** command specifies a source interface for a Telnet server.

The **undo telnet server-source** command restores the default setting.

By default, the source interface of a Telnet server is not specified.

Format

telnet server-source -i *interface-type interface-number*

undo telnet server-source

telnet server-source all-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the source interface of the local device.	-
all-interface	Indicates that any interface that has an IPv4 address configured can be used as the source interface of a Telnet server.	-

NOTE

In V200R020C00 and later versions, a Telnet server does not accept login connection requests from any interface by default. To allow authorized users to log in to the server, run a command to specify the source interface or source address of the server. For details about the command, see "Usage Scenario" in "Usage Guidelines" in this section.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In versions earlier than V200R020C00, a Telnet server receives connection requests from all interfaces by default, incurring security risks. For details, see the product documentation of the corresponding version.

In V200R020C00 and later versions, a Telnet server does not accept login requests from any interface by default. To allow authorized users to log in to the Telnet server, run either of the following commands to specify the source interface of the Telnet server.

- Run the **telnet server-source -i** *interface-type interface-number* command to configure a specified interface as the source interface of the Telnet server.
- Run the **telnet server-source all-interface** command to configure all interfaces configured with IPv4 addresses as the source interfaces of the Telnet server.

Prerequisites

Before you specify a logical interface as the source interface, ensure that the interface to be specified is created and has an IP address configured. Before you specify a physical interface as the source interface, ensure that the interface has an IPv4 address configured. Otherwise, the **telnet server-source** command cannot be successfully executed.

Precautions

By default, no source interface is specified for an SSH server.

After the source interface is specified, a device allows Telnet users to log in to the Telnet server only through this source interface, and Telnet users logging in through other interfaces are denied. Note that setting this parameter only affects Telnet users who attempt to log in to the Telnet server, and it does not affect Telnet users who have logged in to the server.

After the source interface of a Telnet server is specified using this command, ensure that Telnet users can access the source interface at Layer 3. Otherwise, the Telnet users will fail to log in to the Telnet server.

No source address or source interface is specified, so security risks exist.

After the **telnet server-source all-interface** command is run, the system allows Telnet users to log in to the Telnet server through all interfaces with IPv4 addresses configured. This increases system security risks. Therefore, you are not advised to run this command.

Example

Specify loopback0 as the source interface of the Telnet server.

```
<HUAWEI> system-view
[HUAWEI] interface loopback 0
```



```
[HUAWEI-LoopBack0] ip address 10.1.1.1 24
[HUAWEI-LoopBack0] quit
[HUAWEI] telnet server-source -i loopback 0
```

2.6.82 telnet ipv6 server-source

Function

The **telnet ipv6 server-source** command specifies an IPv6 source address for a Telnet server.

The **undo telnet ipv6 server-source** command cancels the IPv6 source address specified for a Telnet server.

By default, the IPv6 source address of a Telnet server is not specified.

Format

telnet ipv6 server-source -a *ipv6_address* [**vpn-instance** *vpn_name*]

undo telnet ipv6 server-source

telnet ipv6 server-source all-interface

Parameters

Parameter	Description	Value
-a *ipv6_address*	Specifies the IPv6 source address for a Telnet server.	The total length of an IPv6 address is 128 bits, which are divided into eight groups. Each group contains four hexadecimal digits. The value is in the format X:X:X:X:X:X:X:X.
vpn-instance *vpn_name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain spaces. The VPN instance name cannot be _**public**_. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
all-interface	Indicates that any interface IPv6 address on the device can be used as the IPv6 source address of the Telnet server.	-

NOTE

In V200R020C00 and later versions, a Telnet server does not accept login connection requests from any IPv6 address by default. To allow authorized users to log in to the server, run a command to specify the source interface or source address of the server. For details about the command, see "Usage Scenario" in "Usage Guidelines" in this section.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In versions earlier than V200R020C00, a Telnet server accepts connection requests from all IPv6 addresses by default, incurring security risks. For details, see the product documentation of the corresponding version.

In V200R020C00 and later versions, a Telnet server does not accept login requests from any IPv6 address by default. To allow authorized users to log in to the Telnet server, run either of the following commands to specify an IPv6 source address for the Telnet server.

- Run the **telnet ipv6 server-source -a** *ipv6_address* [**vpn-instance** *vpn_name*] command to configure the specified IPv6 address as the IPv6 source address of the Telnet server.
- Run the **telnet ipv6 server-source all-interface** command to configure all interface IPv6 addresses on the device as the IPv6 source addresses of the Telnet server.

Prerequisites

A VPN instance has been created before you specify it for a Telnet server. Otherwise, the **telnet ipv6 server-source** command cannot be executed.

Configuration Impact

After an IPv6 source address is specified for a Telnet server, Telnet users can log in to the Telnet server only using this IPv6 address. This configuration applies to the Telnet users who attempt to log in to the server, not to the Telnet users who have logged in to the server.

Precautions

After this command is run, the new configuration takes effect upon the next login.

After an IPv6 source address is specified for a Telnet server using this command, ensure that Telnet users can access this IPv6 address at Layer 3. Otherwise, Telnet users will fail to log in to the Telnet server.

If the specified IPv6 source address is bound to a VPN instance, the Telnet server is also bound to the VPN instance.

After the **telnet ipv6 server-source all-interface** command is run, the system allows Telnet users to log in to the Telnet server through all interfaces with IPv6 addresses configured. This increases system security risks. Therefore, running this command is not recommended.

Example

Specify the IPv6 source address 2001:DB8:: for a Telnet server.

```
<HUAWEI> system-view
[HUAWEI] telnet ipv6 server-source -a 2001:DB8::
```

2.6.83 telnet server enable

Function

The **telnet server enable** command enables the Telnet service.

The **undo telnet server enable** command disables the Telnet service.

The **telnet server disable** command disables the Telnet service.

By default, the Telnet service is disabled.

Format

telnet [**ipv6**] **server enable**

undo telnet [**ipv6**] **server enable**

telnet [**ipv6**] **server disable**

Parameters

Parameter	Description	Value
ipv6	Specifies a Telnet IPv6 server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **telnet server enable** command to enable the Telnet service. A Telnet server can be connected only when it is enabled.

Prerequisites

Before enabling the Telnet service, run either of the following commands as required:

- Run the **telnet server-source -i** *interface-type interface-number* command to configure a specified interface as the source interface of the Telnet server or run the **telnet server-source all-interface** command to specify any interface with an IPv4 address configured on the device as the source interface of the Telnet server.
- Run the **telnet ipv6 server-source -a** *ipv6_address* [**-vpn-instance** *vpn_name*] command to configure a specified IPv6 address as the IPv6 source address of the Telnet server or run the **telnet ipv6 server-source all-interface** command to specify any interface IPv6 address on the device as the IPv6 source address of the Telnet server.

Precautions

If the user who logged in to the server through Telnet is online, the **undo telnet** [**ipv6**] **server enable** command fails to be run on the server.

When a Telnet server is disabled, you can log in to the device only through the console port or SSH.

NOTICE

The Telnet protocol poses a security risk, and therefore using STelnet V2 is recommended.

Example

Enable the Telnet service.

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

Disable the Telnet service.

```
<HUAWEI> system-view
[HUAWEI] undo telnet server enable
```

Enable the IPv6 Telnet service.

```
<HUAWEI> system-view
[HUAWEI] telnet ipv6 server enable
```

2.6.84 telnet server port

Function

The **telnet server port** command configures a listening port number for a Telnet server.

The **undo telnet server port** command restores the default listening port of a Telnet server.

The default listening port of a Telnet server is 23.

Format

telnet server port *port-number*

undo telnet server port

Parameters

Parameter	Description	Value
port-number	Specifies the listening port number of a Telnet server.	The value is an integer that is 23 or ranges from 1025 to 55535. The default value 23 is the standard Telnet server port number.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To prevent attackers from attacking the standard Telnet listening port number, run the **telnet server port** command to configure a new listening port. This improves security.

Precautions

If the server is listening on port 23, the Telnet client can log in successfully with no port specified. If the server is listening on another port, the port number must be specified.

Before changing the current port number, disconnect all devices from the port. After the port number is changed, the server starts to listen on the new port.

Example

Set the listening port number to 1026.

```
<HUAWEI> system-view
[HUAWEI] telnet server port 1026
```

Restore the listening port number to the default value.

```
<HUAWEI> system-view
[HUAWEI] undo telnet server port
```

2.7 File Management Commands

2.7.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

2.7.2 ascii

Function

The **ascii** command sets the file transfer mode to ASCII on an FTP client.

The default file transfer mode is ASCII.

Format

ascii

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Files can be transferred in ASCII or binary mode.

ASCII mode is used to transfer plain text files, and binary mode is used to transfer application files, such as system software, images, video files, compressed files, and database files.

Example

Set the file transfer mode to ASCII.

```
<HUAWEI> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] ascii
200 Type set to A.
```


2.7.3 binary

Function

The **binary** command sets the file transfer mode to binary on an FTP client.

The default file transfer mode is ASCII.

Format

binary

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Files can be transferred in ASCII or binary mode.

ASCII mode is used to transfer plain text files, and binary mode is used to transfer application files, such as system software, images, video files, compressed files, and database files.

Example

Set the file transfer mode to binary.

```
<HUAWEI> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[ftp] binary
200 Type set to I
```

2.7.4 binding cipher-suite-customization

Function

The **binding cipher-suite-customization** command binds a customized SSL cipher suite policy to an SSL policy.

The **undo binding cipher-suite-customization** command unbinds the customized SSL cipher suite policy from an SSL policy.

By default, no customized cipher suite policy is bound to an SSL policy. Each SSL policy uses a default cipher suite.

Format

binding cipher-suite-customization *customization-policy-name*

undo binding cipher-suite-customization

Parameters

Parameter	Description	Value
customization-policy-name	Specifies the name of a customized SSL cipher suite policy.	The value is a string of 1 to 32 case-insensitive characters, spaces not supported.

Views

SSL policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To bind a customized SSL cipher suite policy to an SSL policy, run the **binding cipher-suite-customization** command. After a customized SSL cipher suite policy is bound to an SSL policy, the device uses an algorithm in the specified cipher suite to perform SSL negotiation.

After a customized cipher suite policy is unbound from an SSL policy, the SSL policy uses one of the following cipher suites supported by default:

- tls1_ck_rsa_with_aes_256_sha
- tls1_ck_rsa_with_aes_128_sha
- tls1_ck_dhe_rsa_with_aes_256_sha
- tls1_ck_dhe_dss_with_aes_256_sha
- tls1_ck_dhe_rsa_with_aes_128_sha
- tls1_ck_dhe_dss_with_aes_128_sha
- tls12_ck_rsa_aes_256_cbc_sha256

Prerequisites

The customized cipher suite policy to be bound to an SSL policy contains cipher suites.

Precautions

If the cipher suite in the customized cipher suite policy bound to an SSL policy contains only one type of algorithm (RSA or DSS), the corresponding certificate must be loaded for the SSL policy to ensure successful SSL negotiation.

Example

Bind customized SSL cipher suite policy named **cipher1** to an SSL policy.

```
<HUAWEI> system-view
[HUAWEI] ssl policy ftp_server
[HUAWEI-ssl-policy-ftp_server] binding cipher-suite-customization cipher1
```

2.7.5 bye

Function

The **bye** command terminates the connection with the remote FTP server and enters the user view.

Format

bye

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

This command is equivalent to the **quit** command.

You can use the **close** and **disconnect** commands to terminate the connection with the remote FTP server and retain the FTP client view.

Example

Terminate the connection with the remote FTP server and enter the user view.

```
<HUAWEI>ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] bye
```



```
221 server closing.
<HUAWEI>
```

2.7.6 cd (FTP client view)

Function

The **cd** command changes the working directory of the FTP server.

Format

cd *remote-directory*

Parameters

Parameter	Description	Value
remote-directory	Specifies the name of a working directory on the FTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

The FTP server authorizes users to access files in certain directories and their subdirectories.

Example

Change the working directory to **d:/temp**.

```
<HUAWEI>ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] cd d:/temp
250 "D:/temp" is current directory.
```


2.7.7 cd (SFTP client view)

Function

The **cd** command changes the working directory of the SFTP server.

Format

cd [*remote-directory*]

Parameters

Parameter	Description	Value
remote-directory	Specifies the name of a directory on the SFTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

- The SFTP server authorizes users to access files in certain directories and their subdirectories.
- The specified working directory must exist on the SFTP server. If the *remote-directory* parameter is not included in the **cd** command, only the current working directory of an SSH user is displayed as the command output.

Example

Change the current working directory of the SFTP server to /bill.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> cd bill
Current directory is:
/bill
```

2.7.8 cd (user view)

Function

The **cd** command changes the current working directory of a user.

By default, the current working directory is flash:.

Format

cd *directory*

Parameters

Parameter	Description	Value
directory	Specifies the current working directory of a user.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] path** format. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' " For example, a directory name is flash:/selftest/test/.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the drive name.

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.

- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

For example, if you change the current working directory flash:/selftest/ to the logfile directory in flash, the absolute path is flash:/logfile/, and the relative path is /logfile/. The logfile directory is not **logfile/** because it is not in the current working directory **selftest**.

Precautions

- The directory specified in the **cd** command must exist; otherwise, the error messages will be displayed:

  You can perform the following operations to rectify faults:

  a. Run the **pwd** command to view the current working directory.
  b. Run the **dir** command to view the current working directory and verify that the directory specified in the **cd** command exists.

Example

Change the current working directory from flash:/temp to flash:.

```
<HUAWEI> pwd
flash:/temp
<HUAWEI> cd flash:
<HUAWEI> pwd
flash:
```

Change the current working directory from flash: to flash:/t1/t2.

```
<HUAWEI> pwd
flash:
<HUAWEI> cd flash:/t1/t2
<HUAWEI> pwd
flash:/t1/t2
```

Change the current working directory from flash:/selftest to flash:/logfile.

```
<HUAWEI> pwd
flash:/selftest
<HUAWEI> cd /logfile/
<HUAWEI> pwd
flash:/logfile
```

Change the current working directory from flash:/selftest to flash:/selftest/test.

```
<HUAWEI> pwd
flash:/selftest
<HUAWEI> cd test/
<HUAWEI> pwd
flash:/selftest/test
```

2.7.9 cdup (SFTP client view)

Function

The **cdup** command changes the current working directory of an SSH user to its parent directory.

Format

cdup

Parameters

None

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **cdup** command to change the current working directory to its parent directory.

Precautions

If the current working directory is the SFTP authorization directory, the command cannot change the current working directory.

Example

Change the current working directory to its parent directory.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> cd dhcp
Current directory is:
/dhcp
sftp-client> cdup
Current directory is:
/
sftp-client> cdup
Error: Failed to change the current directory.
sftp-client>
```

2.7.10 cdup (FTP client view)

Function

The **cdup** command enables you to return to the upper-level directory.

Format

cdup

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To exit from the current directory and return to the upper-level directory, run the **cdup** command.

Precautions

The directories accessible to an FTP user are restricted by the authorized directories configured for the user.

Example

Exit from the current directory and return to the upper-level directory.

```
<HUAWEI>ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] cd security
250 CWD command successfully.
[ftp] cdup
200 CDUP command successfully.
```

2.7.11 certificate load

Function

The **certificate load** command loads a digital certificate for a Secure Sockets Layer (SSL) policy.

The **undo certificate load** command unloads a digital certificate for the SSL policy.

By default, no digital certificate is loaded for an SSL policy.

Format

Load a PEM digital certificate for an SSL policy.

certificate load pem-cert *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename* **auth-code cipher** *auth-code*

Load an ASN1 digital certificate for an SSL policy.

certificate load asn1-cert *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename*

Load a PFX digital certificate for an SSL policy.

certificate load pfx-cert *cert-filename* **key-pair** { **dsa** | **rsa** } { **mac cipher** *mac-code* | **key-file** *key-filename* } **auth-code cipher** *auth-code*

Load a PEM certificate chain for an SSL policy.

certificate load pem-chain *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename* **auth-code cipher** *auth-code*

Unload a digital certificate for an SSL policy.

undo certificate load

Parameters

Parameter	Description	Value
pem-cert	Loads a PEM digital certificate for the SSL policy. A PEM digital certificate has a file name extension .pem. A PEM digital certificate transfers text data between systems.	-
cert-filename	Specifies the name of a certificate file. The file is in the subdirectory of the system directory **security**. If the **security** directory does not exist in the system, create this directory.	The value is a string of 1 to 64 characters. The file name is the same as that of the uploaded file.
key-pair	Specifies the key pair type.	-
dsa	Sets the key pair type to DSA.	-
rsa	Sets the key pair type to RSA.	-

Parameter	Description	Value
key-file *key-filename*	Specifies the key pair file. The file is in the subdirectory of the system directory **security**. If the **security** directory does not exist in the system, create this directory.	The value is a string of 1 to 64 characters. The file name is the same as that of the uploaded file.
auth-code cipher *auth-code*	Specifies the authentication code of the key pair file. The authentication code verifies user identity to ensure that only authorized clients access the server.	The value is a string of case-sensitive characters without spaces. If the value begins and ends with double quotation marks (" "), the string of characters can contain spaces. When the value is displayed in plaintext, its length ranges from 1 to 31. When the value is displayed in ciphertext, its length is 48 or 68. A ciphertext password with the length of 32 or 56 characters is also supported.
asn1-cert	Loads an ASN1 digital certificate for the SSL policy. An ASN1 digital certificate has a file name extension .der. By default, most browsers support the ASN1 digital certificate.	-
pfx-cert	Loads a PFX digital certificate for the SSL policy. A PFX digital certificate has a file name extension .pfx. A digital certificate can be converted from the PFX format to another format.	-

Parameter	Description	Value
mac cipher *mac-code*	Specifies a message authentication code. The message authentication code ensures the packet data reliability and security.	The value is a string of case-sensitive characters without spaces. If the value begins and ends with double quotation marks (" "), the string of characters can contain spaces. When the value is displayed in plaintext, its length ranges from 1 to 31. When the value is displayed in ciphertext, its length is 48 or 68. A ciphertext password with the length of 32 or 56 characters is also supported.
pem-chain	Specifies a PEM certificate chain.	-

Views

SSL policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

SSL security mechanism includes:

- Data transmission security: Uses the symmetric key algorithm to encrypt data.
- Message integrity: uses the multiplexed analog component (MAC) algorithm to ensure message integrity.
- Identity authentication mechanism: authenticates users based on the digital signatures and certificates.

The Certificate Authority (CA) issues PEM, ASN1, and PFX digital certificates that provide user identity information. Based on digital certificates, users establish trust relationships with partners who require high security.

A digital certificate data includes the applicant information such as the applicant's name, applicant's public key, digital signature of the CA that issues the certificate, and the certificate validity period. The CA can issue a certificate chain along with the digital certificate. After receiving a certificate chain, the receiver owns all the certificates on the chain.

Prerequisites

The **ssl policy** command has been run in the system view to create an SSL policy.

Precautions

You can load a certificate or certificate chain for only one SSL policy. Before loading a certificate or certificate chain, you must unload the existing certificate or certificate chain.

To ensure security, the device automatically saves the key file in the system and deletes the file from the storage medium after a certificate is successfully loaded. It is recommended that you do not delete a certificate or certificate chain that has been successfully loaded; otherwise, services using the SSL policy will be affected.

For device that supports the NOR flash, after the certificate is loaded, the key pair file is stored in the NOR flash, and the file in the **security** directory is deleted. After the SSL policy is deleted, the file in the NOR flash is deleted. To re-load the certificate, upload the key file again.

Example

Load an ASN1 digital certificate for the SSL policy.

```
<HUAWEI> system-view
[HUAWEI] ssl policy ftp_server
[HUAWEI-ssl-policy-ftp_server] certificate load asn1-cert servercert.der key-pair dsa key-file serverkey.der
```

Load a PEM digital certificate for the SSL policy.

```
<HUAWEI> system-view
[HUAWEI] ssl policy ftp_server
[HUAWEI-ssl-policy-ftp_server] certificate load pem-cert servercert.pem key-pair dsa key-file serverkey.pem auth-code cipher YsHsjx_202206
```

Load a PFX digital certificate for the SSL policy.

```
<HUAWEI> system-view
[HUAWEI] ssl policy http_server
[HUAWEI-ssl-policy-http_server] certificate load pfx-cert servercert.pfx key-pair dsa key-file serverkey.pfx auth-code cipher YsHsjx_202206
```

Load a PEM certificate chain for the SSL policy.

```
<HUAWEI> system-view
[HUAWEI] ssl policy http_server
[HUAWEI-ssl-policy-http_server] certificate load pem-chain chain-servercert.pem key-pair dsa key-file chain-servercertkey.pem auth-code cipher YsHsjx_202206
```

2.7.12 close

Function

The **close** command terminates the connection with the remote FTP server and retains the FTP client view.

Format

close

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command is equivalent to the **disconnect** command.

You can run the **bye** and **quit** commands to terminate the connection with the remote FTP server and enter the user view.

Precautions

To enter the user view from the FTP client view, you can run the **bye** or **quit** command.

Example

Terminate the connection with the remote FTP server and enter the FTP client view.

```
<HUAWEI>ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] close
221 Server closing.

[ftp]
```

2.7.13 copy

Function

The **copy** command copies a file.

The **copy** command allows downloading files from an HTTP/HTTPS server or uploading files to an HTTP/HTTPS server.

NOTE

HTTPS is recommended because it is more secure than HTTP.

Format

copy *source-filename destination-filename* [**all**]

copy { *source-http-urlname destination-filename* | *source-filename destination-http-urlname* } [**username** *user-name* **password** *password*]
(V200R013C00SPC500 or later)

copy { *source-https-urlname destination-filename* | *source-filename destination-https-urlname* } [**username** *user-name* **password** *password*] **ssl-policy** *ssl-policy*
(V200R013C00SPC500 or later)

Parameters

Parameter	Description	Value
source-filename	Specifies the path and name of a source file.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "

Parameter	Description	Value
destination-filename	Specifies the path and name of a destination file.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "
all	Copies a file to all member devices. **NOTE** This parameter is available only in a stack system.	-
username *user-name*	Specifies the user name used to log in to a server.	The value is a string of 1 to 64 characters.
password *password*	Specifies the password used to log in to a server.	The value is a string of 1 to 64 characters.
source-http-urlname	Specifies the URL of an HTTP server from which a file is downloaded.	The value is a string of 1 to 230 case-insensitive characters without spaces.
destination-http-urlname	Specifies the URL of an HTTP server to which a file is uploaded.	The value is a string of 1 to 230 case-insensitive characters without spaces.

Parameter	Description	Value
source-https-urlname	Specifies the URL of an HTTPS server from which a file is downloaded.	The value is a string of 1 to 230 case-insensitive characters without spaces.
destination-https-urlname	Specifies the URL of an HTTPS server to which a file is uploaded.	The value is a string of 1 to 230 case-insensitive characters without spaces.
ssl-policy *ssl-policy*	Specifies the name of an SSL policy.	The value is a string of 1 to 23 case-insensitive characters without spaces.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the drive name.

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Precautions

- If the destination file name is not specified, the designation file and the source file have the same name. If the source file and the destination file are

in the same directory, you must specify the destination file name. If the destination file name is not specified, you cannot copy the source file.

- If the destination file name is the same as that of an existing file, the system prompts you whether to overwrite the existing file. The system prompt is displayed only when **file prompt** is set to **alert**.

Example

Copy the file **config.cfg** from the root directory of the flash card to flash:/temp. The destination file name is **temp.cfg**.

```
<HUAWEI> copy flash:/config.cfg flash:/temp/temp.cfg
Copy flash:/config.cfg to flash:/temp/temp.cfg?[Y/N]:y
100%  complete.
Info: Copied file flash:/config.cfg to flash:/temp/temp.cfg...Done.
```

If the current directory is the root directory of the flash card, you can perform the preceding configuration using the relative path.

```
<HUAWEI> pwd
flash:
<HUAWEI> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time       FileName
   0   -rw-     6,721,804  Mar 19 2012 12:31:58   devicesoft.cc
   1   -rw-           910  Mar 19 2012 12:32:58   config.cfg
   2   drw-             -  Mar 05 2012 09:54:34   temp
...
65,233 KB total (7,289 KB free)
<HUAWEI> copy config.cfg temp/temp.cfg
Copy flash:/config.cfg to flash:/temp/temp.cfg?[Y/N]:y
100%  complete.
Info: Copied file flash:/config.cfg to flash:/temp/temp.cfg...Done.
```

Copy the file **config.cfg** from the root directory of the flash card to flash:/temp. The destination file name is **config.cfg**.

```
<HUAWEI> pwd
flash:
<HUAWEI> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time       FileName
   0   -rw-     6,721,804  Mar 19 2012 12:31:58   devicesoft.cc
   1   -rw-           910  Mar 19 2012 12:32:58   config.cfg
   2   drw-             -  Mar 05 2012 09:54:34   temp
...
65,233 KB total (7,289 KB free)
<HUAWEI> copy config.cfg temp
Copy flash:/config.cfg to flash:/temp/config.cfg?[Y/N]:y
100%  complete.
Info: Copied file flash:/config.cfg to flash:/temp/config.cfg...Done.
```

Copy the file **backup.zip** to **backup1.zip** in the test directory from the current working directory flash:/test/.

```
<HUAWEI> pwd
flash:/test
<HUAWEI> copy backup.zip backup1.zip
Copy flash:/test/backup.zip to flash:/test/backup1.zip?[Y/N]:y
100%  complete.
Info: Copied file flash:/test/backup.zip to flash:/test/backup1.zip...Done.
```


2.7.14 crl load

Function

The **crl load** command loads the CRL for the SSL policy.

The **undo crl load** command unloads the SSL policy CRL.

By default, the SSL policy CRL is not loaded.

Format

crl load { **pem-crl** | **asn1-crl** } *crl-filename*

undo crl load { **pem-crl** | **asn1-crl** } *crl-filename*

Parameters

Parameter	Description	Value
pem-crl	Loads the CRL in the PEM format for the SSL policy.	-
asn1-crl	Loads the CRL in the ASN1 format for the SSL policy.	-
crl-filename	Specifies the name of a CRL. The file is in the subdirectory of the system directory **security**. If the **security** directory does not exist in the system, create this directory.	The value is a string of 1 to 64 case-insensitive characters without spaces. The file name is the same as that of the uploaded file.

Views

SSL policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The CA can shorten the validity period of a certificate using a CRL. The CA releases the CRL that specifies a set of invalid certificates. If the CA revokes a certificate in the CRL, the declaration about authorized key pair is revoked before the certificate expires. When the certificate expires, data related to the certificate is cleared from the CRL.

If the certificate key is disclosed or if you need to revoke a certificate due to other reasons, use a third-party tool to revoke released certificates and mark them as invalid, generating a CRL.

Prerequisites

Before running the **crl load** command, you have run the **ssl policy** command to create the SSL policy in the system view.

Precautions

- When you load the CRL on the FTPS client and access the FTPS server on the FTPS client, the FTPS server checks whether the certificate is declared in the CRL. If the certificate has been declared, the FTPS client and server disconnects.
- A maximum of two CRL files can be loaded in an SSL policy. For the sake of security, deleting the installed CRL file is not recommended; otherwise, services using the SSL policy will be affected.

Example

Load the CRL in the PEM format for the SSL policy.

```
<HUAWEI> system-view
[HUAWEI] ssl policy ftp_server
[HUAWEI-ssl-policy-ftp_server] crl load pem-crl server.pem
```

Load the CRL in the ASN1 format for the SSL policy.

```
<HUAWEI> system-view
[HUAWEI] ssl policy ftp_server
[HUAWEI-ssl-policy-ftp_server] crl load asn1-crl server.der
```

2.7.15 delete (FTP client view)

Function

The **delete** command deletes a file from the FTP server.

Format

delete *remote-filename*

Parameters

Parameter	Description	Value
remote-filename	Specifies the name of a file to be deleted.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

A file deleted in the FTP client view cannot be restored.

Example

Delete the file **temp.c**.

```
<HUAWEI>ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] delete temp.c
Warning: File temp.c will be deleted. Continue? [Y/N]: y
250 DELE command successfully.
```

2.7.16 delete (user view)

Function

The **delete** command deletes a specified file in the storage device.

Format

delete [**/unreserved**] [**/quiet**] { *filename* | *devicename* } [**all**]

Parameters

Parameter	Description	Value
/unreserved	Deletes a specified file. The deleted file cannot be restored.	-
/quiet	Deletes a file directly without any confirmation.	-

Parameter	Description	Value
filename	Specifies the name of a file to be deleted.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "
devicename	Deletes all the files in the storage device.	-
all	Deletes files in the specified directory in a batch from all storage devices. **NOTE** This parameter is available only in a stack system.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the drive name.

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Like *devicename*, **drive** specifies the storage device name.

Precautions

- The wildcard (*) character can be used in the **delete** command.
- If the parameter **/unreserved** is not included, the file is stored in the recycle bin. To display all files including deleted files that are displayed in square brackets ([ ]), run the **dir /all** command. To restore these files that are displayed in square brackets ([ ]), run the **undelete** command. To clear these files from the recycle bin, run the **reset recycle-bin** command.

  NOTICE

  If you delete a file using the **/unreserved** parameter, the file cannot be restored.

- If you delete a specified storage device, all files are deleted from the root directory of the storage device.
- If you delete two files with the same name from different directories, the last file deleted is kept in the recycle bin.
- If you attempt to delete a protected file, such as a configuration file, log file, or patch file, a system prompt is displayed.
- If you need to delete protected log files, you can run the **info-center max-logfile-number** command to modify the maximum number of protected log files. When the number of log files exceeds the maximum value, the system will delete the older log files to ensure that the number of log files is less than or equal to the configured value.
- You cannot delete a directory by running the **delete** command. To delete a directory, run the **rmdir (user view)** command.

Example

Delete the file **test.txt** from the **flash:/test/** directory.

```
<HUAWEI> delete flash:/test/test.txt
Delete flash:/test/test.txt?[Y/N]:y
```

Delete the file **test.txt** from the current working directory **flash:/selftest**.

```
<HUAWEI> delete test.txt
Delete flash:/selftest/test.txt?[Y/N]:y
```

2.7.17 dir (user view)

Function

The **dir** command displays information about files and directories in the storage medium.

NOTE

The **dir** command cannot display information about files and directories in a USB flash drive.

Format

dir [**/all**] [*filename* | *directory* | **/all-filesystems**]

Parameters

Parameter	Description	Value
/all	Displays information about all files and directories in the current directory, including files and directories moved to the recycle bin from the current directory.	-

Parameter	Description	Value
filename	Specifies the file name.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "
directory	Specifies the file directory.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] path** format. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "

Parameter	Description	Value
/all-filesystems	Display information about files and directories in the root directories of all the storage media on the device.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

The wildcard character (*) can be used in this command. If no parameter is specified, this command displays information about files and directories in the current directory.

The following describes the drive name:

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

You can run the **dir /all** command to view information about all files and directories of the storage medium, including those moved to the recycle bin. The name of a file in the recycle bin is placed in square brackets ([]), for example, [test.txt].

Example

Display information about all files and directories in the current directory.


```
<HUAWEI> dir /all
Directory of flash:/

 Idx  Attr     Size(Byte)  Date       Time       FileName
   0  -rw-          889  Feb 25 2012 10:00:58   private-data.txt
   1  -rw-        6,311  Feb 17 2012 14:05:04   backup.cfg
   2  -rw-          836  Jan 01 2012 18:06:20   rr.dat
   3  drw-            -  Jan 01 2012 18:08:20   logfile
   4  -rw-          836  Jan 01 2012 18:06:20   rr.bak
   5  drw-            -  Feb 27 2012 00:00:54   security
   6  -rw-      523,240  Mar 16 2011 11:21:36   bootrom_53hib66.bin
   7  -rw-        2,290  Feb 25 2012 16:46:06   vrpcfg.cfg
   8  -rw-          812  Dec 12 2011 15:43:10   hostkey
   9  drw-            -  Jan 01 2012 18:05:48   compatible
  10  -rw-   25,841,428  Nov 17 2011 09:48:10   basicsoft.cc
  11  -rw-          540  Dec 12 2011 15:43:12   serverkey
  12  -rw-   26,101,692  Dec 21 2011 11:44:52   devicesoft.cc
  13  -rw-        6,292  Feb 14 2012 11:14:32   1.cfg
  14  -rw-        6,311  Feb 17 2012 10:22:56   1234.cfg
  15  -rw-        6,311  Feb 25 2012 17:22:30   [11.cfg]

65,233 KB total (13,632 KB free)
```

Display information about files and directories in the root directories of all the storage media on the devices in a stack.

```
<HUAWEI> dir /all-filesystems
Directory of flash:/

 Idx  Attr     Size(Byte)  Date       Time       FileName
   0  -rw-       10,872  Nov 22 2012 20:26:28   private-data.txt
   1  -rw-          836  Nov 22 2012 20:26:44   rr.dat
   2  -rw-          836  Nov 22 2012 20:26:44   rr.bak
   3  -rw-        1,640  Nov 22 2012 20:24:50   vrpcfg.zip
   4  -rw-           10  Jun 05 2012 09:58:50   dhcp-duid
   5  -rw-      216,399  Nov 22 2012 20:16:52   patch_all_pack.pat
   6  drw-            -  Nov 22 2012 20:06:58   dhcp
   7  drw-            -  Nov 22 2012 20:26:32   compatible
   8  drw-            -  Nov 22 2012 20:28:46   logfile
   9  -rw-        1,399  Oct 25 2012 16:32:12   vrpcfg11.zip
  10  drw-            -  Sep 26 2009 11:02:52   user
  11  -rw-   15,298,556  Nov 20 2012 03:21:16   basicsoft.cc
  12  -rw-      289,596  Nov 16 2012 14:58:00   patch.pat

65,233 KB total (33,632 KB free)

Directory of slot1#flash:/

 Idx  Attr     Size(Byte)  Date       Time       FileName
   0  -rw-       10,872  Nov 22 2012 20:28:24   private-data.txt
   1  -rw-          836  Nov 22 2012 20:27:48   rr.dat
   2  -rw-          836  Nov 22 2012 20:27:48   rr.bak
   3  -rw-        1,640  Nov 22 2012 20:24:52   vrpcfg.zip
   4  -rw-           10  Oct 10 2008 22:58:40   dhcp-duid
   5  -rw-      216,399  Nov 22 2012 14:34:36   patch_all_pack.pat
   6  drw-            -  Nov 22 2012 20:28:22   dhcp
   7  drw-            -  Nov 22 2012 20:27:16   compatible
   8  drw-            -  Oct 10 2008 23:00:40   logfile
   9  drw-            -  Nov 24 2012 00:00:18   resetinfo
  10  drw-            -  Sep 26 2009 11:03:02   user
  11  -rw-   15,298,556  Nov 21 2012 14:39:54   basicsoft.cc

65,233 KB total (33,632 KB free)
```

Display information about the file vrpcfg.cfg in the current directory.

```
<HUAWEI> dir vrpcfg.cfg
Directory of flash:/
```

```
  Idx  Attr     Size(Byte)  Date       Time       FileName
    0  -rw-          2,290  Feb 25 2012 16:46:06   vrpcfg.cfg

65,233 KB total (13,632 KB free)
```

Display information about all .txt files in the current directory.

```
<HUAWEI> dir *.txt
Directory of flash:/

  Idx  Attr     Size(Byte)  Date       Time       FileName
    0  -rw-            889  Feb 25 2012 10:00:58   private-data.txt

65,233 KB total (13,632 KB free)
```

Table 2-46 Description of the **dir** command output

Item	Description
d	Directory. If this item is not displayed, the corresponding **FileName** field displays a file. For example, **devicesoft.cc** is a file and **security** is a directory.
r	The file or directory is readable.
w	The file or directory is writable.
[ ]	A file moved to the recycle bin.
FileName	• private-data.txt: The file saves service initialization data. Initialization data of some tasks is irrelevant to the configuration and is not recorded in the configuration file. The **private-data.txt** file records initialization data of these tasks, for example, the number of times the device restarts. • vrpcfg.cfg: configuration file. The file name extension of the configuration file must be .cfg or .zip. • basicsoft.cc: system software. The file name extension of the system software must be .cc. • logfile: log file. Some software sub-systems store necessary data in other files in the file system when the device is running properly.

2.7.18 dir/ls (FTP client view)

Function

The **dir** and **ls** commands display all files or specified files that are stored on the FTP server, and save them to a local disk.

Format

dir [*remote-filename* [*local-filename*]]

ls [*remote-filename* [*local-filename*]]

Parameters

Parameter	Description	Value
remote-filename	Specifies the name and directory of a file stored on the FTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.
local-filename	Specifies the name of the local file that saves the FTP server file information.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes differences between the **dir** and **ls** commands.

- When you run the **dir** command, detailed file information is displayed, including the file size, date when the file was created, whether the file is a directory, and whether the file can be modified. When you run the **ls** command, only the file name is displayed.
- The **dir** command is used to save detailed file information, while the **ls** command is used to save only the file name even if the file is specified and saved in a local directory.

Precautions

A wildcard character (*) can be used in commands **dir** and **ls**.

Example

Display the name or detailed information about a file that is saved in the test directory.

```
<HUAWEI>ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] cd test
250 CWD command successfully.
```



```
[ftp] dir
200 Port command okay.
150 Opening ASCII mode data connection for *.
drwxrwxrwx   1 noone    nogroup         0 Mar 24 10:48 .
drwxrwxrwx   1 noone    nogroup         0 Mar 26 15:52 ..
drwxrwxrwx   1 noone    nogroup         0 Mar 23 16:04 yourtest
-rwxrwxrwx   1 noone    nogroup      5736 Mar 24 10:38 backup.txt
-rwxrwxrwx   1 noone    nogroup      5736 Mar 24 10:38 backup1.txt
226 Transfer complete.
[ftp] ls
200 Port command okay.
150 Opening ASCII mode data connection for *.
. ..
yourtest
backup.txt
backup1.txt
226 Transfer complete.
```

Display the detailed information for the file **temp.c**, and save the displayed information in file **temp1**.

```
[ftp] dir temp.c temp1
200 Port command okay.
150 Opening ASCII mode data connection for temp.c.

226 Transfer complete.

[ftp] quit

221 Server closing.

<HUAWEI> more temp1
-rwxrwxrwx  1  noone   nogroup  3929  Apr 27 18:13  temp.c
```

Display the name of file **test.bat**, and save the displayed information in file **test**.

```
<HUAWEI>ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[ftp] ls test.bat test
200 Port command okay.
150 Opening ASCII mode data connection for test.bat.

226 Transfer complete.

[ftp] quit

221 Server closing.

<HUAWEI> more test
test.bat
```

Table 2-47 Description of the dir/ls command output

Item	Description
d	Indicates a directory. If this parameter is not present, the command output indicates a file.
r	Indicates that the file or directory can be read.

Item	Description
w	Indicates that the file or directory can be modified.

2.7.19 dir/ls (SFTP client view)

Function

The **dir** and **ls** commands display a list of specified files that are stored on the SFTP server.

Format

dir [**-l** | **-a**] [*remote-directory*]

ls [**-l** | **-a**] [*remote-directory*]

Parameters

Parameter	Description	Value
-l	Displays detailed information about all files and directories in a specified directory.	-
-a	Displays names of all files and directories in a specified directory.	-
remote-directory	Specifies the name of a directory on the SFTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

The **dir** and **ls** commands are equivalent.

- If **-l** and **-a** parameters are not specified, detailed information about all files and directories in a specified directory is displayed when you run the **dir** or **ls** command. The effect is the same as the **dir -l** command output.
- By default, if the *remote-directory* parameter is not specified, the list of current directory files is displayed when you run the **dir** or **ls** command.

Example

Display a list of files in the **test** directory of the SFTP server.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> dir test
drwxrwxrwx   1 noone    nogroup        0 Mar 24 2012 .
drwxrwxrwx   1 noone    nogroup        0 Mar 29 2012 ..
-rwxrwxrwx   1 noone    nogroup        0 Mar 24 2012 yourtest
-rwxrwxrwx   1 noone    nogroup     5736 Mar 24 2012 backup.txt
-rwxrwxrwx   1 noone    nogroup     5736 Mar 24 2012 backup1.txt
sftp-client> dir -a test
.
..
yourtest
backup.txt
backup1.txt
sftp-client> ls test
drwxrwxrwx   1 noone    nogroup        0 Mar 24 2012 .
drwxrwxrwx   1 noone    nogroup        0 Mar 29 2012 ..
-rwxrwxrwx   1 noone    nogroup        0 Mar 24 2012 yourtest
-rwxrwxrwx   1 noone    nogroup     5736 Mar 24 2012 backup.txt
-rwxrwxrwx   1 noone    nogroup     5736 Mar 24 2012 backup1.txt
sftp-client> ls -a test
.
..
yourtest
backup.txt
backup1.txt
```

2.7.20 disconnect

Function

The **disconnect** command terminates the connection with the remote FTP server and displays the FTP client view.

Format

disconnect

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

This command is equivalent to the **close** command.

You can run the **bye** and **quit** commands to terminate the connection with the remote FTP server and enter the user view.

To enter the user view from the FTP client view, you can run the **bye** or **quit** command.

Example

Terminate the connection with the remote FTP server and enter the FTP client view.

```
<HUAWEI>ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] disconnect

221 Server closing.

[ftp]
```

2.7.21 display ftp-client

Function

The **display ftp-client** command displays the source IP address configured for the FTP client.

Format

display ftp-client

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

The default source IP address 0.0.0.0 is used if **ftp client-source** is not configured.

Example

Display the source IP address of the FTP client.

```
<HUAWEI> display ftp-client
The source address of FTP client is 10.1.1.1.
```

Table 2-48 Description of the display ftp-client command output

Item	Description
The source IP address of FTP client is 10.1.1.1.	10.1.1.1 is the source IP address of the FTP client. You can run the **ftp client-source** command to configure the source IP address. If a source IP address has been configured by using the **ftp client-source** command, the message "The source interface of FTP client is LoopBack0" is displayed.

2.7.22 display ftp-server

Function

The **display ftp-server** command displays FTP server parameter settings.

Format

display [**ipv6**] **ftp-server**

Parameters

Parameter	Description	Value
ipv6	Specifies the IPv6 FTP server.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to display FTP server parameter settings.

Example

Display FTP server parameter settings.

```
<HUAWEI> display ftp-server
  FTP server is running
  Max user number              5
  User count                   1
  Timeout value(in minute)     30
  Listening port               21
  Acl number                   2010
  FTP server's source address  10.1.1.1
  FTP SSL policy
  FTP Secure-server is stopped
```

Display FTP server parameter settings when the secure FTP server function is enabled.

```
<HUAWEI> display ftp-server
  FTP server is stopped
  Max user number              5
  User count                   0
  Timeout value(in minute)     1
  Listening port               21
  Acl number                   0
  FTP server's source interface  LoopBack0
  FTP SSL policy
  FTP Secure-server is running
```

Table 2-49 Description of the display ftp-server command output

Item	Description
FTP server is running	The FTP server starts. You can run the **ftp** [**ipv6**] **server enable** command to start the FTP server.
Max user number	Maximum number of users who can access the FTP server.
User count	Number of users who are accessing the FTP server.
Timeout value(in minute)	Idle timeout duration of FTP users. You can run the **ftp** [**ipv6**] **timeout** command to set the idle timeout duration of FTP users.
Listening port	Number of the listening port on the FTP server. The default value is 21. If the value is not 21, you can run the **ftp** [**ipv6**] **server port** command to configure the listening port number.
Acl number	Number of the ACL of the FTP server. The default value is 0. You can run the **ftp** [**ipv6**] **acl** command to change the ACL number.

Item	Description
FTP server's source address	Source IP address for the FTP server to send packets. The default value is 0.0.0.0. You can run the **ftp server-source** command to configure the source IP address for the FTP server. Here, the source IP address 10.1.1.1 is displayed. If a source interface is configured, this field displays "FTP server's source interface." **NOTE** If you run the **display ipv6 ftp-server** command, the **FTP server's source address** is not displayed.
FTP SSL policy	SSL policy that the secure FTP server function uses. Before enabling the FTP function, you must run the **ftp secure-server ssl-policy** *policy-name* command to configure the SSL policy.
FTP Secure-server is stopped	Whether to enable the secure FTP server function. To enable the secure FTP server function, disable the common FTP function and run the **ftp secure-server enable** command.

2.7.23 display ftp-users

Function

The **display ftp-users** command displays FTP user parameters on the FTP server.

Format

display ftp-users

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can check FTP user parameters on the FTP server, such as the FTP user name, IP address of the client host, port number, idle duration, and the authorized directories.

Example

Display FTP user parameters.

```
<HUAWEI> display ftp-users
  username  host                                  port  idle  topdir
  user      10.138.77.41                          4028  0     flash:/test
  huawei    10.137.217.159                          51156 0     flash:
```

The preceding information indicates that two users are connected to the FTP server.

Table 2-50 Description of the display ftp-users command output

Item	Description
username	FTP user name.
host	IP address of the client host.
port	Port number of the client host.
idle	Idle duration.
topdir	Authorized directory of a user. You can run the **local-user ftp-directory** command to configure the authorized directory.

2.7.24 display scp-client

Function

The **display scp-client** command displays source parameters of the current SCP client.

Format

display scp-client

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display scp-client** command to check source parameters of the SCP client.

If **scp client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* } is not configured, source parameters are not displayed.

Example

Display source parameters of the SCP client.

```
<HUAWEI> display scp-client
 The source of SCP ipv4 client: 10.1.1.1
```

2.7.25 display sftp-client

Function

The **display sftp-client** command displays the source IP address configured for the SFTP client.

Format

display sftp-client

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display sftp client** command to display the source IP address of the SFTP client. The default source IP address 0.0.0.0 is used if **sftp client-source** is not configured.

Example

Display the source IP address configured for the SFTP client.

```
<HUAWEI> display sftp-client
The source address of SFTP client is 10.1.1.1.
```

Table 2-51 Description of the display sftp-client command output

Item	Description
The source address of SFTP client is 10.1.1.1.	10.1.1.1 is the source IP address of the SFTP client. You can run the **sftp client-source** command to configure the source IP address for the SFTP client. If an IP address has been configured for the source port, the message "The source interface of SFTP client is LoopBack0" is displayed.

2.7.26 display ssl policy

Function

The **display ssl policy** command displays information about an SSL policy.

Format

display ssl policy [*policy-name*]

Parameters

Parameter	Description	Value
policy-name	Displays the configuration of a specific SSL policy. If the SSL policy name is not specified, configurations of all SSL policies are displayed.	The value is a string of 1 to 23 case-insensitive characters without spaces. The value can contain digits, letters, and underscores (_).

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ssl policy** command to display the SSL policy configuration when the device functions as a server or client.

After an SSL policy and its certificates are loaded and configured, you can run this command to obtain information such as the SSL policy name, service applications supported by the SSL policy, certificate name, and certificate type so that you can determine whether the existing SSL policy and certificates are available.

Example

Display the configuration of SSL policy **ftp_server**.

```
<HUAWEI> display ssl policy ftp_server
      SSL Policy Name: ftp_server
    Policy Applicants:
       Key-pair Type: DSA
Certificate File Type: ASN1
    Certificate Type: certificate
Certificate Filename: servercert.der
   Key-file Filename: serverkey.der
           Auth-code:
                 MAC:
            CRL File:
      Trusted-CA File:
         Issuer Name:
  Validity Not Before:
   Validity Not After:
```

Display the configuration of SSL policy **ftp_client**.

```
<HUAWEI> display ssl policy ftp_client

      SSL Policy Name: ftp_client
    Policy Applicants:
       Key-pair Type: RSA
Certificate File Type: ASN1
    Certificate Type: certificate
Certificate Filename: servercert.der
   Key-file Filename: serverkey.der
           Auth-code:
                 MAC:
            CRL File:
      Trusted-CA File:
         Issuer Name:
  Validity Not Before:
   Validity Not After:
```

Table 2-52 Description of the display ssl policy command output

Item	Description
SSL Policy Name	SSL policy name. You can run the **ssl policy** command to configure the SSL policy name.
Policy Applicants	Service using SSL policies. Currently, SSL policies are supported in HTTP, FTP and Syslog services.

Item	Description
Key-pair Type	Type of a key pair. • RSA • DSA • ECC You can run the **certificate load** command to configure the type of a key pair.
Certificate File Type	Certificate format. This parameter is mandatory when the device functions as a server. • PEM • ASN1 • PFX You can run the **certificate load** command to configure the certificate format.
Certificate Type	Certificate type. This parameter is mandatory when the device functions as a server. • certificate • certificate-chain You can run the **certificate load** command to configure the certificate type.
Certificate Filename	Certificate name. This parameter is mandatory when the device functions as a server. You can run the **certificate load** command to configure the certificate name.
Key-file Filename	Key pair file name. This parameter is mandatory when the device functions as a server. You can run the **certificate load** command to configure the key pair file name.
Auth-code	Authentication code of a key file. You can run the **certificate load** command to configure the authentication code of a key file. If an ASN1 certificate is loaded, the authentication code is unavailable.

Item	Description
MAC	Message authentication code. The message authentication code is required only when you load PFX digital certificates. You can run the **certificate load** command to configure the message authentication code.
CRL File	CRL file. You are advised to configure the CRL file for a client. You can run the **crl load** command to configure the CRL file.
Trusted-CA File	File of a trusted CA. This parameter is mandatory when the device functions as a client. • **Format**: file format. • **Auth-code**: authentication code of a PFX file. This field is displayed only when a PFX file has been loaded to the device. • **Filename**: file name. You can run the **trusted-ca load** command to configure the file of a trusted CA.
Issuer Name	Issuer name.
Validity Not Before	Time when validity starts.
Validity Not After	Time when validity ends.

2.7.27 display tftp-client

Function

The **display tftp-client** command displays the source IP address configured for the TFTP client.

Format

display tftp-client

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display tftp client** command to query source IP address of the TFTP client. The default source IP address is 0.0.0.0 if **tftp client-source** is not configured.

Example

Display the source IP address configured for the TFTP client.

```
<HUAWEI> display tftp-client
The source address of TFTP client is 10.1.1.1.
```

Table 2-53 Description of the display tftp-client command output

Parameter	Description
The source address of TFTP client is 10.1.1.1.	10.1.1.1 is the source IP address of the TFTP client. You can run the **tftp client-source** command to configure the source IP address for the TFTP client. If the IP address is configured for the source port, the message "The source interface of TFTP client is LoopBack0" is displayed.

2.7.28 execute

Function

The **execute** command executes a specified batch file.

Format

execute *batch-filename*

Parameters

Parameter	Description	Value
batch-filename	Specifies the name of a batch file. *batch-filename* supports file name association. The disk and directory where the file resides can be automatically associated. • Full help: All the disks of the device can be associated and displayed. • Partial help: The related disk, directory, and file can be associated and displayed after you enter a specified character string.	The value is a string of 5 to 160 case-sensitive characters. It cannot contain spaces. The file name extension is .bat.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a series of commands are frequently executed, write these commands in a batch file, and store this file in system. In this way, you can only execute this command to run multiple commands which were manually entered before. This command improves maintenance and management efficiency.

NOTE

- The batch file is edited in .txt format. When editing the file, ensure that one command occupies one line. After editing the file, save the file and change the file name extension to .bat.
- Transfer the batch file in file transmission mode to the device.

Prerequisites

Before running the **execute** command, ensure that the batch file to be processed is in the current directory; otherwise, the system cannot find the batch file.

Precautions

- The commands in a batch file are run one by one. A batch file cannot contain invisible characters (control characters or escape characters, such as \r, \n, and \b). If any invisible character is detected, the execute command exits from the current process and no rollback is performed.
- The **execute** command does not ensure that all commands can be run. If the system runs a wrong or immature command, it displays the error and goes to

next command. The **execute** command does not perform the hot backup operation, and the command format or content is not restricted.

- In case of interactive commands, batch file execution waits the device to interact with users before continuing.

NOTE

When processing files in batches, add the **echo off** field in the first line to mask command line prompts. After the **echo off** field is added, the command line prompts and command lines are not displayed when command lines are processed in batches. Comply with the following rules:

- The **echo off** field can be added only to the first line of the files to be processed in batches.
- The **echo off** field is case-insensitive.
- The line where the **echo off** field resides cannot contain any special characters, spaces excluded.

In the batch file, you can enter **wait(*time*)** between commands to set a command execution delay. The value of *time* ranges from 1 to 1800, in seconds. For example, **wait(10)** indicates that the next command is executed 10 seconds later. The value of **wait(*time*)** is case-insensitive. In the line where **wait(*time*)** resides, spaces cannot be placed before or after **wait(*time*)**, or before or after *time*. Other characters are also not allowed.

Example

Execute the **test.bat** file in the directory flash:/. The **test.bat** file contains the following commands: **system-view**, **local-user huawei password irreversible-cipher Helloworld@6789**, and **aaa**.

```
<HUAWEI> system-view
[HUAWEI] execute test.bat
[HUAWEI]
        ^
Error: Unrecognized command found at '^' position.
[HUAWEI]
[HUAWEI-aaa]
 Info: Add a new user
[HUAWEI-aaa]
```

When the system runs the first command **system-view** in the current system view, it displays an error and continues to run the following commands.

The system displays the execution of a batch file in AAA view.

```
[HUAWEI-aaa] display this
 local-user huawei password irreversible-cipher $1a$HW=5%Mr;:2)/RX$FnU1HLO%-TBMp4wn%;~\#
%iAut}_~O%0L$
```

2.7.29 feat

Function

The **feat** command displays extended commands that the FTP server supports.

Format

feat

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

You can run the **feat** command to display extended functions that the FTP server supports, such as:

- Authentication transport layer security (AUTH TLS)
- Data channel protection level (PROT)
- Protection buffer size (PBSZ)

Precautions

If no extended command is supported, the message "211 no features" is displayed.

Example

Display extended commands that the FTP server supports.

```
[ftp] feat
211-Extension Supported
AUTH TLS
PROT
PBSZ
211 End
```

Table 2-54 Description of the feat command output

Parameter	Description
211	Value of the FTP relay code. The value is returned in the help information or system status query result.
AUTH TLS	AUTH TLS commands supported.
PROT	PROT commands supported.s
PBSZ	PBSZ commands supported.

2.7.30 file prompt

Function

The **file prompt** command changes the prompt mode when you perform operations on files.

The **undo file prompt** command restores the default prompt mode.

The default prompt mode is alert.

Format

file prompt { **alert** | **quiet** }

undo file prompt quiet

Parameters

Parameter	Description	Value
alert	Display a prompt message before users perform an operation.	-
quiet	Do not display a prompt message before users perform an operation.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

NOTICE

If the prompt mode is set to quiet, the system does not provide prompt messages when operations leading to data loss are executed, such as deleting or overwriting files. Therefore, this prompt mode should be used with caution.

Example

Set the prompt mode to quiet. When you rename a copied file **test.txt** using an existing file name **test1.txt**, no prompt message is displayed.

```
<HUAWEI> system-view
[HUAWEI] file prompt quiet
[HUAWEI] quit
<HUAWEI> copy test.txt test1.txt
```



```
100%  complete
Info: Copied file flash:/test.txt to flash:/test1.txt...Done.
```

Set the prompt mode to alert.

```
<HUAWEI> system-view
[HUAWEI] file prompt alert
[HUAWEI] quit
<HUAWEI> copy test.txt test1.txt
Copy flash:/test.txt to flash:/test1.txt?[Y/N]:y
The file flash:/test1.txt exists. Overwrite it?[Y/N]:y
100%  complete
Info: Copied file flash:/test.txt to flash:/test1.txt...Done.
```

2.7.31 fixdisk

Function

The **fixdisk** command restores a storage device in which the file system fails to run properly.

Format

fixdisk *drive*

Parameters

Parameter	Description	Value
drive	Specifies the name of the storage device to restore.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the storage device name.

- **drive** is the storage device and is named as flash:.
- In a stack system, *devicename* can be set as follows:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

If the file system does not run properly, the system prompts you to restore it. You can run the **fixdisk** command to attempt to restore the file system. You can run

the **fixdisk** command to release the space whose usage status is unknown from the storage device.

You can run the **dir** command to display information about a specified file or directory on the storage device. If the command output contains **unknown**, for example, 30,000 KB total (672 KB free, 25,560 KB used, 3,616 KB unknown), you can run the **fixdisk** command to release the space whose usage status is unknown.

Precautions

- The **fixdisk** command is not recommended when the system works properly. This command cannot rectify device-level faults.
- If you are still prompted to restore the storage device after running the **fixdisk** command, the physical medium may have been damaged.
- Running the **fixdisk** command to restore a flash memory requires high CPU usage. Therefore, do not run this command when the CPU usage in the system is high.

Example

Restore the flash memory when an error message indicating that the flash memory is faulty is displayed.

```
Lost chains in flash detected, please use fixdisk to recover them!
<HUAWEI> fixdisk flash:
Fix disk flash: will take long time if needed...
% Fix disk flash: completed.
```

2.7.32 format

Function

The **format** command formats a storage device.

NOTE

In V200R013C00SPC500 and later versions, this command can be run only if you log in to the device through the serial port.

The following models do not support this command:

S300, S500, S2730S-S, S5735-L1, S5735S-L1, S5731-S (S5731-S24P4X, S5731-S24T4X, S5731-S24T4X-A, S5731-S24T4X-D, S5731-S48P4X, S5731-S48T4X, S5731-S48T4X-A), S5731S-S (S5731S-S24P4X-A, S5731S-S24T4X-A, S5731S-S24T4X-A1, S5731S-S48P4X-A, S5731S-S48T4X-A, S5731S-S48T4X-A1), S5731-H, S5731S-H, S5732-H (S5732-H24S6Q, S5732-H24UM2CC, S5732-H48S6Q, S5732-H48UM2CC), S6730-S, S6730S-S, S6730-H (S6730-H24X6C, S6730-H48X6C), S6730S-H

Format

format *drive*

Parameters

Parameter	Description	Value
drive	Specifies the name of the storage device to format.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the storage device name.

- **drive** is the storage device and is named as flash:.
- In a stack system, *devicename* can be set as follows:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

When the file system fault cannot be rectified or the data on the storage device is unnecessary, the storage device can be formatted. When you run the **format** command, all files and directories are cleared from the storage device.

Configuration Impact

When the storage device has the configuration file and system software package required for the next start, do not format the storage device because data on it will be deleted after the format. If the configuration file required for the next start is deleted, the configuration is lost after the switch restarts. If the system software package is deleted, the switch will fail to start.

After the storage is formatted, you can upload the system software through the Enter ethernet submenu option in the Bootload menu. The Modify startup configuration option modifies the startup configuration information and restarts the device.

Precautions

NOTICE

After the **format** command is run, files and directories are cleared from the specified storage device and cannot be restored. Therefore, this command should be used with caution.

If the storage device is still unavailable after the **format** command is run, a physical exception may have occurred.

Example

Format the storage device.

```
<HUAWEI> format flash:
All data(include configuration and system startup file) on flash: will be lost, proceed with format ? [Y/N]:y
%Format flash: completed.
```

2.7.33 format ssd

Function

The **format ssd** command formats the SSD card.

Format

format ssd [**slot** *slot-id*]

NOTE

Only the S5731-H, S5731-S, S5731S-H, and S5731S-S support this command.

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID.	The value depends on the device configuration.

Views

User view

Default Level

3: Management level

Usage Guidelines

Application Scenario

When the file system fault cannot be rectified or all data on the SSD card is unnecessary, the SSD card can be formatted. When this command is run, all files and directories are cleared from the SSD card.

Configuration Impact

If the SSD card contains the configuration file and software package required for the next startup, do not format the card because formatting the SSD card will cause all data on the card to be cleared. As a result, the configuration file for the next startup is deleted, and configurations are lost after the device is restarted; the software package for the next startup is deleted, and the device cannot be started.

Precautions

NOTICE

After this command is run, all files and directories are cleared from the SSD card and cannot be restored. Therefore, exercise caution when running this command.

If the SSD card is still unavailable after this command is run, a physical exception may have occurred.

Example

Format the SSD card.

```
<HUAWEI> format ssd
Warning: The format requires a long time. All data on SSD will be lost, proceed
with format, Continue? [Y/N]:y
Info: Operating, please wait for a moment.....
....
Info: Succeed in formating the SSD.
```

2.7.34 ftp

Function

The **ftp** command connects the FTP client to the FTP server and enters the FTP client view.

Format

Connect the FTP client to the FTP server based on the IPv4 address.

ftp [[**ssl-policy** *policy-name*] [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *host-ip* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]]

Connect the FTP client to the FTP server based on the IPv6 address.

ftp [**ssl-policy** *policy-name*] **ipv6** *host-ipv6* [*port-number*]

ftp [**ssl-policy** *policy-name*] **ipv6** *ipv6-linklocal-address* **-oi** { *interface-name* | *interface-type interface-number* } [*port-number*]

Parameters

Parameter	Description	Value
ssl-policy *policy-name*	Specifies the name of the SSL policy that provides the secure FTP function.	The value is a string of 1 to 23 case-insensitive characters without spaces.

Parameter	Description	Value
-a *source-ip-address*	Specifies the source IP address for connecting to the FTP client. You are advised to use the loopback interface IP address.	The value is in dotted decimal notation.
-i *interface-type interface-number*	Specifies the source interface type and ID. You are advised to use the loopback interface. The IP address configured for this interface is the source IP address for sending packets. If no IP address is configured for the source interface, the FTP connection cannot be set up.	-
host-ip	Specifies the IP address or host name of the remote IPv4 FTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
port-number	Specifies the port number of the FTP server.	The value is an integer that ranges from 1 to 65535. The default value is the standard port number 21.
public-net	Specifies the FTP server on the public network. You must set the **public-net** parameter when the FTP server IP address is a public network IP address.	-
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance where the FTP server is located.	The value must be an existing VPN instance name.

Parameter	Description	Value
host-ipv6	Specifies the IP address or host name of the remote IPv6 FTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
ipv6-linklocal-address	Specifies the local link address that is automatically generated by the remote IPv6 FTP server.	-
-oi	Specifies the outbound interface for the local IPv6 link address.	-
interface-name	Specifies the name of the outbound interface for the local IPv6 link address.	-
interface-typeinterface-number	Specifies the number of the outbound interface for the local IPv6 link address.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before accessing the FTP server on the FTP client, you must first run the **ftp** command to connect the FTP client to the FTP server. If an SSL-based secure FTP connection is set up between the device and remote FTP server, you must specify **ssl-policy**. If the connection is a common FTP connection, you do not need to specify this parameter.

Precautions

- Before running the **ftp** command to set up a secure FTP connection, you must perform the following steps on the FTP client:

a. In the system view, run the **ssl policy** command to create an SSL policy and enter the SSL policy view.
b. In the SSL policy view, run the **trusted-ca load** command to load a trusted CA.
c. In the SSL policy view, run the **crl load** command to load a CRL. This step is optional but recommended.

- You can set the source IP address to the source or destination IP address in the ACL rule when the **-a** or **-i** parameter is specified on the IPv4 network. This shields the IP address differences and interface status impact, filters incoming and outgoing packets, and implements security authentication.
- You can run the **set net-manager vpn-instance** command to configure the NMS management VPN instance before running the **open** command to connect the FTP client and server.
  - If **public-net** or **vpn-instance** is not specified, the FTP client accesses the FTP server in the VPN instance managed by the NMS.
  - If **public-net** is specified, the FTP client accesses the FTP server on the public network.
  - If **vpn-instance** *vpn-instance-name* is specified, the FTP client accesses the FTP server in a specified VPN instance.
- If no parameter is set in the **ftp** command, only the FTP client view is displayed, and no connection is set up between the FTP server and client.
- If the port number that the FTP server uses is non-standard, you must specify a standard port number; otherwise, the FTP server and client cannot be connected.
- When you run the **ftp** command, the system prompts you to enter the user name and password for logging in to the FTP server. You can log in to the FTP server if the user name and password are correct.
- If the number of login users exceeds the maximum value that the FTP server allows (that is, 5), other authorized users cannot log in to the FTP server. To allow news authorized users to log in to the FTP server, users who have performed FTP services must disconnect their clients from the FTP server. You can run the **bye** or **quit** command to disconnect the FTP client from the FTP server and return to the user view, or run the **close** or **disconnect** command to disconnect the FTP client from the FTP server and retain in the FTP client view.

Example

Connect to the FTP server whose IP address is 10.137.217.201.

```
<HUAWEI>ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp]
```

Connect to the remote IPv6 FTP server whose address is fc00:2001:db8::1.


```
<HUAWEI> ftp ipv6 fc00:2001:db8::1
Trying fc00:2001:db8::1
Press CTRL+K to abort
Connected to ftp fc00:2001:db8::1
220 FTP service ready.
User(fc00:2001:db8::1:(none)):huawei
331 Password required for huawei
Enter Password:
230 User logged in.

[ftp]
```

Connect to the FTPS server whose IP address is 10.1.1.2.

```
<HUAWEI> ftp ssl-policy ftp_server 10.1.1.2
Trying 10.1.1.2 ...
Press CTRL+K to abort
Connected to 10.1.1.2.
220 FTP service ready.
234 AUTH command successfully, Security mechanism accepted.
200 PBSZ is ok.
200 Data channel security level is changed to private.
User(10.1.1.2:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp]
```

2.7.35 ftp acl

Function

The **ftp acl** command specifies an ACL number for the current FTP server so that the FTP client with the same ACL number can access the FTP server.

The **undo ftp acl** command deletes an ACL number of the current FTP server.

By default, no ACL is configured for FTP server.

Format

ftp [**ipv6**] **acl** *acl-number*

undo ftp [**ipv6**] **acl**

Parameters

Parameter	Description	Value
ipv6	Specifies the IPv6 FTP server.	-
acl-number	Specifies the number of the ACL.	The value is an integer that ranges from 2000 to 3999.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the device functions as an FTP server, you can configure an access control list (ACL) on the device to control the source IP address, destination IP address, source port, destination port, VPN instance, and packets whose protocol type is TCP, allows specific clients to log in to the device through FTP.

Precautions

The **ftp server acl** command takes effect only after you run the **rule** command to configure the ACL rule.

Example

Allow the client whose ACL number is 2000 to log in to the FTP server.

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule permit source 10.10.10.1 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] ftp acl 2000
```

2.7.36 ftp client-source

Function

The **ftp client-source** command specifies the source IP address for the FTP client to send packets.

The **undo ftp client-source** command restores the default source IP address for the FTP client to send packets.

The default source IP address for the FTP client to send packets is 0.0.0.0.

Format

ftp client-source { **-a** *source-ip-address* | **-i** *interface-type interface-number* }

undo ftp client-source

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the IPv4 address of the source interface on the local device.	The value is in dotted decimal notation.

Parameter	Description	Value
-i *interface-type interface-number*	Specifies the source interface of the local device. The IP address configured for the source interface is the source IP address for sending packets. If no IP address is configured for the source interface, the FTP connection cannot be set up.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If no source IP address is specified, the client uses the source IP address that the router specifies to send packets. The source IP address must be configured for an interface with stable performance. The loopback interface is recommended. Using the loopback interface as the source interface simplifies the ACL rule and security policy configuration. This shields the IP address differences and interface status impact, filters incoming and outgoing packets, and implements security authentication.

Prerequisites

Before you specify a logical interface as the source interface, ensure that the interface to be specified is created and has an IP address configured. Before you specify a physical interface as the source interface, ensure that the interface has an IPv4 address configured. Otherwise, the **ftp server-source** command cannot be successfully executed.

Precautions

- You can also run the **ftp** command to configure the source IP address whose priority is higher than that of the source IP address specified by the **ftp client-source** command. If you specify the source IP addresses by running the **ftp client-source** and **ftp** commands, the source IP address specified by the **ftp** command is used for data communication and is available only for the current FTP connection, while the source IP address specified by the **ftp client-source** command is available for all FTP connections.
- The IP address that a user displays on the FTP server is the specified source IP address or source interface IP address.
- No source address or source interface is specified, so security risks exist.

Example

Set the source IP address of the FTP client to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] ftp client-source -a 10.1.1.1
Info: Succeeded in setting the source address of the FTP client to 10.1.1.1.
```

2.7.37 ftp secure-server enable

Function

The **ftp secure-server enable** command enables the secure FTP server function for FTP users.

The **undo ftp secure-server** command disables the secure FTP server function.

By default, the secure FTP server function is disabled.

Format

ftp [**ipv6**] **secure-server enable**

undo ftp [**ipv6**] **secure-server**

Parameters

Parameter	Description	Value
ipv6	Specifies the IPv6 FTP server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After SSL policies are configured on an FTP server, the secure FTP server function is provided based on SSL policies. To use the secure FTP server function, you must run the **ftp secure-server enable** command to enable the secure FTP server function. You can log in to the FTP server with secure FTP function configured from a client, and manage files between the FTP server and client.

Prerequisites

To enable the secure FTP server function, you must disable the common FTP server function.

Precautions

- If the FTP server function is disabled, no user can log in to the FTP server, and users who have logged in to the FTP server cannot perform any operation except logout.
- After the **ftp secure-server enable** command is run, the FTP server does not accept login requests from any interface by default, you should run the **ftp server-source** command to specify the source interface of the FTP server.
- After the **ftp ipv6 secure-server enable** command is run, the FTP server does not accept login requests from any IPv6 address by default, you should run the **ftp ipv6 server-source** command to specify the IPv6 source address for the FTP server.

Example

Enable the secure FTP server function.

```
<HUAWEI> system-view
[HUAWEI] ftp secure-server enable
```

2.7.38 ftp secure-server ssl-policy

Function

The **ftp secure-server ssl-policy** command configures an SSL policy for the FTP server.

The **undo ftp secure-server ssl-policy** command deletes an SSL policy from the FTP server.

By default, no SSL policy is configured for the FTP server.

Format

ftp secure-server ssl-policy *policy-name*

undo ftp secure-server ssl-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an SSL policy.	The value is a string of 1 to 23 case-insensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The traditional FTP function transmits data in plain text, which can be intercepted and tampered with. You can run the **ftp secure-server ssl-policy** command to configure an SSL policy for the FTP server to ensure data security so that the FTP server implements session negotiation, sets up connections, and transmits data based on the SSL policy. You can log in to the FTP server from a client and manage files between the FTP server and client.

Prerequisites

Before running the **ftp secure-server ssl-policy** command to configure the SSL policy, you must first run the **ssl policy** command to create an SSL policy for the FTP server.

Precautions

- You must apply for a digital certificate for the FTP client from a trusted CA to authenticate the validity of the FTP server digital certificate.
- Only one SSL policy can be configured for the FTP server, and the latest configured SSL policy takes effect.

Example

Configure an SSL policy for the FTP server.

```
<HUAWEI> system-view
[HUAWEI] ftp secure-server ssl-policy ftp_server
```

2.7.39 ftp server enable

Function

The **ftp server enable** command enables the FTP server function to allow FTP users to log in to the FTP server.

The **undo ftp server** command disables the FTP server function so that FTP users cannot log in to the FTP server.

By default, the FTP function is disabled.

Format

ftp [**ipv6**] **server enable**

undo ftp [**ipv6**] **server**

Parameters

Parameter	Description	Value
ipv6	Specifies the IPv6 FTP server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To manage FTP server files on a client, you must run the **ftp server enable** command to enable the FTP server function to allow FTP users to log in to the FTP server.

Prerequisites

Before enabling the FTP service, run either of the following commands as required:

- Run the **ftp server-source -i** *interface-type interface-number* command to configure a specified interface as the source interface of the FTP server or run the **ftp server-source all-interface** command to specify any interface with an IPv4 address configured on the device as the source interface of the FTP server.
- Run the **ftp ipv6 server-source -a** *ipv6_address* [**vpn-instance** *vpn_name*] command to configure a specified IPv6 address as the IPv6 source address of the FTP server or run the **ftp ipv6 server-source all-interface** command to specify any interface IPv6 address on the device as the IPv6 source address of the FTP server.

Precautions

If the FTP server function is disabled, no user can log in to the FTP server, and users who have logged in to the FTP server cannot perform any operation except logout.

NOTICE

The FTP protocol compromises device security. SFTP V2 or FTPS mode is recommended.

Example

Enable the FTP server function.

```
<HUAWEI> system-view
[HUAWEI] ftp server enable
Warning: FTP is not a secure protocol, and it is recommended to use SFTP.
Info: Succeeded in starting the FTP server.
```


2.7.40 ftp server max-sessions

Function

The **ftp server max-sessions** command sets the maximum number of sessions supported by the FTP server.

The **undo ftp server max-sessions** command restores the maximum number of sessions supported by the FTP server to the default value.

By default, the FTP server supports a maximum of five sessions.

Format

ftp [**ipv6**] **server max-sessions** *max-sessions-number*

undo ftp [**ipv6**] **server max-sessions**

Parameters

Parameter	Description	Value
ipv6	Specifies the IPv6 FTP server.	-
max-sessions *max-sessions-number*	Specifies the maximum number of sessions supported by the FTP server.	The value is an integer ranging from 0 to 5.

Views

System view

Default Level

3: Management level

Usage Guidelines

You can run this command to set the maximum number of sessions supported by the FTP server. When the number of online users is equal to the maximum number of sessions supported by the FTP server, other users cannot log in to the FTP server.

Example

Set the maximum number of sessions supported by the FTP server to 3.

```
<HUAWEI> system-view
[HUAWEI] ftp server max-sessions 3
```


2.7.41 ftp server port

Function

The **ftp server port** command specifies the listening port number of the FTP server.

The **undo ftp server port** command restores the default value of the listening port number.

The default value is 21.

Format

ftp [**ipv6**] **server port** *port-number*

undo ftp [**ipv6**] **server port**

Parameters

Parameter	Description	Value
ipv6	Specifies the IPv6 FTP server.	-
port *port-number*	Specifies the listening port number of the FTP server.	The value is 21 or an integer that ranges from 1025 to 55535.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, the listening port number of the FTP server is 21. Attackers may frequently access the default listening port, which wastes bandwidth, deteriorates server performance, and prevents authorized users from accessing the FTP server through the listening port. You can run the **ftp server port** command to specify another listening port number to prevent attackers from accessing the listening port.

Prerequisites

Before running the **ftp server port** command to specify the listening port number, you must first run the **undo ftp server** command to disable FTP services.

Precautions

- After the **ftp server port** command is executed, the FTP server disconnects all FTP connections and uses the new listening port.

- If the current listening port number is 21, FTP client users do not need to specify the port number for logging in to the FTP server. If the current listening port number is not 21, FTP client users must use the FTP server's listening port number to log in to the FTP server.
- After the listening port number is changed, you must run the **ftp server enable** command to enable FTP services to make the configuration take effect.

Example

Change the port number of the FTP server to 1028.

```
<HUAWEI> system-view
[HUAWEI] undo ftp server
[HUAWEI] ftp server port 1028
```

2.7.42 ftp server-source

Function

The **ftp server-source** command specifies the source IP address for an FTP server to send packets.

The **undo ftp server-source** command restores the default source IP address for an FTP server to send packets.

By default, the source IP address of an FTP server is not specified.

Format

ftp server-source { **-a** *source-ip-address* | **-i** *interface-type interface-number* }

undo ftp server-source

ftp server-source all-interface

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the IPv4 address of the source interface on the local device.	The value is in dotted decimal notation.
-i *interface-type interface-number*	Specifies the source interface of the local device. The primary IP address of the source interface is the source IP address for sending packets. If no IP address is configured for the source IP address, the FTP connection cannot be set up.	-

Parameter	Description	Value
all-interface	Indicates that any interface that has an IPv4 address configured can be used as the source interface of an FTP server.	-

NOTE

In V200R020C00 and later versions, the source address for the FTP server to send packets is not specified by default. To allow authorized users to log in to the server, run a command to specify the source interface or source address of the server. For details about the command, see "Usage Scenario" in "Usage Guidelines" in this section.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In versions earlier than V200R020C00, the default source IP address for the FTP server to send packets is 0.0.0.0, incurring security risks. For details, see the product documentation of the corresponding version.

In V200R020C00 and later versions, the default source IP address for the FTP server to send packets is not specified. To allow authorized users to log in to the FTP server, run either of the following commands to specify the source IP address of the FTP server.

- Run the **ftp server-source -i** *interface-type interface-number* command to configure a specified interface as the source interface of the FTP server.
- Run the **ftp server-source all-interface** command to configure all interfaces configured with IPv4 addresses as the source interfaces of the FTP server.

Prerequisites

Before you specify a logical interface as the source interface, ensure that the interface to be specified is created and has an IP address configured. Before you specify a physical interface as the source interface, ensure that the interface has an IPv4 address configured. Otherwise, the **ftp server-source** command cannot be successfully executed.

Precautions

- After the source IP address is specified for the FTP server, you must use the specified IP address to log in to the FTP server.
- If the FTP service has been enabled, the FTP service restarts after the **ftp server-source** command is executed.

- After the **ftp server-source all-interface** command is run, the system allows FTP users to log in to the FTP server through all interfaces with IPv4 addresses configured. This increases system security risks. Therefore, you are not advised to run this command.

Example

Set the source IP address of the FTP server to **LoopBack0**.

```
<HUAWEI> system-view
[HUAWEI] ftp server-source -i loopback 0
Warning: To make the server source configuration take effect, the FTP server will be restarted. Continue? [Y/
N]: y
Info: Succeeded in setting the source interface of the FTP server to LoopBack0.
Info: Succeeded in starting the FTP server.
```

2.7.43 ftp ipv6 server-source

Function

The **ftp ipv6 server-source** command specifies an IPv6 source address for an FTP server.

The **undo ftp ipv6 server-source** command cancels the IPv6 source address specified for an FTP server.

By default, the IPv6 source address of an FTP server is not specified.

Format

ftp ipv6 server-source -a *ipv6_address* [**vpn-instance** *vpn_name*]

undo ftp ipv6 server-source

ftp ipv6 server-source all-interface

Parameters

Parameter	Description	Value
-a *ipv6_address*	Specifies an IPv6 source address for an FTP server.	The total length of an IPv6 source address is 128 bits, which are divided into eight groups. Each group contains four hexadecimal digits. The value is in the format X:X:X:X:X:X:X:X.
vpn-instance *vpn_name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain spaces. The VPN instance name cannot be **_public_**. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Parameter	Description	Value
all-interface	Indicates that any interface IPv6 address on the device can be used as the IPv6 source address of the FTP server.	-

NOTE

In V200R020C00 and later versions, the source address for the FTP server to send packets is not specified by default. To allow authorized users to log in to the server, run a command to specify the source interface or source address of the server. For details about the command, see "Usage Scenario" in "Usage Guidelines" in this section.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In versions earlier than V200R020C00, the default source IP address for the FTP server to send packets is ::, incurring security risks. For details, see the product documentation of the corresponding version.

In V200R020C00 and later versions, the default source IP address for the FTP server to send packets is not specified. To allow authorized users to log in to the FTP server, run either of the following commands to specify the source IP address of the FTP server.

- Run the **ftp ipv6 server-source -a** *ipv6_address* [**vpn-instance** *vpn_name*] command to specify the specified IPv6 address as the IPv6 source address of the FTP server.
- Run the **ftp ipv6 server-source all-interface** command to specify all interface IPv6 addresses on the device as the IPv6 source addresses of the FTP server.

Prerequisites

A VPN instance has been created before you specify it for an FTP server. Otherwise, the **ftp ipv6 server-source** command cannot be executed.

Configuration Impact

After an IPv6 source address is specified for an FTP server, FTP users can log in to the FTP server only using this IPv6 address. This configuration applies to the FTP users who attempt to log in to the FTP server, not to the FTP users who have logged in to the server.

Precautions

After an IPv6 source address is specified for an FTP server using this command, ensure that FTP users can access this IPv6 address at Layer 3. Otherwise, FTP users will fail to log in to the FTP server.

If the specified IPv6 source address is bound to a VPN instance, the FTP server is also bound to the VPN instance.

After the **ftp ipv6 server-source all-interface** command is run, the system allows FTP users to log in to the FTP server through all interfaces with IPv6 addresses configured. This increases system security risks. Therefore, running this command is not recommended.

Example

Specify the IPv6 source address 2001:DB8:: for an FTP server.

```
<HUAWEI> system-view
[HUAWEI] ftp ipv6 server-source -a 2001:DB8::
```

2.7.44 ftp timeout

Function

The **ftp timeout** command configures the idle timeout duration of the FTP server.

The **undo ftp timeout** command restores the default idle timeout duration.

By default, the idle timeout duration of the FTP server is 10 minutes.

Format

ftp [**ipv6**] **timeout** *minutes*

undo ftp [**ipv6**] **timeout**

Parameters

Parameter	Description	Value
ipv6	Specifies the IPv6 FTP server.	-
minutes	Specifies idle timeout duration.	The value is an integer that ranges from 1 to 35791, in minutes. By default, the idle timeout duration is 10 minutes.

Views

System view

Default Level

3: Management level

Usage Guidelines

After a user logs in to the FTP server, a connection is set up between the FTP server and the user's client. The idle timeout duration is configured to release the connection when the connection is interrupted or when the user performs no operation for a specified time.

NOTICE

When you use the **get** command in the FTP view to overwrite a file, the operation may fail due to timeout of the FTP connection. To prevent this problem, set a long timeout period for the FTP connection.

Example

Set the idle timeout duration to 36 minutes.

```
<HUAWEI> system-view
[HUAWEI] ftp timeout 36
```

2.7.45 get (SFTP client view)

Function

The **get** command downloads a file from the SFTP server and saves the file to the local device.

Format

get *remote-filename* [*local-filename*]

Parameters

Parameter	Description	Value
remote-filename	Specifies the name of the file to be downloaded from the SFTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.
local-filename	Specifies the name of a downloaded file to be saved to the local device.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **get** command to download files from the FTP server to upgrade devices.

Precautions

- If *local-filename* is not specified on the local device, the original file name is used.
- If the name of the downloaded file is the same as that of an existing local file, the system prompts you whether to overwrite the existing file.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Download a file from the SFTP server.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> get test.txt
Remote file: / test.txt --->  Local file: test.txt
Info: Downloading file successfully ended.
```

2.7.46 get (FTP client view)

Function

The **get** command downloads a file from the FTP server and saves the file to the local device.

Format

get *remote-filename* [*local-filename*]

Parameters

Parameter	Description	Value
remote-filename	Specifies the name of the file to be downloaded from the FTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.
local-filename	Specifies the name of a downloaded file to be saved to the local device.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **get** command to download system software, backup configuration files, and patch files from the FTP server to upgrade devices.

Precautions

- If the downloaded file name is not specified on the local device, the original file name is used.
- If the name of the downloaded file is the same as that of an existing local file, the system prompts you whether to overwrite the existing file.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Download the system software **devicesoft.cc** from the FTP server.

```
<HUAWEI>ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] get devicesoft.cc
200 Port command successful. 150 Opening BINARY mode data connection for file transfer. 226 Transfer complete  FTP: 6482944 byte(s) received in 54.500 second(s) 1117.40Kbyte(s)/sec.
```

2.7.47 help (SFTP client view)

Function

The **help** command displays the help information in the SFTP client view.

Format

help [**all** | *command-name*]

Parameters

Parameter	Description	Value
all	Displays all commands in the SFTP client view.	-
command-name	Displays the format and parameters of a specified command in the SFTP client view.	-

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In the SFTP view, you can only enter the question mark (?) to obtain all commands in the SFTP client view. If you enter a command keyword and the question mark (?) to query command parameters, an error message is displayed, as shown in the following:

```
sftp-client> dir ?
Error: Failed to list files.
```

You can run the **help** command to obtain the help information and display all commands or a command format in the SFTP client view.

Precautions

If you specify no parameter when running the **help** command, all commands in the SFTP client view are displayed. This has the same effect as the **help all** command or directly entering the question mark (?) in the SFTP client view.

Example

Display the format of the command **get**.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> help get
get Remote file name STRING<1-64>   [Local file name STRING<1-64>]  Download file
Default local file name is the same with remote file.
```

Display all commands in the SFTP client view.

```
sftp-client> help all
cd
cdup
dir
get
```



```
help
ls
mkdir
put
pwd
quit
rename
remove
rmdir
```

2.7.48 lcd

Function

The **lcd** command displays and changes the local working directory of the FTP client in the FTP client view.

Format

lcd [*local-directory*]

Parameters

Parameter	Description	Value
local-directory	Specifies the local working directory of the FTP client.	The value is a string of 1 to 128 case-insensitive characters without spaces.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **lcd** command to display the local working directory of the FTP client when uploading or downloading files, and set the upload or download path to the path of the local working directory.

Precautions

The **lcd** command displays the local working directory of the FTP client, while the **pwd** command displays the working directory of the FTP server. If you specify the parameter *local-directory* in the **lcd** command, you can directly change the local working directory in the FTP client view.

Example

Change the local working directory to **flash:/test**.


```
<HUAWEI> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] lcd
The current local directory is flash:.
[ftp] lcd flash:/test
The current local directory is flash:/test.
```

2.7.49 mget

Function

The **mget** command downloads multiple files from the remote FTP server to the local device.

Format

mget *remote-filenames*

Parameters

Parameter	Description	Value
remote-filenames	Specifies multiple files to download to the local device. File names are separated using spaces, and the wildcard (*) is supported.	The value is a string of 1 to 255 characters.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **mget** command to download multiple files at the same time.

Precautions

- The command cannot download all files in a directory or subdirectory.
- If the name of the downloaded file is the same as that of an existing local file, the system prompts you whether to overwrite the existing file.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Download files **1.txt**, **2.txt**, and **vrp221.cfg** from the remote FTP server.

```
<HUAWEI> ftp 10.10.10.1
Trying 10.10.10.1 ...
Press CTRL+K to abort
Connected to 10.10.10.1.
220 FTP service ready.
User(10.10.10.1:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] mget 1.txt 2.txt vrp221.cfg
200 Port command okay.
150 Opening ASCII mode data connection for 1.txt.

226 Transfer complete.
FTP: 3885 byte(s) received in 0.174 second(s) 22.32Kbyte(s)/sec.

200 Port command okay.
150 Opening ASCII mode data connection for 2.txt.

226 Transfer complete.
FTP: 8721 byte(s) received in 0.179 second(s) 48.72Kbyte(s)/sec.

200 Port command okay.
150 Opening ASCII mode data connection for vrp221.cfg.

226 Transfer complete.
FTP: 6700 byte(s) received in 0.151 second(s) 44.37Kbyte(s)/sec.

[ftp]
```

2.7.50 mkdir (FTP client view)

Function

The **mkdir** command creates a directory on the remote FTP server.

Format

mkdir *remote-directory*

Parameters

Parameter	Description	Value
remote-directory	Specifies the directory to be created.	The value is a string of case-insensitive characters without spaces. The absolute path length ranges from 1 to 64, while the directory name length ranges from 1 to 15.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

- You can run the **mkdir** command to create a subdirectory in a specified directory, and the subdirectory name must be unique.
- If no path is specified when you create a subdirectory, the subdirectory is created in the current directory.
- The created directory is stored on the FTP server.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Create a directory **test** on the remote FTP server.

```
<HUAWEI> ftp 172.16.104.110
Trying 172.16.104.110 ...
Press CTRL+K to abort
Connected to 172.16.104.110.
220 FTP service ready.
User(172.16.104.110:(none)):huawei
331 Password required for huawei
Enter password:
230 User logged in.

[ftp] mkdir test
257 "test" new directory created.
```

2.7.51 mkdir (SFTP client view)

Function

The **mkdir** command creates a directory on the remote SFTP server.

Format

mkdir *remote-directory*

Parameters

Parameter	Description	Value
remote-directory	Specifies the directory to be created.	The value is a string of case-insensitive characters without spaces. The absolute path length ranges from 1 to 64, while the directory name length ranges from 1 to 15.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

- You can run the **mkdir** command to create a subdirectory in a specified directory, and the subdirectory name must be unique.
- If no path is specified when you create a subdirectory, the subdirectory is created in the current directory.
- The created directory is stored on the SFTP server.
- After a directory is created, you can run the **dir/ls (SFTP client view)** command to view the directory.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Create a directory on the SFTP server.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> mkdir ssh
Info: Succeeded in creating a directory.
```

2.7.52 mkdir (User view)

Function

The **mkdir** command creates a directory in the current storage device.

Format

mkdir *directory*

Parameters

Parameter	Description	Settings
directory	Specifies a directory or directory and its path.	The value is a string of case-insensitive characters in the **[drive] [path] directory** format. The absolute path length ranges from 1 to 64, while the directory name length ranges from 1 to 15. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. The directory name cannot contain the following characters: ~ * / \ : ' "

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the drive name.

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

If you only the subdirectory name is specified, a subdirectory is created in the current working directory. You can run the **pwd** command to query the current working directory. If the subdirectory name and directory path are specified, the subdirectory is created in the specified directory.

Precautions

- The subdirectory name must be unique in a directory; otherwise, the message "Error: Directory already exists." is displayed.
- A maximum of four directory levels are supported when you create a directory.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Create the subdirectory **new** in the flash card.

```
<HUAWEI> mkdir flash:/new
Info: Create directory flash:/new.....Done.
```

2.7.53 more

Function

The **more** command displays the content of a specified file.

Format

more *filename* [*offset*] [**all**]

Parameters

Parameter	Description	Value
filename	Specifies the file name.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "
offset	Specifies the file offset.	The value is an integer that ranges from 0 to 2147483647, in bytes.
all	Displays all the file content on one screen.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **more** command to display the file content directly on a device.

- The following describes the drive name.
  - **drive** is the storage device and is named as **flash:**.
  - If devices are stacked, **drive** can be named as:
    - flash: root directory of the flash memory of the master switch in the stack.
    - chassis ID#flash: root directory of the flash memory on a device in the stack.

    For example, **slot2#flash:** indicates the flash memory in slot 2.
- The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working

directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Precautions

- You are not advised to use this command to display non-text files; otherwise, the terminal is shut down or displays garbled characters, which is harmless to the system.
- Files are displayed in text format.
- You can display the file content flexibly by specifying parameters before running the **more** command:
  - You can run the **more** *filename* command to view a specified text file. The content of the specified text file is displayed on multiple screens. You can press the spacebar consecutively on the current session GUI to display all content of the file.

    To display the file content on multiple screens, you must ensure that:

    - The number of lines that can be displayed on a terminal screen is greater than 0. (The number of lines that can be displayed on a terminal screen is set by running the **screen-length** command.)
    - The total number of file lines is greater than the number of lines that can be displayed on a terminal screen. (The number of lines that can be displayed on a terminal screen is set by running the **screen-length** command.)
  - You can run the **more** *filename offset* command to view a specified file. The content of the specified text file starting from *offset* is displayed on multiple screens. You can press the spacebar consecutively on the current session GUI to display all content of the file.

    To display the file content on multiple screens, you must ensure that:

    - The number of lines that can be displayed on a terminal screen is greater than 0. (The number of lines that can be displayed on a terminal screen is set by running the **screen-length** command.)
    - The number of lines starting from *offset* in the file is greater than the number of lines that can be displayed on a terminal screen. (The number of lines that can be displayed on a terminal screen is set by running the **screen-length** command.)
  - You can run the **more** *file-name* **all** command to view a specified file. The file content is displayed on one screen.

Example

Display the content of the file **test.bat**.

```
<HUAWEI> more test.bat
rsa local-key-pair create
```



```
user-interface vty 12 14
authentication-mode aaa
protocol inbound ssh
user privilege level 5
quit
ssh user sftpuser authentication-type password
ssh user sftpuser service-type all
sftp server enable
```

Display the content of the file **log.txt** and set the offset to 100.

```
<HUAWEI> more log.txt 100
:               CHINA HUAWEI TECHNOLOGY LIMITTED CO.,LTD
#   FILE NAME:                Product Adapter File(PAF)
#   PURPOSE:                  MAKE VRPV5 SUITABLE FOR DIFFERENT PRODUCT IN LIB
#   SOFTWARE PLATFORM:          V6R2C00
#   DETAIL VERSION:             B283
#   DEVELOPING GROUP:           8090 SYSTEM MAINTAIN GROUP
#   HARDWARE PLATFORM:           8090 (512M Memory)
#   CREATED DATE:               2003/05/10
#   AUTH:                      RAINBOW
#   Updation History:           Kelvin dengqiulin update for 8090(2004.08.18)
#                            lmg update for R3(2006.11.7)
#                            fsr update for R5 (2008.1.18)
#                            qj update for R6 (2008.08.08)
#   COPYRIGHT:                        2003---2008
#-------------------------------------------------------------------------------


#BEGIN FOR RESOURCE DEFINATION
[RESOURCE]
FORMAT: SPECS RESOURCE NAME STRING = CONTROLLABLE(1 : ABLE , 0: NOT ABLE),DEFAUL
T VALUE , MAX VALUE , MIN VALUE
#BEGIN  SPECS RESOURCE FOR TE tunnel Nto1 PS MODULE
PAF_LCS_TUNNEL_SPECS_TE_PS_MAX_PROTECT_NUM = 1, 8, 16, 1
PAF_LCS_TUNNEL_SPECS_TE_PS_REBOOT_TIME     = 1, 180000, 3600000, 60000
  ---- More ----
```

2.7.54 move

Function

The **move** command moves the source file from a specified directory to a destination directory.

Format

move *source-filename destination-filename*

Parameters

Parameter	Description	Settings
source-filename	Specifies the directory and name of a source file.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "

Parameter	Description	Settings
destination-filename	Specifies the directory and name of a destination file.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the drive name.

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Precautions

- If the destination file has the same name as an existing file, the system prompts you whether to overwrite the existing file. The system prompt is displayed only when **file prompt** is set to **alert**. If **file prompt** is set to **quiet**, no prompt is displayed.
- The **move** and **copy** commands have different effects:
  - The **move** command moves the source file to the destination directory.
  - The **copy** command copies the source file to the destination directory.

Example

Move a file from **flash:/test/sample.txt** to **flash:/sample.txt**.

```
<HUAWEI> move flash:/test/sample.txt flash:/sample.txt
Move flash:/test/sample.txt to flash:/sample.txt ?[Y/N]: y
%Moved file flash:/test/sample.txt to flash:/sample.txt.
```

2.7.55 mput

Function

The **mput** command uploads multiple files from the local device to the remote FTP server.

Format

mput *local-filenames*

Parameters

Parameter	Description	Value
local-filenames	Specifies files to be uploaded. File names are separated using spaces, and the wildcard (*) is supported.	The value is a string of 1 to 255 characters.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **mput** command to upload multiple files to the remote FTP server at the same time, especially in the upgrade scenario.

Precautions

If the name of the uploaded file is the same as that of an existing file on the FTP server, the system overwrites the existing file.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Upload two local files **111.text** and **vrp222.cfg** to the remote FTP server.

```
<HUAWEI> ftp 10.10.10.1
Trying 10.10.10.1 ...
Press CTRL+K to abort
Connected to 10.10.10.1.
220 FTP service ready.
User(10.10.10.1:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] mput 111.txt vrp222.cfg
200 Port command successful.
150 Opening ASCII mode data connection for file transfer.
226 Transfer complete.
FTP: 6556 byte(s) sent in 0.231 second(s) 28.38Kbyte(s)/sec.

200 Port command successful.
150 Opening ASCII mode data connection for file transfer.
226 Transfer complete.
FTP: 4198 byte(s) sent in 0.171 second(s) 24.54Kbyte(s)/sec.

[ftp]
```

2.7.56 open

Function

The **open** command connects the FTP client and server.

Format

Connect the FTP client to the FTP server based on the IPv4 address.

open [**ssl-policy** *policy-name*] [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *host-ip* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]

Connect the FTP client to the FTP server based on the IPv6 address.

open [**ssl-policy** *policy-name*] **ipv6** *host-ipv6* [*port-number*]

If the connection address is the IPv6 link-local address generated automatically by the interface of the remote IPv6 FTP server, the command format is as follows:

open [**ssl-policy** *policy-name*] **ipv6** *ipv6-linklocal-address* **-oi** *interface-type interface-number* [*port-number*]

Parameters

Parameter	Description	Value
ssl-policy *policy-name*	Specifies the name of the SSL policy that provides the secure FTP function.	The value is a string of 1 to 23 case-insensitive characters without spaces.
-a *source-ip-address*	Specifies the source IP address for connecting to the FTP client. You are advised to use the loopback interface IP address.	-
-i *interface-type interface-number*	Specifies the source interface type and ID. You are advised to use the loopback interface. The IP address configured for this interface is the source IP address for sending packets. If no IP address is configured for the source interface, the FTP connection cannot be set up.	-
host-ip	Specifies the IP address or host name of the remote IPv4 FTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
port-number	Specifies the port number of the FTP server.	The value is an integer that ranges from 1 to 65535. The default value is the standard port number 21.

Parameter	Description	Value
public-net	Specifies the FTP server on the public network. You must set the **public-net** parameter when the FTP server IP address is a public network IP address.	-
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance where the FTP server is located.	The value must be an existing VPN instance name.
host-ipv6	Specifies the IP address or host name of the remote IPv6 FTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
ipv6-linklocal-address	Specifies the IPv6 link-local address generated automatically by the interface of the remote IPv6 FTP server.	-
-oi	Indicates the outbound interface of the IPv6 link-local address.	-
interface-typeinterface-number	Specifies the outbound interface type and number of the IPv6 link-local address.	-

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **open** command in the FTP client view to connect the FTP client to the server to transmit files and manage files and directories of the FTP server.

Precautions

- You can run the **ftp** command in the user view to connect the FTP client and server and enter the FTP client view.
- Before enabling the FTP or FTPS function and specifying the **ssl-policy** *policy-name* parameter, you must first configure an SSL policy.
- You can set the source IP address to the source or destination IP address in the ACL rule when the **-a** or **-i** parameter is specified on the IPv4 network. This shields the IP address differences and interface status impact, filters incoming and outgoing packets, and implements security authentication.
- You can run the **set net-manager vpn-instance** command to configure the NMS management VPN instance before running the **open** command to connect the FTP client and server.
  - If **public-net** or **vpn-instance** is not specified, the FTP client accesses the FTP server in the VPN instance managed by the NMS.
  - If **public-net** is specified, the FTP client accesses the FTP server on the public network.
  - If **vpn-instance** *vpn-instance-name* is specified, the FTP client accesses the FTP server in a specified VPN instance.
- If the port number that the FTP server uses is non-standard, you must specify a standard port number; otherwise, the FTP server and client cannot be connected.
- When you run the **open** command, the system prompts you to enter the user name and password for logging in to the FTP server. You can log in to the FTP client and enter the FTP client view if the user name and password are correct.

Example

Connect the FTP client with the FTP server whose IP address is 10.137.217.204.

```
<HUAWEI> ftp
[ftp] open 10.137.217.204
Trying 10.137.217.204 ...
Press CTRL+K to abort
Connected to 10.137.217.204.
220 FTP service ready.
User(10.137.217.204:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp]
```

Connect the FTP client with the FTP server whose IP address is fc00:2001:db8::1.

```
<HUAWEI> ftp
[ftp] open ipv6 fc00:2001:db8::1
Trying fc00:2001:db8::1 ...
Press CTRL+K to abort
Connected to fc00:2001:db8::1
220 FTP service ready.
User(fc00:2001:db8::1:(none)):huawei
331 Password required for huawei
Enter Password:
230 User logged in.

[ftp]
```


2.7.57 passive

Function

The **passive** command sets the data transmission mode to passive.

The **undo passive** command sets the data transmission mode to active.

By default, the data transmission mode is active.

Format

passive

undo passive

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

The device supports the active and passive data transmission modes. In active mode, the server initiates a connection request, and the client and server need to enable and monitor a port to establish a connection. In passive mode, the client initiates a connection request, and only the server needs to monitor the corresponding port. This command is used together with the firewall function. When the client is configured with the firewall function, FTP connections are restricted between internal clients and external FTP servers if the FTP transmission mode is active. If the FTP transmission mode is passive, FTP connections between internal clients and external FTP servers are not restricted.

Example

Set the data transmission mode to passive.

```
<HUAWEI> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] passive
Info: Succeeded in switching passive on.
```


2.7.58 prompt

Function

The **prompt** command enables the prompt function when files are transmitted between the FTP client and server.

The **undo prompt** command disables the prompt function.

By default, the prompt function is disabled.

Format

prompt

undo prompt

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can enable the prompt function as required when transmitting files between the FTP client and server.

Precautions

- The **prompt** command can be used when you run the **put**, **mput**, **get**, and **mget** commands.
- The prompt function can be enabled only for confirming service upload and download.
  - When you run the **put** or **mput** command, the system always overwrites the existing file if the name of the uploaded file is the same as that of an existing file on the FTP server.
  - When you run the **get** or **mget** command, the system always prompts you whether to overwrite the existing file if the name of the uploaded file is the same as an existing file name in the specified directory.

Example

Enable the FTP message prompt function.

```
<HUAWEI> ftp 10.137.217.201
Trying 10.137.217.201 ...
```



```
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] prompt
Info: Succeeded in switching prompt on.
```

Disable the FTP message prompt function.

```
[ftp] undo prompt
Info: Succeeded in switching prompt off.
```

2.7.59 put (FTP client view)

Function

The **put** command uploads a local file to the remote FTP server.

Format

put *local-filename* [*remote-filename*]

Parameters

Parameter	Description	Value
local-filename	Specifies the local file name of the FTP client.	The value is a string of 1 to 64 case-insensitive characters without spaces.
remote-filename	Specifies the name of the file to be uploaded to the remote FTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **put** command to upload a local file to the remote FTP server for further check and backup. For example, you can upload the local log file to the FTP server for other users to check, and upload the configuration file to the FTP server as a backup before upgrading the device.

Precautions

- If the file name is not specified on the remote FTP server, the local file name is used.
- If the name of the uploaded file is the same as that of an existing file on the FTP server, the system overwrites the existing file.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Upload the configuration file **vrpcfg.zip** to the remote FTP server as a backup, and save it as **backup.zip**.

```
<HUAWEI> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] put vrpcfg.zip backup.zip
200 Port command successful.
150 Opening BINARY mode data connection for file transfer.
226 Transfer complete
FTP: 1098 byte(s) sent in 0.131 second(s) 8.38Kbyte(s)/sec.
```

2.7.60 put (SFTP client view)

Function

The **put** command uploads a local file to a remote SFTP server.

Format

put *local-filename* [*remote-filename*]

Parameters

Parameter	Description	Value
local-filename	Specifies a local file name on the SFTP client.	The value is a case-insensitive character string without spaces. The file name (including the absolute path) contains 1 to 64 characters.
remote-filename	Specifies the name of the file uploaded to the remote SFTP server.	The value is a case-insensitive character string without spaces. The file name (including the absolute path) contains 1 to 64 characters.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command enables you to upload files from the local device to a remote SFTP server to view the file contents or back up the files. For example, you can upload log files of a device to an SFTP server and view the logs in the server. During an upgrade, you can upload the configuration file of the device to the SFTP server for backup.

Precautions

- If *remote-filename* is not specified, the uploaded file is saved on the remote SFTP server with the original file name.
- If the specified *remote-filename* is the same as an existing file name on the SFTP server, the uploaded file overwrites the existing file on the server.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Upload a file to the SFTP server.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> put wm.cfg
local file: wm.cfg --->  Remote file: /wm.cfg
Info: Uploading file successfully ended.
```

2.7.61 pwd (FTP client view)

Function

The **pwd** command displays the FTP client's working directory on the remote FTP server.

Format

pwd

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

After logging in to the FTP server, you can run the **pwd** command to display the FTP client's working directory on the remote FTP server.

If the displayed working directory is incorrect, you can run the **cd** command to change the FTP client's working directory on the remote FTP server.

Example

Display the FTP client's working directory on the remote FTP server.

```
<HUAWEI> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] pwd
257 "/" is current directory.
```

2.7.62 pwd (SFTP client view)

Function

The **pwd** command displays the SFTP client's working directory on the remote FTP server.

Format

pwd

Parameters

None

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

After logging in to the SFTP server, you can run the **pwd** command to display the SFTP client's working directory on the remote SFTP server.

If the displayed working directory is incorrect, you can run the **cd** command to change the SFTP client's working directory on the remote SFTP server.

Example

Display the SFTP client's working directory on the remote SFTP server.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> pwd
/
sftp-client> cd test
Current directory is:
/test
sftp-client> pwd
/test
```

2.7.63 pwd (user view)

Function

The **pwd** command displays the current working directory.

Format

pwd

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You can run the **pwd** command in any directory to display the current working directory. To change the current working directory, you can run the **cd** command.

Example

Display the current working directory.


```
<HUAWEI> pwd
flash:/test
```

2.7.64 remotehelp

Function

The **remotehelp** command displays the help information about an FTP command when the FTP client and server are connected.

Format

remotehelp [*command*]

Parameters

Parameter	Description	Value
command	Specifies the FTP command.	The value is a string of 1 to 16 characters.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

You can run the **remotehelp** command to display help information about an FTP command.

- The help information is provided by the remote server. Different remote servers may provide different help information for an FTP command.
- The help information can be displayed for FTP commands **user**, **pass**, **cwd**, **cdup**, **quit**, **port**, **pasv**, **type**, **retr**, **stor**, **dele**, **rmd**, **mkd**, **pwd**, **list**, **nlst**, **syst**, **help**, **xcup**, **xcwd**, **xmkd**, **xpwd**, **xrmd**, **eprt**, **epsv**, and **feat**.

Example

Display the syntax of the **cdup** command.

```
<HUAWEI> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] remotehelp
```



```
214-The following commands are recognized (Commands marked with '*' are unimplem ented).    USER
PASS   ACCT*  CWD    CDUP   SMNT*  QUIT   REIN*   PORT   PASV   TYPE   STRU*  MODE*  RETR   STOR
STOU*   APPE   ALLO   REST*  RNFR*  RNTO*  ABOR*  DELE   RMD    MKD    PWD    LIST   NLST   SITE*
SYST   STAT*  HELP   NOOP*  XCUP   XCWD   XMKD   XPWD   XRMD   EPRT   EPSV    FEAT 214 Direct
comments to Huawei Tech.

[ftp] remotehelp cdup
214 Syntax: CDUP <change to parent directory>.
```

2.7.65 remove (SFTP client view)

Function

The **remove** command deletes specified files from the remote SFTP server.

Format

remove *remote-filename* &<1-10>

Parameters

Parameter	Description	Value
remote-filename	Specifies the name of the file to be deleted from the remote SFTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

- You can configure a maximum of 10 file names in the command and separate them using spaces and delete them at one time.
- If the file to be deleted is not in the current directory, you must specify the file path.

Example

Delete the file **3.txt** from the server and **backup1.txt** from the **test** directory.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> remove 3.txt test/backup1.txt
Warning: Make sure to remove these files? [Y/N]:y
Info: Succeeded in removing the file /3.txt.
Info: Succeeded in removing the file /test/backup1.txt.
```


2.7.66 rename (SFTP client view)

Function

The **rename** command renames a file or directory stored on the SFTP server.

Format

rename *old-name new-name*

Parameters

Parameter	Description	Value
old-name	Specifies the name of a file or directory.	The value is a string of 1 to 64 case-insensitive characters without spaces.
new-name	Specifies the new name of the file or directory.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

You can run the **rename** command to rename a file or directory.

Example

Rename the directory **yourtest** on the SFTP server.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> rename test/yourtest test/test
Warning: Rename /test/yourtest to /test/test? [Y/N]:y
Info: Succeeded in renaming file.
sftp-client> cd test
Current directory is:
/test
sftp-client> dir
drwxrwxrwx   1 noone    nogroup        0 Mar 29 2012 .
drwxrwxrwx   1 noone    nogroup        0 Mar 29 2012 ..
drwxrwxrwx   1 noone    nogroup        0 Mar 24 2012 test
-rwxrwxrwx   1 noone    nogroup     5736 Mar 24 2012 backup.txt
```

2.7.67 rename (user view)

Function

The **rename** command renames a file or folder.

Format

rename *old-name new-name*

Parameters

Parameter	Description	Settings
old-name	Specifies the name of a file or folder.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] [path] filename** format. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "

Parameter	Description	Settings
new-name	Specifies the new name of the file or directory.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] [path] filename** format. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the drive name:

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.

- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Precautions

- You must rename a file or directory in its source directory.
- If the renamed file or directory has the same name as an existing file or directory, an error message is displayed.
- If you specify *old-name* or *new-name* without specifying the file path, the file must be saved in your current working directory.

Example

Rename the directory **mytest** to **yourtest** in the directory **flash:/test/**.

```
<HUAWEI> pwd
flash:/test
<HUAWEI> rename mytest yourtest
Rename flash:/test/mytest to flash:/test/yourtest ?[Y/N]:y
Info: Rename file flash:/test/mytest to flash:/test/yourtest ......Done.
```

Rename the file **sample.txt** to **sample.bak**.

```
<HUAWEI> rename sample.txt sample.bak
Rename flash:/sample.txt to flash:/sample.bak ?[Y/N] :y
Info: Rename file flash:/sample.txt to flash:/sample.bak .......Done.
```

2.7.68 reset recycle-bin

Function

The **reset recycle-bin** command permanently deletes files from the recycle bin.

Format

reset recycle-bin [*filename* | *devicename*]

Parameters

Parameter	Description	Value
filename	Specifies the name of a file to be deleted.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' " The wildcard (*) character is supported.
devicename	Specifies the storage device name.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If you run the **delete** command without specifying the **/unreserved** parameter, the file is moved to the recycle bin and still occupies the memory. To free up the space, you can run the **reset recycle-bin** command to permanently delete the file from the recycle bin.

The following describes the drive name.

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Like *devicename*, **drive** specifies the storage device name.

Precautions

- You can run the **dir /all** command to display all files that are moved to the recycle bin from the current directory, and file names are displayed in square brackets ([ ]).
- If you delete a specified storage device, all files in the root directory of the storage device are deleted.
- If you run the **reset recycle-bin** command directly, all files that are moved to the recycle bin from the current directory are permanently deleted.

Example

Delete the file **test.txt** that is moved to the recycle bin from the directory **test**.

```
<HUAWEI> reset recycle-bin flash:/test/test.txt
Squeeze flash:/test/test.txt?[Y/N]:y
%Cleared file flash:/test/test.txt.
```

Delete files that are moved to the recycle bin from the current directory.

```
<HUAWEI> pwd
flash:/test
<HUAWEI> reset recycle-bin
Squeeze flash:/test/backup.zip?[Y/N]:y
%Cleared file flash:/test/backup.zip.
Squeeze flash:/test/backup1.zip?[Y/N]:y
%Cleared file flash:/test/backup1.zip.
```

2.7.69 rmdir (FTP client view)

Function

The **rmdir** command deletes a specified directory from the remote FTP server.

Format

rmdir *remote-directory*

Parameters

Parameter	Description	Value
remote-directory	Specifies a directory or path on the FTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **rmdir** command to delete a specified directory from the remote FTP server.

Precautions

- Before running the **rmdir** command to delete a directory, you must delete all files and subdirectories from the directory.
- If no path is specified when you delete a subdirectory, the subdirectory is deleted from the current directory.
- The directory is deleted from the FTP server rather than the FTP client.

Example

Delete the directory **d:/temp1** from the remote FTP server.

```
<HUAWEI> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] ascii
200 Type set to A.
[ftp] rmdir d:/temp1
250 'D:\temp1': directory removed.
```

2.7.70 rmdir (user view)

Function

The **rmdir** command deletes a specified directory from the storage device.

Format

rmdir *directory*

Parameters

Parameter	Description	Value
directory	Specifies a directory or directory and its path.	The value is a string of case-insensitive characters in the **[drive] [path] directory** format. The absolute path length ranges from 1 to 64, while the directory name length ranges from 1 to 15. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. The directory name cannot contain the following characters: ~ * / \ : ' "

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the drive name.

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Precautions

- Before running the **rmdir** command to delete a directory, you must delete all files and subdirectories from the directory.
- A deleted directory and its files cannot be restored from the recycle bin.

Example

Delete the directory **test** from the current directory.

```
<HUAWEI> rmdir test
Remove directory flash:/test?[Y/N]:y
%Removing directory flash:/test...Done!%Removing directory flash:/test....Done!
```

2.7.71 rmdir (SFTP client view)

Function

The **rmdir** command deletes a specified directory from the remote SFTP server.

Format

rmdir *remote-directory* &<1-10>

Parameters

Parameter	Description	Value
remote-directory	Specifies the name of a file on the SFTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

- You can configure a maximum of 10 file names in the command and separate them using spaces and delete them at one time.
- Before running the **rmdir** command to delete a directory, you must delete all files and subdirectories from the directory.
- If the directory to be deleted is not in the current directory, you must specify the file path.

Example

Delete the directory **1** from the current directory, and the directory **2** from the **test** directory.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.137.217.201
```



```
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> rmdir 1 test/2
Warning: Make sure to remove these directories? [Y/N]:y
Info: Succeeded in removing the directory /test/1.
Info: Succeeded in removing the directory /test/test/2.
```

2.7.72 scp

Function

The **scp** command uploads a local file to the remote SCP server or downloads a file from the remote SCP server to a local directory.

Format

Transfer a file between the local client and the remote SCP server based on IPv4.

scp [**-port** *port-number* | { **public-net** | **vpn-instance** *vpn-instance-name* } | **identity-key** { **dsa** | **rsa** | **ecc** | **rsa_sha2_256** | **rsa_sha2_512** } | **user-identity-key** { **rsa** | **dsa** | **ecc** } | { **-a** *source-address* | **-i** *interface-type interface-number* } | **-r** | **-cipher** *-cipher* | **-c**] * *sourcefile destinationfile*

Transfer a file between the local client and the remote SCP server based on IPv6.

scp ipv6 [**-port** *port-number* | { **public-net** | **vpn-instance** *vpn-instance-name* } | **identity-key** { **dsa** | **rsa** | **ecc** | **rsa_sha2_256** | **rsa_sha2_512** } | **user-identity-key** { **rsa** | **dsa** | **ecc** } | **-a** *source-address* | **-r** | **-cipher** *-cipher* | **-c**] * *sourcefile destinationfile* [**-oi** *interface-type interface-number*]

Parameters

Parameter	Description	Value
-port *port-number*	Specifies the port number of the SCP server.	The value is an integer that ranges from 1 to 65535. The default value is 22.
public-net	Indicates that the SCP server is connected to the public network.	-
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance where the SCP server is located.	The value must be an existing VPN instance name.

Parameter	Description	Value
identity-key	Specifies the public key algorithm for server authentication.	Public key algorithms include DSA, RSA, RSA_SHA2_256, RSA_SHA2_512 and ECC. By default, ECC is used for server authentication. **NOTE** To improve security, it is not recommended that you use RSA or DSA as the authentication algorithm.
user-identity-key	Specifies the public key algorithm for client authentication.	Public key algorithms include DSA, RSA, and ECC. By default, RSA is used for client authentication. **NOTE** To improve security, it is not recommended that you use RSA or DSA as the authentication algorithm.
-a *source-address*	Specifies the source IP address for connecting to the SCP client. You are advised to use the loopback interface IP address.	-
-i *interface-type interface-number*	Specifies the source interface used by the SCP client to set up connections. It consists of the interface type and number. It is recommended that you specify a loopback interface. The IP address configured for this interface is the source IP address for sending packets. If no IP address is configured for the source interface, the SCP connection cannot be set up.	-

Parameter	Description	Value
-oi *interface-type interface-number*	Specifies an outbound interface on the local device. If the remote host uses an IPv6 address, you must specify the outbound interface on the local device.	-
-r	Uploads or downloads files in batches.	-
-cipher *-cipher*	Specifies the encryption algorithms for uploading or downloading files.	Encryption algorithms **des**, **3des**, **aes256**, **aes128_ctr**, **aes256_ctr**, and **aes128** are supported. The default encryption algorithm is **aes256_ctr**. You are advised to use aes128_ctr and aes256_ctr encryption algorithms to ensure high security. **NOTE** • If an encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select an encryption algorithm from the list. • If no encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select one from **3des**, **aes128**, **aes256**, **aes128_ctr**, and **aes256_ctr**.
-c	Compress files when uploading or downloading them.	-
sourcefile	Specifies a source file to be uploaded or downloaded.	The source file format is *username*@*hostname*:[*path*][*filename*].

Parameter	Description	Value
destinationfile	Specifies a destination file to be uploaded or downloaded.	The destination file format is *username*@*hostname*:[*path*][*filename*].

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

SCP is an SSH2.0-based secure file transfer protocol. Compared with the SFTP file transfer mode, the SCP file transfer mode allows you to upload or download files when the connection is set up between the SCP client and server.

- You are advised to set the source IP address to the loopback address, or set the outbound interface to the loopback interface using **-a** and **-i**, to improve security.
- When **-r** is specified, you can use the wildcard (*) to upload or download files in batches, for example, *.txt and huawei.*.
- When **-c** is specified, files are compressed before being transmitted. File compression takes a long time and affects file transfer speed; therefore, you are not advised to compress files before transferring them.

Precautions

- The format of uploaded and downloaded files of the SCP server is *username*@*hostname*:[*path*][*filename*]. In the preceding file format, *username* indicates the user name for logging in to the SCP server, *hostname* indicates the SCP server name or IP address, and *path* indicates user's working directory specified on the SCP server, and *filename* indicates the file name. The following describes the preceding parameters when you upload a file to the SCP server:
  - If *filename* and *path* are not specified, the file is transferred to the root directory of the user's working directory.
  - If only *path* is specified, the file is transferred to the specified directory.
  - If only *filename* is specified, the file is named as *filename*, and transferred to the SCP server.
  - To set *hostname* to the IPv6 address, you must add the IPv6 address with square brackets ([ ]), for example, zhangsan@[FC00::/7]:.
- If the destination file name is the same as the name of an existing directory, the file is moved to this directory with the source file name. If the destination

file has the same name as an existing file, the system prompts you whether to overwrite the existing file.

- If an SCP user on the client authenticates the server using an RSA, a DSA, or an ECC public key, the SCP user is prompted to select the key pair for authentication.
- You can run the **set net-manager vpn-instance** command to configure the NMS management VPN instance before running the **open** command to connect the FTP client and server.
  - If **public-net** or **vpn-instance** is not specified, the FTP client accesses the FTP server in the VPN instance managed by the NMS.
  - If **public-net** is specified, the FTP client accesses the FTP server on the public network.
  - If **vpn-instance** *vpn-instance-name* is specified, the FTP client accesses the FTP server in a specified VPN instance.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Log in through ECC authentication and copy the **xxxx.txt** file to the flash memory of remote SCP server at 10.10.0.114.

```
<HUAWEI> system-view
[HUAWEI] scp identity-key ecc flash:/xxxx.txt root@10.10.0.114:flash:/xxxx.txt
Trying 10.10.0.114 ...
Press CTRL+K to abort
Connected to 10.10.0.114 ...
The server's public key does not match the one catched before.
The server is not authenticated. Continue to access it? [Y/N]:y
Update the server's public key now? [Y/N]: y

Enter password:
flash:/xxxx.txt              100%          12Bytes          1KByte(s)/sec
```

2.7.73 scp client-source

Function

The **scp client-source** command specifies the source IP address for the SCP client to send packets.

The **undo scp client-source** command cancels the source IP address for the SCP client to send packets.

By default, no source IP address is configured on the SCP client.

Format

scp client-source { **-a** *source-ip-address* | **-i** *interface-type interface-number* }

undo scp client-source

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the source IP address of the SCP client. You are advised to use the loopback interface IP address.	-
-i *interface-type interface-number*	Source interface type and ID. You are advised to use the loopback interface. The IP address configured for this interface is the source IP address for sending packets. If no IP address is configured for the source interface, the SCP connection cannot be set up.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If no source IP address is specified, the client uses the source IP address that the router specifies to send packets. The source IP address must be configured for an interface with stable performance. The loopback interface is recommended. Using the loopback interface as the source interface simplifies the ACL rule and security policy configuration. This shields the IP address differences and interface status impact, filters incoming and outgoing packets, and implements security authentication.

Prerequisites

The source interface specified using the command must exist and have an IP address configured.

Precautions

The **scp** command also configures the source IP address whose priority is higher than that of the source IP address specified in the **scp client-source** command. If you specify source addresses in the **scp client-source** and **scp** commands, the source IP address specified in the **scp** command is used for data communication. The source address specified in the **scp client-source** command applies to all SCP connections. The source address specified in the **scp** command applies only to the current SCP connection.

Example

Set the source IP address of the SCP client to the loopback interface IP address 10.1.1.1.


```
<HUAWEI> system-view
[HUAWEI] scp client-source -a 10.1.1.1
```

2.7.74 scp server enable

Function

The **scp server enable** command enables the SCP service on the SSH server.

The **undo scp server enable** command disables the SCP service on the SSH server.

By default, the SCP function is disabled.

Format

scp [**ipv4** | **ipv6**] **server enable**

undo scp [**ipv4** | **ipv6**] **server enable**

Parameters

Parameter	Description	Value
ipv4	Indicates that the SCP IPv4 service is enabled on the SSH server.	-
ipv6	Indicates that the SCP IPv6 service is enabled on the SSH server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To use SCP for file transfer, you need to first enable the SCP service on the SSH server. The client can establish an SCP connection with the SSH server only after SCP service has been enabled on the SSH server.

Prerequisites

Before enabling the SCP service, run either of the following commands as required:

- Run the **ssh server-source -i** *interface-type interface-number* command to configure a specified interface as the source interface of the SSH server or run the **ssh server-source all-interface** command to specify any interface with an IPv4 address configured on the device as the source interface of the SSH server.

- Run the **ssh ipv6 server-source -a** *ipv6_address* [**-vpn-instance** *vpn_name*] command to configure a specified IPv6 address as the IPv6 source address of the SSH server or run the **ssh ipv6 server-source all-interface** command to specify any interface IPv6 address on the device as the IPv6 source address of the SSH server.

Precautions

After the **scp server enable** command is run, the numbers of IPv4 port and IPv6 port are both changed. To change the number of IPv4 port or IPv6 port separately, run the **scp** [**ipv4** | **ipv6**] **server enable** command.

Example

Enable the SCP service.

```
<HUAWEI> system-view
[HUAWEI] scp server enable
```

Enable the SCP IPv4 service.

```
<HUAWEI> system-view
[HUAWEI] scp ipv4 server enable
```

2.7.75 set cipher-suite

Function

The **set cipher-suite** command configures cipher suites for a customized SSL cipher suite policy.

The **undo set cipher-suite** command deletes cipher suites in a customized SSL cipher suite policy.

By default, no cipher suite is configured for a customized SSL cipher suite policy.

Format

set cipher-suite { **tls12_ck_dss_aes_128_gcm_sha256** | **tls12_ck_dss_aes_256_gcm_sha384** | **tls12_ck_rsa_aes_128_gcm_sha256** | **tls12_ck_rsa_aes_256_gcm_sha384** }

undo set cipher-suite { **tls12_ck_dss_aes_128_gcm_sha256** | **tls12_ck_dss_aes_256_gcm_sha384** | **tls12_ck_rsa_aes_128_gcm_sha256** | **tls12_ck_rsa_aes_256_gcm_sha384** }

Parameters

Parameter	Description	Value
tls12_ck_dss_aes_128_gcm_sha256	Configures the TLS12_CK_DSS_AES_128_GCM_SHA256 cipher suite.	-

Parameter	Description	Value
tls12_ck_dss_aes_256_gcm_sha384	Configures the TLS12_CK_DSS_AES_256_GCM_SHA384 cipher suite.	-
tls12_ck_rsa_aes_128_gcm_sha256	Configures the TLS12_CK_RSA_AES_128_GCM_SHA256 cipher suite.	-
tls12_ck_rsa_aes_256_gcm_sha384	Configures the TLS12_CK_RSA_AES_256_GCM_SHA384 cipher suite.	-

Views

Customized SSL cipher suite policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure cipher suites for a customized SSL cipher suite policy, run the **set cipher-suite** command.

Precautions

- If a customized SSL cipher suite policy is being referenced by an SSL policy, the cipher suites in the customized cipher suite policy can be added, modified, or partially deleted. Deleting all of the cipher suites is not allowed.
- The system software does not support the **tls12_ck_rsa_aes_256_cbc_sha256**, **tls1_ck_dhe_dss_with_aes_128_sha**, **tls1_ck_dhe_dss_with_aes_256_sha**, **tls1_ck_dhe_rsa_with_aes_128_sha**, **tls1_ck_dhe_rsa_with_aes_256_sha**, **tls1_ck_rsa_with_aes_128_sha**, and **tls1_ck_rsa_with_aes_256_sha** parameters. To use the **tls12_ck_rsa_aes_256_cbc_sha256**, **tls1_ck_dhe_dss_with_aes_128_sha**, **tls1_ck_dhe_dss_with_aes_256_sha**, **tls1_ck_dhe_rsa_with_aes_128_sha**, **tls1_ck_dhe_rsa_with_aes_256_sha**, **tls1_ck_rsa_with_aes_128_sha**, or **tls1_ck_rsa_with_aes_256_sha** parameter, you need to install the WEAKEA plug-in. For higher security purposes, you are advised to use other parameters. For details about how to install the WEAKEA plug-in, see WEAKEA Configuration.

Example

Configure the **tls12_ck_dss_aes_128_gcm_sha256** cipher suite for the customized SSL cipher suite policy named **cipher1**.


```
<HUAWEI> system-view
[HUAWEI] ssl cipher-suite-list cipher1
[HUAWEI-ssl-cipher-suite-cipher1] set cipher-suite tls12_ck_dss_aes_128_gcm_sha256
```

2.7.76 set default ftp-directory

Function

The **set default ftp-directory** command configures the default FTP working directory.

The **undo set default ftp-directory** command disables the default FTP working directory.

By default, no default FTP working directory is configured.

Format

set default ftp-directory *directory*

undo set default ftp-directory

Parameters

Parameter	Description	Value
directory	Specify the default FTP working directory.	The value is a string of 1 to 160 case-insensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **set default ftp-directory** command to configure a default FTP working directory for all FTP users at one time.

Precautions

- The **set default ftp-directory** command takes effect only when the device functions as an FTP server and the user function as an FTP client.
- You can run the **local-user ftp-directory** command to configure an authorized working directory for a local user.
- If you have configured the FTP working directory by running the **local-user ftp-directory** command, you must use this FTP working directory.
- You can run the **lcd** command to view the working directory of FTP users.

- If no FTP working directory is specified on the device, FTP users cannot log in to the device, and are prompted that the working directory is unauthorized.

Example

Set the default FTP working directory to **flash:/**.

```
<HUAWEI> system-view
[HUAWEI] set default ftp-directory flash:/
```

2.7.77 set device auto-delete-file disable

Function

The **set device auto-delete-file disable** command disables the automatic file deletion function.

The **undo set device auto-delete-file disable** command enables the automatic file deletion function.

By default, the device is enabled to automatically delete files.

Format

set device auto-delete-file disable

undo set device auto-delete-file disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device periodically checks the storage space. When the space usage exceeds 85%, the device automatically releases the space using the following methods in sequence: empty the recycle bin, delete the system software package, delete patches, and delete logs. If you need to manually delete the files, run this command to disable the automatic file deletion function.

If no command output is displayed, run the **display current-configuration** command to check the parameters that have taken effect on the device and determine whether the automatic file deletion function is enabled.

Example

Disable the automatic file deletion function.

```
<HUAWEI> system-view
[HUAWEI] set device auto-delete-file disable
```

2.7.78 set net-manager vpn-instance

Function

The **set net-manager vpn-instance** command configures the default VPN instance that the NMS uses on the device.

The **undo set net-manager vpn-instance** command deletes the default VPN instance from the device.

By default, no VPN instance is configured on the device.

Format

set net-manager vpn-instance *vpn-instance-name*

undo set net-manager vpn-instance

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the default VPN instance.	The value must be an existing VPN instance name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the NMS manages devices on the VPN network, you need to send the device information to the NMS using the VPN instance.

You can run the **set net-manager vpn-instance** command to configure the default VPN instance for the NMS to manage the device so that the device can use this VPN instance to communicate with the NMS.

Precautions

- Before running the **set net-manager vpn-instance** command, you must create VPN instances.
- After running this command, you can successfully run file transfer commands that you have configured based on the FTP, TFTP, SCP, and SFTP commands only in the default VPN instance.
- If the host has been configured as a log host, the NMS can receive device logs from the default VPN instance.
- After you configure a VPN instance using the **set net-manager vpn-instance** command, the FTP, SFTP, SCP, and TFTP clients as well as the Information Center (IC), SNMP, and TACACS modules will use this instance by default.

  If the preceding clients or modules need to use a public network server or a specified VPN server, run the following commands to set parameters. If **public-net** is specified, the device accesses the server on the public network. If **vpn-instance***vpn-instance-name* is specified, the device accesses the server in the specified VPN instance.
  - FTP client: **ftp**
  - SFTP client: **sftp**
  - SCP client: **scp**
  - TFTP client: **tftp**
  - IC module: **info-center loghost**
  - SNMP module: **snmp-agent target-host trap**
  - TACACS module: **hwtacacs-server accounting**, **hwtacacs-server authentication**, **hwtacacs-server authorization**

Example

Set the default VPN instance to v1.

```
<HUAWEI> system-view
[HUAWEI] set net-manager vpn-instance v1
```

2.7.79 sftp

Function

The **sftp** command connects the device to the SSH server so that you can manage files that are stored on the SFTP server.

Format

Connect the SFTP client to the SFTP server based on IPv4.

sftp [**-a** *source-address* | **-i** *interface-type interface-number*] *host-ip* [*port*] [[**public-net** | **-vpn-instance** *vpn-instance-name*] | **identity-key** { **dsa** | **rsa** | **ecc** | **rsa_sha2_256** | **rsa_sha2_512** } | **user-identity-key** { **rsa** | **dsa** | **ecc** } | **prefer_kex** *prefer_key-exchange* | **prefer_ctos_cipher** *prefer_ctos_cipher* | **prefer_stoc_cipher** *prefer_stoc_cipher* | **prefer_ctos_hmac** *prefer_ctos_hmac* | **prefer_stoc_hmac** *prefer_stoc_hmac*| **-ki** *aliveinterval*] | [**-kc** *alivecountmax*] *

Connect the SFTP client to the SFTP server based on IPv6.

sftp ipv6 [**-a** *source-address*] *host-ipv6* [**-oi** *interface-type interface-number*] [*port*] [**identity-key** { **dsa** | **rsa** | **ecc** | **rsa_sha2_256** | **rsa_sha2_512** } | **user-identity-key** { **rsa** | **dsa** | **ecc** } | **-vpn-instance** *vpn-instance-name* | **prefer_kex** *prefer_key-exchange* | **prefer_ctos_cipher** *prefer_ctos_cipher* | **prefer_stoc_cipher** *prefer_stoc_cipher* | **prefer_ctos_hmac** *prefer_ctos_hmac* | **prefer_stoc_hmac** *prefer_stoc_hmac* | **-ki** *aliveinterval* | **-kc** *alivecountmax*] *

Parameters

Parameter	Description	Value
-a *source-address*	Specifies the source IP address for connecting to the SFTP client. You are advised to use the loopback interface IP address.	-
-i *interface-type interface-number*	Specifies the source interface type and ID. You are advised to use the loopback interface. The IP address configured for this interface is the source IP address for sending packets. If no IP address is configured for the source interface, the SFTP connection cannot be set up.	-
host-ip	Specifies the IP address or host name of the remote IPv4 SFTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.
host-ipv6	Specifies the IPv6 address or host name of the remote IPv6 SFTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
-oi *interface-type interface-number*	Specifies an outbound interface on the local device. If the remote host uses an IPv6 address, you must specify the outbound interface on the local device.	-
port	Specifies the port number of the SSH server.	The value is an integer that ranges from 1 to 65535. The default port number is 22.
public-net	Specifies the SFTP server on the public network. You must set the **public-net** parameter when the SFTP server IP address is a public network IP address.	-
-vpn-instance *vpn-instance-name*	Name of the VPN instance where the SFTP server is located.	The value must be an existing VPN instance name.
prefer_kex *prefer_key-exchange*	Indicates the preferred key exchange algorithm.	The **dh_exchange_group**, **dh_exchange_group_sha256**, **dh_group14_sha1**, **dh_group14_sha256**, **dh_group15_sha512**, and **dh_group16_sha512** algorithms are supported currently. The default key exchange algorithm is dh_group14_sha1.

Parameter	Description	Value
prefer_ctos_cipher *prefer_ctos_cipher*	Specify an encryption algorithm for transmitting data from the client to the server.	Encryption algorithms 3des, aes128, aes128_ctr, aes256_ctr, and aes256 are supported. The default encryption algorithm is aes256_ctr. You are advised to use aes128_ctr and aes256_ctr encryption algorithms to ensure high security. **NOTE** • If an encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select an encryption algorithm from the list. • If no encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select one from **3des**, **aes128**, **aes256**, **aes128_ctr**, and **aes256_ctr**.

Parameter	Description	Value
prefer_stoc_cipher *prefer_stoc_cipher*	Specify an encryption algorithm for transmitting data from the server to the client	Encryption algorithms 3des, aes128, aes128_ctr, aes256_ctr, and aes256 are supported. The default encryption algorithm is aes256_ctr. You are advised to use aes128_ctr and aes256_ctr encryption algorithms to ensure high security. **NOTE** • If an encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select an encryption algorithm from the list. • If no encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select one from **3des**, **aes128**, **aes256**, **aes128_ctr**, and **aes256_ctr**.
prefer_ctos_hmac *prefer_ctos_hmac*	Specify an HMAC algorithm for transmitting data from the client to the server.	HMAC algorithms sha1, sha1_96, md5, sha2_256, sha2_256_96, and md5_96 are supported. The default HMAC algorithm is sha2_256. **NOTE** To enhance security, you are not advised to use the md5 or md5_96 algorithm.
prefer_stoc_hmac *prefer_stoc_hmac*	Specify an HMAC algorithm for transmitting data from the server to the client.	HMAC algorithms sha1, sha1_96, md5, sha2_256, sha2_256_96, and md5_96 are supported. The default HMAC algorithm is sha2_256. **NOTE** To enhance security, you are not advised to use the md5 or md5_96 algorithm.

Parameter	Description	Value
-ki *aliveinterval*	Specifies the interval for sending keepalive packets when no packet is received in reply.	The value is an integer that ranges from 1 to 3600, in seconds.
-kc *alivecountmax*	Specifies the times for sending keepalive packets when no packet is received in reply.	The value is an integer that ranges from 3 to 10. The default value is 5.
identity-key	Specifies the public key for server authentication.	Public key algorithms include dsa, rsa, rsa_sha2_256, rsa_sha2_512 and ecc. By default, the server authentication uses the ECC public key. **NOTE** To improve security, it is not recommended that you use RSA or DSA as the authentication algorithm.
user-identity-key	Specifies the public key algorithm for the client authentication.	Public key algorithms include dsa, rsa, and ecc. By default, the client authentication uses the RSA public key. **NOTE** To improve security, it is not recommended that you use RSA or DSA as the authentication algorithm.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

SFTP is short for SSH FTP that is a secure FTP protocol. SFTP is on the basis of SSH. It ensures that users can log in to a remote device securely for file management and transmission, and enhances the security in data transmission. In addition, you can log in to a remote SSH server from the device that functions as an SFTP client.

When the connection between the SFTP server and client fails, the SFTP client must detect the fault in time and disconnect from the SFTP server. To ensure this, before being connected to the server in SFTP mode, the client must be configured with the interval and times for sending the keepalive packet when no packet is received in reply. If the client receives no packet in reply within the specified interval, the client sends the keepalive packet to the server again. If the maximum number of times that the client sends keepalive packets exceeds the specified value, the client releases the connection. By default, when no packet is received, the function for sending keepalive packets is not enabled.

Precautions

- You can set the source IP address to the source or destination IP address in the ACL rule when the **-a** or **-i** parameter is specified. This shields the IP address differences and interface status impact, filters incoming and outgoing packets, and implements security authentication.
- The SSH client can log in to the SSH server with no port number specified only when the port number of the SSH server is 22. If the SSH server uses another port, the port number must be specified when SSH clients log in to the SSH server.
- You can run the **set net-manager vpn-instance** command to configure the NMS management VPN instance before running the **open** command to connect the FTP client and server.
  - If **public-net** or **vpn-instance** is not specified, the FTP client accesses the FTP server in the VPN instance managed by the NMS.
  - If **public-net** is specified, the FTP client accesses the FTP server on the public network.
  - If **vpn-instance** *vpn-instance-name* is specified, the FTP client accesses the FTP server in a specified VPN instance.
- If you cannot run the **sftp** command successfully when you configured the ACL on the SFTP client, or when the TCP connection fails, an error message is displayed indicating that the SFTP client cannot be connected to the server.

Example

Set keepalive parameters when the client is connected to the server in SFTP mode.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.164.39.223 -ki 10 -kc 4
Please input the username: client001
Trying 10.164.39.223 ...
Press CTRL+K to abort
Connected to 10.164.39.223 ...
Enter password:
sftp-client>
```

Connect the client to the server using the DSA authentication in SFTP mode.

```
<HUAWEI> system-view
[HUAWEI] sftp 10.164.39.223 identity-key dsa
Please input the username:root
Trying 10.164.39.223 ...
Press CTRL+K to abort
Connected to 10.164.39.223 ...
Enter password:
```



```
sftp-client> quit
Bye
```

2.7.80 sftp client-source

Function

The **sftp client-source** command specifies the source IP address for the SFTP client to send packets.

The **undo sftp client-source** command restores the default source IP address for the SFTP client to send packets.

The default source IP address for the SFTP client to send packets is 0.0.0.0.

Format

sftp client-source { **-a** *source-ip-address* | **-i** *interface-type interface-number* }

undo sftp client-source

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the source IP address. Set the value to the IP address of a loopback interface.	The value is in dotted decimal notation.
-i *interface-type interface-number*	Specifies the loopback interface as the source interface. The IP address configured for the source interface is the source IP address for sending packets. If no IP address is configured for the source interface, the FTP connection cannot be set up.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If no source IP address is specified, the client uses the source IP address that the router specifies to send packets. The source IP address must be configured for an interface with stable performance. The loopback interface is recommended. Using

the loopback interface as the source interface simplifies the ACL rule and security policy configuration. This shields the IP address differences and interface status impact, filters incoming and outgoing packets, and implements security authentication.

Prerequisites

The loopback source interface specified using the command must exist and have an IP address configured.

Precautions

- The source interface must be set to the loopback interface. You can query the source IP address or primary IP address of the source interface for the SFTP connection on the SFTP server.
- The **sftp** command also configures the source IP address whose priority is higher than that of the source IP address specified in the **sftp client-source** command. If you specify source addresses in the **sftp client-source** and **sftp** commands, the source IP address specified in the **sftp** command is used for data communication. The source address specified in the **sftp client-source** command applies to all SFTP connections. The source address specified in the **sftp** command applies only to the current SFTP connection.

Example

Set the source IP address of the SFTP client to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] sftp client-source -a 10.1.1.1
Info: Succeeded in setting the source address of the SFTP client to 10.1.1.1.
```

2.7.81 sftp client-transfile

Function

The **sftp client-transfile** command uploads files to or downloads files from the SFTP server.

Format

Establish an SFTP connection on an IPv4 network.

sftp client-transfile { **get** | **put** } [**-a** *source-address* | **-i** *interface-type interface-number*] **host-ip** *host-ipv4* [*port*] [[**public-net** | **-vpn-instance** *vpn-instance-name*] | **prefer_kex** *prefer_key-exchange* | **identity-key** { **rsa** | **dsa** | **ecc** | **rsa_sha2_256** | **rsa_sha2_512** } | **prefer_ctos_cipher** *prefer_ctos_cipher* | **prefer_stoc_cipher** *prefer_stoc_cipher* | **prefer_ctos_hmac** *prefer_ctos_hmac* | **prefer_stoc_hmac** *prefer_stoc_hmac* | **-ki** *aliveinterval* | **-kc** *alivecountmax*] * **username** *user-name* **password** *password* **sourcefile** *source-file* [**destination** *destination*]

Establish an SFTP connection on an IPv6 network.

sftp client-transfile { **get** | **put** } **ipv6** [**-a** *source-address*] **host-ip** *host-ipv6* [**-oi** *interface-type interface-number*] [*port*] [**-vpn-instance** *vpn-instance-name* | **prefer_kex** *prefer_key-exchange* | **identity-key** { **rsa** | **dsa** | **ecc** | **rsa_sha2_256** |

rsa_sha2_512 } | **prefer_ctos_cipher** *prefer_ctos_cipher* | **prefer_stoc_cipher** *prefer_stoc_cipher* | **prefer_ctos_hmac** *prefer_ctos_hmac* | **prefer_stoc_hmac** *prefer_stoc_hmac* | **-ki** *aliveinterval* | **-kc** *alivecountmax*] * **username** *user-name* **password** *password* **sourcefile** *source-file* [**destination** *destination*]

Parameters

Parameter	Description	Value
get	Downloads files from the SFTP server.	-
put	Uploads files to the SFTP server.	-
-a *source-address*	Specifies the source address of an SFTP client.	-
-i *interface-type interface-number*	Specifies the source interface of an SFTP client.	-
host-ip *host-ipv4*	Specifies the IPv4 address or host name of an SFTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.
port	Specifies the current monitoring port number on the SFTP server. Only when the monitoring port number on the SFTP server is 22, the SFTP client can log in without a port number being specified. If the monitoring port number on the SFTP server is not 22, you must specify a port number for the SFTP client to log in.	The value is an integer ranging from 1 to 65535. The default value is 22.
public-net	Establishes the SFTP connection on a public network.	-

Parameter	Description	Value
-vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance. The SFTP connection is established on a private network.	The value must be an existing VPN instance name.
prefer_kex *prefer_key-exchange*	Specifies a preferred algorithm for key exchange.	• dh_exchange_group • dh_exchange_group_sha256 • dh_group14_sha1 • dh_group14_sha256 • dh_group15_sha512 • dh_group16_sha512 The default algorithm is dh_exchange_group. **NOTE** The **dh_exchange_group** algorithm is recommended.
identity-key	Specifies a public key algorithm for the server authentication.	• dsa • rsa • ecc • rsa_sha2_256 • rsa_sha2_512 The default algorithm is rsa. **NOTE** To improve security, it is not recommended that you use RSA or DSA as the authentication algorithm.

Parameter	Description	Value
prefer_ctos_cipher *prefer_ctos_cipher*	Specifies the preferred encryption algorithm for packets from the client to the server	• 3des • aes128 • aes256 • aes128_ctr(Advanced Encryption Standard 128_ctr) • aes256_ctr(Advanced Encryption Standard 256_ctr) The default algorithm is aes256_ctr. To improve security, it is recommended that you use aes128_ctr, and aes256_ctr algorithms. **NOTE** • If an encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select an encryption algorithm from the list. • If no encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select one from **3des**, **aes128**, **aes256**, **aes128_ctr**, and **aes256_ctr**.

Parameter	Description	Value
prefer_stoc_cipher *prefer_stoc_cipher*	Specifies the preferred encryption algorithm for packets from the server to the client.	• 3des • aes128 • aes256 • aes128_ctr • aes256_ctr The default algorithm is aes256_ctr. To improve security, it is recommended that you use aes128_ctr, and aes256_ctr algorithms. **NOTE** • If an encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select an encryption algorithm from the list. • If no encryption algorithm list has been configured using the **ssh client cipher** command for the SSH client, select one from **3des**, **aes128**, **aes256**, **aes128_ctr**, and **aes256_ctr**.
prefer_ctos_hmac *prefer_ctos_hmac*	Specifies the preferred HMAC algorithm for packets from the client to the server.	• sha1 • sha1_96 • md5 • md5_96 • sha2_256 • sha2_256_96 The default algorithm is sha2_256.
prefer_stoc_hmac *prefer_stoc_hmac*	Specifies the preferred HMAC algorithm for packets from the server to the client.	• sha1 • sha1_96 • md5 • md5_96 • sha2_256 • sha2_256_96 The default algorithm is sha2_256.

Parameter	Description	Value
-ki *aliveinterval*	Specifies the interval at which the client sends a Keepalive packet to the server. When the connection between the server and the client fails, the client must detect the fault in time and removes the connection proactively. Therefore, when logging in to the server using SFTP, the client must be configured with an interval at which the client sends keepalive packets to the server and the maximum number of times that the server provides no response. If a client does not receive any packet within a specified period, the client sends a Keepalive packet to the server. If the maximum number of times that the server does not respond exceeds the specified value, the client proactively removes the connection. By default, the function of sending Keepalive packets to the server in the case of no data transmission is not configured.	The value is an integer ranging from 1 to 3600, in seconds. The default value is 60 seconds.
-kc *alivecountmax*	Specifies the maximum number of times that the server does not respond.	The value is an integer ranging from 3 to 10. The default value is 5.
username *user-name*	Specifies the user name for an SFTP connection.	The value is a string of 1 to 255 case-sensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
password *password*	Specifies the password for an SFTP connection.	The value is a string of 1 to 128 case-sensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.
sourcefile *source-file*	Specifies the source file to be uploaded to or downloaded from the server.	The absolute path of the file ranges from 1 to 160 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.
destination *destination*	Specifies the destination file to be uploaded to or downloaded from the server. If **destination** *destination* is not specified, the name of the file to be downloaded from or uploaded to the server is the same as that on the SFTP server.	The absolute path of the file ranges from 1 to 160 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.
ipv6	Specifies an IPv6 SFTP server.	-
-oi *interface-type interface-number*	Specifies the source IPv6 interface of an SFTP client. If *host-ipv6* is a link-local IPv6 address, you must specify the interface name corresponding to the link-local address. If *host-ipv6* is not a link-local IPv6 address, no interface name is required.	-

Parameter	Description	Value
host-ip *host-ipv6*	Specifies the IPv6 address or host name of an SFTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To upload files to or download files from an SFTP server, run the **sftp client-transfile** command.

Prerequisites

The SFTP function on the SFTP server has been enabled using the **sftp client-transfile** command.

Configuration Impact

After a connection is established between an SFTP client and an SFTP server, they start to intercommunicate.

Precautions

If command execution fails due to ACLs on the SFTP client or the TCP connection fails, the system prompts an error message indicating that the connection to the server fails.

If the **sftp client-transfile** command is run for the device to connect to the SFTP server, only password authentication is supported.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Configure the current monitoring port number 1025 on the SSH server on a private network (SFTP client on the public network), and download the **sample.txt** file to the SFTP client.

```
<HUAWEI> system-view
[HUAWEI] sftp client-transfile get host-ip 10.137.144.231 1025 -vpn-instance ssh username root
password YsHsjx_202206 sourcefile sample.txt
```

Specify Keepalive parameters for the client that attempts to log in to the server using SFTP and download the **sample.txt** file to the SFTP client.

```
<HUAWEI> system-view
[HUAWEI] sftp client-transfile get host-ip 10.164.39.209 -ki 10 -kc 4 username root password
YsHsjx_202206 sourcefile sample.txt
```

Configure the client to pass DSA authentication before logging in to the server using SFTP and download the **sample.txt** file to the SFTP client.

```
<HUAWEI> system-view
[HUAWEI] sftp client-transfile get host-ip 10.100.0.114 identity-key dsa username root password
YsHsjx_202206 sourcefile sample.txt
```

Upload the **sample.txt** file to the IPv6 SFTP server.

```
<HUAWEI> system-view
[HUAWEI] sftp client-transfile put host-ip 10.100.0.114 identity-key dsa username root password
YsHsjx_202206 sourcefile sample.txt
```

2.7.82 sftp server enable

Function

The **sftp server enable** command enables the SFTP service on the SSH server.

The **undo sftp server enable** command disables the SFTP service on the SSH server.

By default, the SFTP service is disabled.

Format

sftp [**ipv4** | **ipv6**] **server enable**

undo sftp [**ipv4** | **ipv6**] **server enable**

Parameters

Parameter	Description	Value
ipv4	Indicates that the SFTP IPv4 service is enabled on the SSH server.	-
ipv6	Indicates that the SFTP IPv6 service is enabled on the SSH server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To connect the client to the SSH server to transfer files in SFTP mode, you must first enable the SFTP server on the SSH server.

Prerequisites

Before enabling the SFTP service, run either of the following commands as required:

- Run the **ssh server-source -i** *interface-type interface-number* command to configure a specified interface as the source interface of the SSH server or run the **ssh server-source all-interface** command to specify any interface with an IPv4 address configured on the device as the source interface of the SSH server.
- Run the **ssh ipv6 server-source -a** *ipv6_address* [**-vpn-instance** *vpn_name*] command to configure a specified IPv6 address as the IPv6 source address of the SSH server or run the **ssh ipv6 server-source all-interface** command to specify any interface IPv6 address on the device as the IPv6 source address of the SSH server.

Precautions

After the **sftp server enable** command is run, the numbers of IPv4 port and IPv6 port are both changed. To change the number of IPv4 port or IPv6 port separately, run the **sftp** [**ipv4** | **ipv6**] **server enable** command.

Example

Enable the SFTP service.

```
<HUAWEI> system-view
[HUAWEI] sftp server enable
Info: Succeeded in starting the SFTP server.
```

Disable the SFTP service.

```
<HUAWEI> system-view
[HUAWEI] undo sftp server enable
Info: Succeeded in closing the SFTP server.
```

Enable the SFTP IPv4 service.

```
<HUAWEI> system-view
[HUAWEI] sftp ipv4 server enable
```

2.7.83 ssh user sftp-directory

Function

The **ssh user sftp-directory** command configures the SFTP service authorized directory for an SSH user.

The **undo ssh user sftp-directory** command cancels the SFTP service authorized directory for an SSH user.

The default SFTP service authorized directory is flash: for an SSH user.

Format

ssh user *username* **sftp-directory** *directoryname*

undo ssh user *username* **sftp-directory**

Parameters

Parameter	Description	Value
username	Specifies the SSH user name.	The value is a string of 1 to 64 case-insensitive characters without spaces.
directoryname	Specifies the directory name on the SFTP server.	The value is a string of 1 to 160 case-insensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If there is the default authorized directory for an SFTP user on the device, you can run this command to change the directory.

Precautions

Users can only access the specified directory on the SFTP server. If the *username* user does not exist, the system creates an SSH user named *username* and uses the SFTP service authorized directory configured for the user. If the configured directory does not exist, the SFTP client fails to connect to the SSH server using this SSH user. After a master/backup switchover or device restart is performed, the SFTP client fails to connect to the SSH server if the configured directory does not exist. In this case, check whether the configured directory is valid. If the configured directory is invalid, re-configure it.

Example

Configure the SFTP service authorized directory flash:/ssh for the SSH user **admin**.

```
<HUAWEI> system-view
[HUAWEI] ssh user admin sftp-directory flash:/ssh
```


2.7.84 ssl cipher-suite-list

Function

The **ssl cipher-suite-list** command customizes an SSL cipher suite policy and displays the view of the cipher suite policy. If the SSL cipher suite policy to be customized already exists, the command directly displays the view of this cipher suite policy.

The **undo ssl cipher-suite-list** command deletes a customized SSL cipher suite policy.

By default, no customized SSL cipher suite policy is configured.

Format

ssl cipher-suite-list *customization-policy-name*

undo ssl cipher-suite-list *customization-policy-name*

Parameters

Parameter	Description	Value
customization-policy-name	Sets a name for a customized SSL cipher suite policy.	The value is a string of 1 to 32 case-insensitive characters, spaces not supported.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To improve system security, the device supports only secure algorithms by default. However, to improve compatibility, the device also allows you to customize cipher suite policies. To customize a cipher suite policy, run the **ssl cipher-suite-list** command.

Example

Customize an SSL cipher suite policy named **cipher1** and enter the view of the cipher suite policy.

```
<HUAWEI> system-view
[HUAWEI] ssl cipher-suite-list cipher1
[HUAWEI-ssl-cipher-suite-cipher1]
```


2.7.85 ssl minimum version

Function

The **ssl minimum version** command configures a minimum SSL version for an SSL policy.

The **undo ssl minimum version** command restores the default version.

By default, the minimum SSL version used by an SSL policy is TLS1.2.

NOTE

When the minimum SSL version used for an SSL policy is set to TLS1.2, an SSL certificate is required, which is provided by a third-party authoritative certificate authority.

Format

ssl minimum version { **tls1.1** | **tls1.2** }

undo ssl minimum version

Parameters

Parameter	Description	Value
tls1.1	Sets the minimum SSL version to TLS1.1 for an SSL policy.	-
tls1.2	Sets the minimum SSL version to TLS1.2 for an SSL policy.	-

Views

SSL policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure a minimum SSL version for an SSL policy, run the **ssl minimum version** command so that service modules can flexibly adopt the SSL policy.

The SSL versions supported by SSL policies include TLS1.1, TLS1.2 in ascending order of security.

Precautions

The system software does not support the tls1.0 parameter. To use the tls1.0 parameter, you need to install the WEAKEA plug-in. For higher security purposes, you are advised to specify the tls1.2 parameter. For details about how to install the WEAKEA plug-in, see WEAKEA Configuration.

Example

Configure the minimum SSL version for the SSL policy **ftp_server** to be TLS1.2.

```
<HUAWEI> system-view
[HUAWEI] ssl policy ftp_server
[HUAWEI-ssl-policy-ftp_server] ssl minimum version tls1.2
```

2.7.86 ssl policy

Function

The **ssl policy** command creates an SSL policy and displays the SSL policy view. If the SSL policy has been created before you run this command, the command directly displays the SSL policy view.

The **undo ssl policy** command deletes an SSL policy.

By default, no SSL policy is created.

Format

ssl policy *policy-name*

undo ssl policy *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an SSL policy.	The value is a string of 1 to 23 case-insensitive characters without spaces. The value can contain digits, letters, and underscores (_).

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Traditional FTP and HTTP protocols does not have the security mechanism. Data that is transmitted in plain text can be modified. User identity cannot be authenticated and data security cannot be ensured. The SSL security policy uses the data encryption, user identity authentication, and message integrity check mechanisms to ensure the security of the TCP-based application layer.

Follow-up Procedure

After you have run the **ssl policy** command to display the SSL policy view, perform either of the following operations:

- When the device functions as a server, run the **certificate load** to load the certificate or certificate chain.
- When the device functions as a client, run the **trusted-ca load** and **crl load** commands to load the trusted CA and CRL so that the server validity can be authenticated.

Precautions

- You can run the **ssl policy** command to create an SSL policy for the secure FTP and HTTP servers.
- A maximum of four SSL policies can be created.

Example

Create SSL policy **https_der** and display the SSL policy view.

```
<HUAWEI> system-view
[HUAWEI] ssl policy https_der
[HUAWEI-ssl-policy-https_der]
```

2.7.87 tftp

Function

The **tftp** command uploads a file to the TFTP server or downloads a file to the local device.

Format

Upload a file to the TFTP server or download a file to the local device based on the IPv4 address

tftp [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *tftp-server* [**public-net** | **vpn-instance** *vpn-instance-name*] { **get** | **put** } *source-filename* [*destination-filename*]

Upload a file to the TFTP server or download a file to the local device based on the IPv6 address

tftp ipv6 [**-a** *source-ip-address*] *tftp-server-ipv6* [**-oi** *interface-type interface-number*] { **get** | **put** } *source-filename* [*destination-filename*]

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the source IP address for connecting to the TFTP client. You are advised to use the loopback interface IP address.	-

Parameter	Description	Value
-i *interface-type interface-number*	Specifies the source interface used by the TFTP client to set up connections. It consists of the interface type and number. It is recommended that you specify a loopback interface. The IP address configured for this interface is the source IP address for sending packets. If no IP address is configured for the source interface, the TFTP connection cannot be set up.	-
-oi *interface-type interface-number*	Specifies an outbound interface on the local device.	If the remote host uses an IPv6 address, you must specify the outbound interface on the local device.
tftp-server	Specifies the IPv4 address or host name for the TFTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces.
tftp-server-ipv6	Specifies the IPv6 address of the IPv6 TFTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces.
public-net	Specifies the TFTP server on the public network.	-
vpn-instance *vpn-instance-name*	Name of the VPN instance where the TFTP server is located.	The value must be an existing VPN instance name.
get	Download a file.	-
put	Upload a file.	-
source-filename	Specifies the source file name.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Parameter	Description	Value
destination-filename	Specifies the destination file name.	The value is a string of 1 to 64 case-insensitive characters without spaces. By default, source and destination file names are the same.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When upgrading the system, you can run the **tftp** command to upload an important file to the TFTP server or download a system software to the local device.

Precautions

- When you run the **tftp** command to upload a file to the TFTP server in TFTP mode, files are transferred in binary mode by default. The tftp does not support the ASCII mode for file transfer.
- After specifying a source IP address, you can use this IP address to communicate with the server and implement packet filtering to ensure data security.
- You can run the **set net-manager vpn-instance** command to configure the NMS management VPN instance before running the **open** command to connect the FTP client and server.
  - If **public-net** or **vpn-instance** is not specified, the FTP client accesses the FTP server in the VPN instance managed by the NMS.
  - If **public-net** is specified, the FTP client accesses the FTP server on the public network.
  - If **vpn-instance** *vpn-instance-name* is specified, the FTP client accesses the FTP server in a specified VPN instance.

NOTE

The file system has a restriction on the number of files in the root directory. Therefore, if more than 50 files exist in the root directory, creating new files in this directory may fail.

Example

Download file **vrpcfg.txt** from the root directory of the TFTP server to the local device. The IP address of the TFTP server is 10.1.1.1. Save the downloaded file to the local device as file **vrpcfg.bak**.

```
<HUAWEI> tftp 10.1.1.1 get vrpcfg.txt flash:/vrpcfg.bak
```

Upload file **vrpcfg.txt** from the root directory of the storage device to the default directory of the TFTP server. The IP address of the TFTP server is 10.1.1.1. Save file **vrpcfg.txt** on the TFTP server as file **vrpcfg.bak**.

```
<HUAWEI> tftp 10.1.1.1 put flash:/vrpcfg.txt vrpcfg.bak
```

Obtain the link local IP address and interface name from the TFTP server.

```
<HUAWEI> tftp ipv6 FC00::/7 -oi gigabitethernet 0/0/1 get file1 file2
Info: Transfer file in binary mode.
Downloading the file from the remote TFTP server. Please wait...
100%
TFTP: Downloading the file successfully.
249704 byte(s) received in 10 second(s).
```

2.7.88 tftp client-source

Function

The **tftp client-source** command specifies the source IP address for the TFTP client to send packets.

The **undo tftp client-source** command restores the default source IP address for the TFTP client to send packets.

By default, the TFTP client source address is the IP address of the outbound interface connecting to the TFTP server, and it is displayed as 0.0.0.0.

Format

tftp client-source { **-a** *source-ip-address* | **-i** *interface-type interface-number* }

undo tftp client-source

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the source IP address of the TFTP client. You are advised to use the loopback interface IP address.	The value is in dotted decimal notation.

Parameter	Description	Value
-i *interface-type interface-number*	Source interface type and ID. You are advised to use the loopback interface. The IP address configured for this interface is the source IP address for sending packets. If no IP address is configured for the source interface, the TFTP connection cannot be set up.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If no source IP address is specified, the client uses the source IP address that the router specifies to send packets. The source IP address must be configured for an interface with stable performance. The loopback interface is recommended. Using the loopback interface as the source interface simplifies the ACL rule and security policy configuration. This shields the IP address differences and interface status impact, filters incoming and outgoing packets, and implements security authentication.

Prerequisites

The source interface specified using the command must exist and have an IP address configured.

Precautions

- The **tftp** command also configures the source IP address whose priority is higher than that of the source IP address specified in the **tftp client-source** command. If you specify source addresses in the **tftp client-source** and **tftp** commands, the source IP address specified in the **tftp** command is used for data communication. The source address specified in the **tftp client-source** command applies to all TFTP connections. The source address specified in the **tftp** command applies only to the current TFTP connection.
- You can query the source IP address or source interface IP address specified in the TFTP connection on the TFTP server.

Example

Set the source IP address of the TFTP client to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] tftp client-source -a 10.1.1.1
Info: Succeeded in setting the source address of the TFTP client to 10.1.1.1.
```


2.7.89 tftp-server acl

Function

The **tftp-server acl** command specifies the ACL number for the local device so that the device can access TFTP servers with the same ACL number.

The **undo tftp-server acl** command deletes the ACL number from the local device.

By default, no ACL number is specified on the local client.

Format

tftp-server [**ipv6**] **acl** *acl-number*

undo tftp-server [**ipv6**] **acl**

Parameters

Parameter	Description	Value
acl-number	Specifies the number of the basic ACL.	The value is an integer that ranges from 2000 to 2999.
ipv6	Specifies the IPv6 address of a specific server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To ensure the security of the local device, you need to run the **tftp-server acl** command to specify an ACL to specify TFTP servers that the local device can access.

Precautions

- The **tftp-server acl** command takes effect only after you run the **rule** command to configure the ACL rule. If no ACL rule is configured, the local device can access a specified TFTP server in TFTP mode.
- The TFTP supports only the basic ACL whose number ranges from 2000 to 2999.

Example

Allow the local device to the access the TFTP server whose ACL number is 2000.

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule permit source 10.10.10.1 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] tftp-server acl 2000
```

2.7.90 trusted-ca load

Function

The **trusted-ca load** command loads the trusted CA file for the SSL policy for the FTP client.

The **undo trusted-ca load** command unloads the trusted CA file of the SSL policy.

By default, no trusted CA file is loaded for the SSL policy.

Format

Load the trusted CA file for the SSL policy in ASN1 format.

trusted-ca load asn1-ca *ca-filename*

Load the trusted CA file for the SSL policy in PEM format.

trusted-ca load pem-ca *ca-filename*

Load the trusted CA file for the SSL policy in PFX format.

trusted-ca load pfx-ca *ca-filename* **auth-code cipher** *auth-code*

Unload the trusted CA file for the SSL policy.

undo trusted-ca load { **asn1-ca** | **pem-ca** | **pfx-ca** } *ca-filename*

Parameters

Parameter	Description	Value
asn1-ca	Load the trusted CA file for the SSL policy in ASN1 format.	-
pem-ca	Load the trusted CA file for the SSL policy in PEM format.	-
pfx-ca	Load the trusted CA file for the SSL policy in PFX format.	-

Parameter	Description	Value
ca-filename	Specifies the name of the trusted CA file. The file is in the subdirectory of the system directory **security**. If the **security** directory does not exist in the system, create this directory.	The value is a string of 1 to 64 characters. The file name is the same as that of the uploaded file.
auth-code cipher *auth-code*	Specifies the verification code for the trusted CA file in PFX format. The authentication code verifies user identity to ensure that only authorized users can log in to the server.	The value is a string of case-sensitive characters without spaces. If the value begins and ends with double quotation marks (" "), the string of characters can contain spaces. When the value is displayed in plaintext, its length ranges from 1 to 31. When the value is displayed in ciphertext, its length is 48 or 68. A ciphertext password with the length of 32 or 56 characters is also supported.

Views

SSL policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

CAs that are widely trusted in the world are called root CAs. Root CAs can authorize other lower-level CAs. The identity information about a CA is provided in the file of a trusted CA. To ensure the communication security and verify the server validity, you must run the **trusted-ca load** command to load the trusted CA file.

Prerequisites

Before running the **trusted-ca load** command, you have run the **ssl policy** command to create the SSL policy in the system view.

Precautions

A maximum of four trusted CA files can be loaded for an SSL policy. For the sake of security, deleting the installed trusted CA file is not recommended; otherwise, services using the SSL policy will be affected.

Example

Load the trusted CA file for the SSL policy in ASN1 format.

```
<HUAWEI> system-view
[HUAWEI] ssl policy ftp_server
[HUAWEI-ssl-policy-ftp_server] trusted-ca load asn1-ca servercert.der
```

Load the trusted CA file for the SSL policy in PEM format.

```
<HUAWEI> system-view
[HUAWEI] ssl policy ftp_server
[HUAWEI-ssl-policy-ftp_server] trusted-ca load pem-ca servercert.pem
```

Load the trusted CA file for the SSL policy in PFX format.

```
<HUAWEI> system-view
[HUAWEI] ssl policy ftp_server
[HUAWEI-ssl-policy-ftp_server] trusted-ca load pfx-ca servercert.pfx auth-code cipher YsHsjx_202206
```

2.7.91 undelete

Function

The **undelete** command restores a file that has been temporally deleted from or moved to the recycle bin.

Format

undelete { *filename* | *devicename* }

Parameters

Parameter	Description	Value
filename	Specifies the name of a file to be restored.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "

Parameter	Description	Value
devicename	Specifies the storage device name.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **undelete** command to restore a file that has been temporally deleted and moved to the recycle bin. However, files that are permanently deleted by running the **delete** or **reset recycle-bin** command with the **/unreserved** parameter cannot be restored.

The following describes the drive name.

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Like *devicename*, **drive** specifies the storage device name.

Precautions

- To display information about a temporally deleted file, run the **dir /all** command. The file name is displayed in square brackets ([ ]).
- If the name of a file is the same as an existing directory, the file cannot be restored. If the destination file has the same name as an existing file, the system prompts you whether to overwrite the existing file. The system prompt is displayed only when **file prompt** is set to **alert**.

Example

Restore file **sample.bak** from the recycle bin.

```
<HUAWEI> undelete sample.bak
Undelete flash:/sample.bak ?[Y/N]:y
%Undeleted file flash:/sample.bak.
```

Restore a file that has been moved from the root directory to the recycle bin.

```
<HUAWEI> undelete flash:
Undelete flash:/test.txt?[Y/N]:y
%Undeleted file flash:/test.txt.
Undelete flash:/rr.bak?[Y/N]:y
%Undeleted file flash:/rr.bak.
```

2.7.92 unzip

Function

The **unzip** command decompresses a file.

Format

unzip *source-filename destination-filename*

Parameters

Parameter	Description	Value
source-filename	Specifies the name of a source file to be decompressed.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "

Parameter	Description	Value
destination-filename	Specifies the name of a destination file that is decompressed.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can decompress files, especially log files that are stored on the storage device and run the **more** command to query the file.

The following describes the drive name.

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.
  - chassis ID#flash: root directory of the flash memory on a device in the stack.

  For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Precautions

- If the destination file path is specified while the file name is not specified, the designation file name is the same as the source file name.
- The source file persists after being decompressed.
- The compressed file must be a .zip file. If a file to be decompressed is not a zip file, the system displays an error message during decompression.
- The source file must be a single file. If you attempt to decompress a directory or multiple files, the decompression cannot succeed.

Example

Decompress log file **logfile-2012-02-27-17-47-50.zip** that is stored in the **logfile** directory and save it to the root directory as file **log.txt**.

```
<HUAWEI> pwd
flash:/logfile
<HUAWEI> unzip logfile-2012-02-27-17-47-50.zip flash:/log.txt
Extract flash:/logfile/logfile-2012-02-27-17-47-50.zip to flash:/log.txt?[Y/N]:y
100%  complete
%Decompressed file flash:/logfile/logfile-2012-02-27-17-47-50.zip to flash
:/log.txt.
```

2.7.93 user

Function

The **user** command changes the current FTP user when the local device is connected to the FTP server.

Format

user *user-name* [*password*]

Parameters

Parameter	Description	Value
user-name	Specifies the name of a login user.	The value is a string of 1 to 255 case-insensitive characters without space.
password	Specifies the login password.	The value is a string of 1 to 255 case-sensitive characters without space, single quotation mark, or question mark.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the device accesses the remote FTP server, to switch from the current user to another user, you only need to run the **user** command to log in to the FTP server by using another user name without disconnecting the FTP connection.

Precautions

After you run the **user** command to change the current user, a new FTP connection is set up, which is the same as that you specify using the **ftp** command.

Example

Log in to the FTP server using the user name **tom**.

```
<HUAWEI> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] user tom
331 Password required for tom.
Enter password:
230 User logged in.
```

2.7.94 verbose

Function

The **verbose** command enables the verbose function on the FTP client.

The **undo verbose** command disables the verbose function.

By default, the verbose function is enabled.

Format

verbose

undo verbose

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

After the verbose function is enabled, all FTP responses are displayed on the FTP client, including FTP protocol information and details about the responses.

Example

Enable the verbose function.

```
<HUAWEI> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[ftp] verbose
Info: Succeeded in switching verbose on.
[ftp] get h1.txt
200 Port command okay.
150 Opening ASCII mode data connection for h1.txt.

226 Transfer complete.
FTP: 69 byte(s) received in 0.160 second(s) 431.25byte(s)/sec.
```

Disable the verbose function.

```
[ftp] undo verbose
Info: Succeeded in switching verbose off.
[ftp] get h1.txt

FTP: 69 byte(s) received in 0.150 second(s) 460.00byte(s)/sec.
```

2.7.95 zip

Function

The **zip** command compresses a file.

Format

zip *source-filename destination-filename*

Parameters

Parameter	Description	Value
source-filename	Specifies the name of a source file to be compressed.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "
destination-filename	Specifies the name of a destination file that is compressed.	The value is a string of 1 to 160 case-insensitive characters without spaces in the format [drive] [path] filename. If the string is enclosed in double quotation marks (" "), the string can contain spaces. If the value is a file name, the value is a string of 1 to 64 characters. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. The directory name cannot contain the following characters: ~ * / \ : ' "

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the drive name.

- **drive** is the storage device and is named as **flash:**.
- If devices are stacked, **drive** can be named as:
  - flash: root directory of the flash memory of the master switch in the stack.

– chassis ID#flash: root directory of the flash memory on a device in the stack.

For example, **slot2#flash:** indicates the flash memory in slot 2.

The path can be an absolute path or relative path. A relative path can be designated relative to either the root directory or the current working directory. A relative path beginning with a slash (/) is a path relative to the root directory.

- **flash:/my/test/** is an absolute path.
- **/selftest/** is a path relative to the root directory and indicates the selftest directory in the root directory.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Precautions

- If the destination file path is specified while the file name is not specified, the designation file name is the same as the source file name.
- The source file persists after being compressed.
- Directories cannot be compressed.

Example

Compress file **log.txt** that is stored in the root directory and save it to the **test** directory as file **log.zip**.

```
<HUAWEI> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-            155  Dec 02 2011 01:28:48   log.txt
    1  -rw-          9,870  Oct 01 2011 00:22:46   patch.pat
    2  drw-              -  Mar 22 2012 00:00:48   test
    3  -rw-            836  Dec 22 2011 16:55:46   rr.dat
...

65,233 KB total (7,289 KB free)
<HUAWEI> zip log.txt flash:/test/log.zip
Compress flash:/log.txt to flash:/test/log.zip?[Y/N]:y
100%  complete
%Compressed file flash:/log.txt to flash:/test/log.zip.
<HUAWEI> cd test
<HUAWEI> dir
Directory of flash:/test/

  Idx  Attr     Size(Byte)  Date        Time       FileName
    0  -rw-            836  Mar 20 2012 19:49:14   test
    1  -rw-            239  Mar 22 2012 20:57:38   test.txt
    2  -rw-          1,056  Dec 02 2011 01:28:48   log.txt
    3  -rw-            240  Mar 22 2012 21:23:46   log.zip

65,233 KB total (7,288 KB free)
```

2.8 Configuring System Startup Commands

2.8.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

2.8.2 check file-integrity

Function

The **check file-integrity** command checks whether a file is consistent with the corresponding signature file.

Format

check file-integrity *filename signature-filename*

Parameters

Parameter	Description	Value
filename	Specifies the name of a file to be checked. The file must exist.	The value is a string of 4 to 64 case-insensitive characters without spaces. The file name extension can be .cc, .pat, .zip, .mod, or .7z.
signature-filename	Specifies the name of the signature file corresponding to the file to be checked. The signature file must exist.	The value is a string of 5 to 64 case-insensitive characters without spaces. The file name extension must be .asc or .p7s.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to check whether a file is consistent with the corresponding signature file. If the check fails, the file cannot be used as the system software, patch file, web page file, or mod file.

NOTE

Signature files are released with each version. Each valid system software, patch file, web page file, or mod file has a corresponding signature file. You need to upload the signature file to the switch before using this command.

Example

Check whether the system software is consistent with the corresponding signature file.

```
<HUAWEI> system-view
[HUAWEI] check file-integrity S5700-V200R023C00.cc S5700-V200R023C00.cc.asc
```

2.8.3 clear configuration interface

Function

Using the **clear configuration interface** command, you can perform one-touch configuration clearance on an interface.

Format

clear configuration interface { *interface-type-start interface-number-start* [**to** *interface-type-end interface-number-end*] } &<1-10>

Parameters

Parameter	Description	Value
interface-type-start interface-number-start [**to** *interface-type-end interface-number-end*]	Indicates the type and number of the interface where one-touch configuration clearance is performed. • *interface-type-start* specifies the type of the first interface. • *interface-number-start* specifies the number of the first interface. • *interface-type-end* specifies the type of the last interface. • *interface-number-end* specifies the number of the last interface.	At present, the tunnel and stack-port interfaces are not supported.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure an interface on a device for other use, original configurations on the interface need to be deleted one by one. If the interface has a large number of configurations, deleting these configurations one-by-one takes a long time and increases the maintenance workload. To reduce the maintenance workload and simplify the deletion operation, you can use this command to perform one-touch configuration clearance on an interface.

You can also run the **clear configuration this** command in the system view to delete configurations on a specified interface.

NOTE

The one-touch configuration clearance function cannot delete the **combo-port** command on an interface.

Configuration Impact

After this command is run, all configurations on an interface will be cleared. The status of the interface is **shutdown**.

Precautions

The execution of this command takes a long time. To terminate the running command, press **Ctrl**+**C**.

In general, after the **clear configuration this** command is run on an interface to clear the configuration, the default configuration is restored. If special configurations exist on the interface on which the **clear configuration this** command is run, the configuration may be displayed in the **undo** command format.

Example

Perform one-touch configuration clearance on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/1
 port link-type hybrid
 port hybrid pvid vlan 50
#
return
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] clear configuration interface gigabitethernet 0/0/1
Warning: All configurations of the interface will be cleared, and its state will
 be shutdown. Continue? [Y/N] :y...
Info: Total execute 2 command(s), 2 successful, 0 failed.
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/1
 shutdown
#
return
```


2.8.4 clear configuration this

Function

The **clear configuration this** command deletes configurations on an interface at a time to restore the default configurations.

Format

clear configuration this

Parameters

None

Views

Interface view (excluding tunnel interface view, stack-port interface view, and port group view)

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure an interface on a device for other use, original configurations on the interface need to be deleted one by one. If the interface has a large number of configurations, deleting these configurations one-by-one takes a long time and increases the maintenance workload. To reduce the maintenance workload and simplify the deletion operation, you can use this command to perform one-touch configuration clearance on an interface.

You can also run the **clear configuration interface** *interface-type interface-num* command in the system view to delete configurations on a specified interface.

Configuration Impact

After you run the **clear configuration this** command, the system displays a message, asking you whether to delete the configurations on the specified interface. If you enter **Y**, all configurations on the specified interface are deleted and the interface status becomes shutdown.

Running the **clear configuration this** command on an interface is similar to running undo commands on the interface in batches.

Precautions

The execution of this command takes a long time. To terminate the running command, press **Ctrl**+**C**.

In general, after the **clear configuration this** command is run on an interface to clear the configuration, the default configuration is restored. If special

configurations exist on the interface on which the **clear configuration this** command is run, the configuration may be displayed in the **undo** command format.

As some commands correlate to each other, if you run the **undo** command to delete the configurations of a command, the configurations of the correlated command are also deleted. After the **clear configuration this** command is run on an interface, the statistics in the command output may be inconsistent with actual clearance results. Refer to the actual clearance results in real-world applications.

Example

Perform one-touch configuration clearance on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/1
 description abc
 port link-type access
#
return
[HUAWEI-GigabitEthernet0/0/1] clear configuration this
Warning: All configurations of the interface will be cleared, and its state will be shutdown. Continue? [Y/
N] :y
Info: Total 2 command(s) executed, 2 successful, 0 failed.
[HUAWEI-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/1
 shutdown
#
return
```

2.8.5 clear inactive-configuration all

Function

The **clear inactive-configuration all** command clears inactive configurations on the switch.

NOTE

This command can only clear inactive configurations on interfaces.

Format

clear inactive-configuration all

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

If a card is removed, the original configurations on the card are saved on the switch. If the standby/slave switch leaves a stack, the configurations on the switch are saved on the master switch. These invalid configurations are called inactive or offline configurations. To view inactive configurations on the switch, run the **display current-configuration inactive** command.

You can run the **clear inactive-configuration all** command to clear all the inactive configurations on the switch to increase available space.

This command can be run by only one user at a time to clear inactive configurations on all interfaces on the device.

NOTICE

Configurations cannot be recovered after clearing. Therefore, exercise caution when deciding to run this command. You are advised to run this command under the guidance of technical support personnel.

Example

Clear inactive configurations on the switch.

```
<HUAWEI> system-view
[HUAWEI] clear inactive-configuration all
Warning: All inactive configurations will be deleted and cannot be restored.
Are you sure you want to continue?[Y/N]y
The command will take a few minutes. Please wait.
Info: There is no inactive configuration.
```

2.8.6 configuration backup local disable

Function

The **configuration backup local disable** command disables the device from backing up the running configurations locally.

The **undo configuration backup local disable** command enables the device to back up the running configurations locally.

By default, the device is enabled to back up the running configurations locally.

Format

configuration backup local disable

undo configuration backup local disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To automatically back up the current running configurations to the local storage after the device configurations are modified, run the **undo configuration backup local disable** command to enable automatic backup of the current running configurations. This function helps check historical records of configuration changes and facilitate fault location.

Precautions

- When the device is enabled to back up the current running configurations, the current running configurations are backed up 2 hours after the device configurations are modified. If saving or automatic saving operation is performed, conflicts may occur. The configuration backup will be triggered every 30 minutes until the backup succeeds.
- If the CPU usage exceeds 60% during the configuration backup, the configuration backup will be triggered every 30 minutes until the backup succeeds.
- Delivering a configuration command fails during the configuration backup.
- If the current configurations are consistent with the configurations saved last time, the device does not repeatedly back up the current configurations to the local storage.

Rules for backup file management:

- The local storage path is **$_backup/running_config/**.
- The format of the backup file name is **yyyymmddhhmmss.sysname.zip**, where **yyyymmdd** indicates the year, month, and day, **hhmmss** indicates the hour, minute, and second, and **sysname** indicates the host name of the device.
- Backup files are aged based on the aging rules each time when the number of backup files exceeds 30, when the total space used by backup files exceeds 10 MB, or when the remaining storage space is less than 30 MB.
- The backup file aging stops when the number of backup files is 5 or less.

Rules for backup file aging:

- A number and an aging priority are specified for a backup file based on the file generation time.

NOTE

File number: The latest file generated is numbered 1, the file generated before the latest file is numbered 2, and so on. A larger number indicates an earlier generation time.

File aging priority: The file with a smaller file number has a higher priority. Files with a lower priority are aged first. Note that files with priority 0 are not aged. If a file has multiple priorities, refer to the highest priority.

- Priority 0: files numbered from 1 to 5
- Priority 1: files numbered from 6 to 10
- Priority 2: the last generated files on each day in the past week
- Priority 3: the last generated files in each month in the past 5 months
- Priority 4: other backup files

- Note for backup file aging:
  - The backup files are aged in time sequence based on the priority. A backup file generated earlier is aged first.

Example

Disable the device from backing up the running configurations locally.

```
<HUAWEI> system-view
[HUAWEI] configuration backup local disable
```

2.8.7 configuration copy file to running

Function

The **configuration copy file to running** command executes commands in a specified configuration file.

Format

configuration copy file *file-name* **to running**

Parameters

Parameter	Description	Value
file-name	Specifies the name of a configuration file to be executed.	The value is a string of 4 to 160 characters in the [*drive*] [*path*] *file-name* format. The file name extension must be .cfg or .zip.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To execute an existing configuration file, run the **configuration copy file to running** command. All the commands in the specified configuration file are executed at one time.

Precautions

- Only one user can execute the **configuration copy file to running** command at one time.
- Running this command does not clear the existing configuration.
- If configuration restoration occurs or a batch backup operation is performed, the **configuration copy file to running** command ends.
- If a command fails during the execution of the **configuration copy file to running** command, the system skips it and executes the next command.
- If the configuration file to be executed contains a restart command, the device will restart when the restart command is executed. Therefore, exercise caution when executing the configuration file.
- Do not change the configuration file manually and execute the configuration file. Otherwise, the device may not start normally.

Example

Execute the commands in the **huawei.cfg** file.

```
<HUAWEI> configuration copy file huawei.cfg to running
Warning: This operation may take a long time, press CTRL+C to break. Continue?[Y/N]:y
```

2.8.8 configuration copy startup to file

Function

The **configuration copy startup to file** command backs up the startup configuration file to a specified file.

Format

configuration copy startup to file *file-name*

Parameters

Parameter	Description	Value
file-name	Specifies the name of a destination file.	The value is a string of 4 to 160 characters in the [*drive*] [*path*] *file-name* format. The file name extension must be .cfg or .zip. The extension of the destination file and the backup file must be the same.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To back up the startup configuration file, run the **configuration copy startup to file** command.

Precautions

If a file with the same name already exists, the system asks whether to replace the previous file. Press **Y** to replace the file or **N** not to do so.

Example

Back up the startup configuration file to the **huawei.cfg** file.

```
<HUAWEI> configuration copy startup to file huawei.cfg
```

2.8.9 compare configuration

Function

The **compare configuration** compares whether the current configurations (including offline configurations) are identical with the next startup configuration file.

Format

compare configuration [*configuration-file*] [*current-line-number save-line-number*]

Parameters

Parameter	Description	Value
configuration-file	Specifies the name of the configuration file to be compared with the current configurations.	The value is a string of 5 to 48 case-insensitive characters without spaces.
current-line-number	Specifies the line number for comparison in the current configuration.	The value is an integer that ranges from 0 to 65535.

Parameter	Description	Value
save-line-number	Specifies the line number for comparison in the saved configuration.	The value is an integer that ranges from 0 to 65535.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If *current-line-number* and *save-line-number* are not specified, the configuration files are compared from the first lines. The two parameters can be specified to skip the differences that are found and continue the comparison.

The **compare configuration** command outputs display the current configuration file (including offline configurations) and the saved configuration file from the line that contains differences respectively. By default, the output difference information is restricted to 120 characters.

- If the characters from differences to the end of the configuration file are less than 120, the system displays the output difference information till the end of the configuration file.
- If the characters from differences to the end of the configuration file are more than 120, the system only displays 120 characters.

Precautions

- The execution of this command takes a long time. To terminate the running command, press **Ctrl+C**.
- The configuration file name extension must be .cfg or .zip.
- If *configuration-file* is not specified, the system compares whether the current configurations (including offline configurations) are identical with the next startup configuration file.
- If *configuration-file* is specified, the system compares whether the current configurations (including offline configurations) are identical with the specified startup configuration file.

Example

Compare whether the current configurations (including offline configurations) are identical with the next startup configuration file.

```
<HUAWEI> compare configuration
Info: The system is now comparing the configuration, please wait....
Warning: The current configuration is not the same as the next startup
configuration file. There may be several differences, and the following are some
```



```
configurations beginning from the first:
====== Current configuration line 6 ======
 vlan batch 1 to 2 10 to 11 15 70 to 71 91 to 92 100 111 230 240 901
 vlan batch 911 1111
#
 l2protocol-tunnel vtp group-mac xxxx-xxxx-xxxx

 ====== Configuration file line 6 ======
 vlan batch 1 to 2 10 to 11 15 70 91 to 92 100 111 230 240 901
 vlan batch 911 1111
#
 l2protocol-tunnel vtp group-mac xxxx-xxxx-xxxx
```

2.8.10 display changed-configuration time

Function

The **display changed-configuration time** command displays the time of the last configuration change.

Format

display changed-configuration time

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After changing the configuration of the device, you can run the **display changed-configuration time** command to view the time of the last configuration change.

Example

Display the time of the last configuration change.

```
<HUAWEI> display changed-configuration time
```

2.8.11 display configuration recover-result

Function

The **display configuration recover-result** command displays the configuration recovery result.

Format

display configuration recover-result

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can use the **display configuration recover-result** command to view the information about the configuration recovery result and records of configuration recovery failures. The records include the command that fails the configuration recovery, the view in which the command resides, the line number of the command in the current startup configuration file, the reason why the command fails, and the execution time of the configuration recovery.

This command displays a maximum of 256 records in time sequence. The latest record is displayed in the last. If the number of commands for configuration recovery exceeds 256, the device no longer records commands that fail the configuration recovery.

Prerequisites

The device has restarted and the configuration recovery is successful.

Example

Display the configuration result.

```
<HUAWEI> display configuration recover-result
The current startup saved-configuration file is flash:/vrpcfg.zip.
The number of failed commands is 2.
-------------------------------------------------------------------------

Command : ip address 10.85.1.1 255.255.255.0
View    : Vlanif85
Line    : 414
Reason  : Failed to parse the command.
Time    : 10:00:06  2012-07-25 UTC+08:00 DST

Command : ip address 10.86.1.1 255.255.255.0
View    : Vlanif86
Line    : 417
Reason  : Failed to parse the command.
Time    : 10:00:06  2012-07-25 UTC+08:00 DST

-------------------------------------------------------------------------
```


Table 2-55 Description of the display configuration recover-result command output

Item	Description
Command	Command that fails the configuration recovery
View	View in which the command resides
Line	Line number of the command in the current startup configuration file
Reason	Reason why the command fails
Time	Execution time of the configuration recovery

2.8.12 display current-configuration

Function

The **display current-configuration** command displays the currently running configuration.

This command does not display parameters that use default settings.

Format

display current-configuration [**configuration** [*configuration-type* [*configuration-instance*]] | **interface** [*interface-type* [*interface-number*]]] [**feature** *feature-name*] [**filter** *filter-expression*]

display current-configuration [**all** | **inactive**]

display current-configuration configuration vpn-instance [*vpn-instance-name*] **related**

NOTE

Only the S5720I-SI, S5735-S, S500, S5735S-S, S5735-S-I, S5735S-H, S5736-S, S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6735-S, S6720-EI, S6720S-EI, S6720S-S, S6730-H, S6730S-H, S6730-S, and S6730S-S support the **display current-configuration configuration vpn-instance** [*vpn-instance-name*] **related** command.

Parameters

Parameter	Description	Value
configuration	Displays all configuration information, except for the configuration on interfaces.	-

Parameter	Description	Value
configuration-type	Specifies information about the configuration that is a specified type, except for the configuration on interfaces. The configuration type depends on the existing configuration. For example: ● system: system configuration ● user-interface: user interface configuration ● aaa: AAA configuration	-
configuration-instance	Specifies information about the specified configuration instance, except for the configuration on interfaces. The configuration instance depends on the existing configuration.	The value is a string of 1 to 180 case-insensitive characters without spaces.
interface [*interface-type* [*interface-number*]]	Specifies an interface type. The information on the interface depends on the existing configuration. ● *interface-type*: specifies the type of an interface ● *interface-number*: specifies the number of an interface	-
feature *feature-name*	Specifies the configuration information about the specified feature. The configuration information about the feature depends on the existing configuration.	-

Parameter	Description	Value
filter *filter-expression*	Displays the configuration information that matches a regular expression.	The value is a string of 1 to 255 case-insensitive characters, spaces not supported. The matching starts from the first character of the command. For example, if snmp-agent is specified for *filter-expression*, only commands beginning with snmp-agent are filtered.
all	Displays all the configuration information.	-
inactive	Displays configurations about the cards that are not installed. When a card is not inserted, its configuration information is in the inactive status. The front of these configurations in the inactive state is marked with an asterisk (*).	-
vpn-instance [*vpn-instance-name*]	Displays configurations of a VPN instance with a specified name.	The value must be an existing VPN instance name.
related	Displays configurations of a specified module.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

To check whether the configured parameters take effect, run the **display current-configuration** command. The parameters that do not take effect are not displayed.

The command output is relevant to user configuration.

You can use a regular expression to filter the command output. For the regular expression rules, see Filtering Output Information Based on the Regular Expression in "CLI Overview" in the *S300, S500, S2700, S5700, and S6700 V200R023C00 Configuration Guide - Basic Configuration*.

If the configuration is in the offline state, the offline configuration is marked with * in the **display current-configuration all** and **display current-configuration inactive** command output.

Example

Display all configurations that include **vlan**.

```
<HUAWEI> display current-configuration | include vlan
vlan batch 10 77 88
 port trunk allow-pass vlan 10
```

Display the FTP feature configuration.

```
<HUAWEI> display current-configuration feature ftp
#
FTP server enable
#
------------ END ------------
```

2.8.13 display factory-configuration information

Function

The **display factory-configuration information** command displays whether the function of restoring the factory configuration by holding down the Reset button is enabled and the mode of restoring the factory configuration.

NOTE

Only the SS1720GW-E, S1720GWR-E, and S1720GFR-P support this command.

Format

display factory-configuration information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before restoring the factory configuration by holding down the Reset button, you can run this command to check whether the function of restoring the factory configuration by holding down the Reset button is enabled and whether the mode of restoring the factory configuration is deleted or reserved.

Example

Display whether the function of restoring the factory configuration by holding down the Reset button is enabled and the mode of restoring the factory configuration.

```
<HUAWEI> display factory-configuration information
Reset function status: enable
Operate mode: deleted
```

Table 2-56 Description of the **display factory-configuration information** command output

Item	Description
Reset function status	Whether the function of restoring the factory configuration after you hold down the Reset button is enabled. • enable: When you hold down the Reset button on a device, the device restarts with the factory configuration. • disable: When you hold down the Reset button on a device, the device restarts without the factory configuration.
Operate mode	Mode of restoring the factory configuration. • deleted: The system deletes the previous configuration when restoring the factory configuration. • reserved: The system reserves the previous configuration when restoring the factory configuration.

2.8.14 display factory-configuration reset-result

Function

The **display factory-configuration reset-result** command displays the latest factory configuration restoration result of a switch.

Format

display factory-configuration reset-result

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the factory configuration of a switch is restored using the **reset factory-configuration** command, you can run the **display factory-configuration reset-result** command to check the factory configuration restoration result.

Example

Display the latest factory configuration restoration result.

```
<HUAWEI> display factory-configuration reset-result
Slot   Time                      Type                          Result
-------------------------------------------------------------------------------
0      2017/10/11 15:55:11 [DST]  Startup saved-configuration file     Succeeded
                                  Configuration in flash              Succeeded
                                  Netconf db-configuration            Succeeded
                                  Data file                           Succeeded
```

Table 2-57 Description of the **display factory-configuration reset-result** command output

Item	Description
Slot	Stack ID.
Time	Time for restoring the factory configuration.

Item	Description
Type	Type of the configuration file that needs to be restored to the factory configuration. • Startup saved-configuration file: configurations in the configuration file • Configuration in flash: configurations in the flash, such as the stack configuration • Netconf db-configuration: database files of the NETCONF and NETCONF • Data file: data files in the file system
Result	Result of restoring the factory configuration of the configuration file. • Succeeded: Factory configuration restoration succeeds. • Failed: Factory configuration restoration fails.

2.8.15 display pnp-button mode

Function

The **display pnp-button mode** command displays the device behavior after the PNP button is pressed and held.

Format

display pnp-button mode

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After running the **pnp-button mode reset-system** command to configure the device behavior after the PNP button is pressed and held, you can run the **display pnp-button mode** command to view the command configuration.

Example

Display the device behavior after the PNP button is pressed and held.

```
<HUAWEI> display pnp-button mode
Pnp configuration mode: reset single switch.
Pnp button enable: enable.
```

Table 2-58 Description of the **display pnp-button mode** command output

Item	Description
Pnp configuration mode	PnP configuration mode: • reset system: The default settings of the stack will be restored and the stack will automatically restart. • reset single switch: The default settings of a specific stack member will be restored and the stack member will automatically restart.
Pnp button enable	Whether the PNP button is available: • enable: The PNP button is available. • disable: The PNP button is unavailable.

2.8.16 display reboot-info

Function

The **display reboot-info** command displays the device reset information.

Format

display reboot-info [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	• Specifies the slot ID if stacking is not configured. • Specifies the stack ID if stacking is configured.	The value is an integer. The value is 0 if stacking is not configured, and varies according to the stacking configuration if stacking is configured.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check the type and time of a reset.

This command displays reset information collected by the device, including the reset type and time. The following reset types may be displayed:

- MANUAL: The device was restarted manually using the **reboot** command or the NMS.
- POWER: The device restarted after being powered off (usually because users switch off the power supply).
- SCHEDU: The device restarted at a scheduled time.
- FSP: The device restarted due to a stack split or merge or an incorrect Mod-ID.
- EXCEPTION: The device restarted due to an exception or a dead loop.
- VRP: The device restarted due to an active/standby switchover or a fault on the VRP platform.
- SOFTWARE: The device restarted due to a software fault which is traceable.
- OS: The kernel was abnormal and initiated a reset.
- WATCHDOG: The device restarted due to the hardware watchdog.
- OTHER: Other causes.
  - A hardware component, such as the CPU, flash, or memory, has failed.
  - The device has overheated.
  - The switch was power recycled instantly, for example, when the power cable is in bad contact or when transient overvoltage and loss of voltage occurs. In this case, check whether the power cable is correctly connected to the switch.
  - The reboot was caused by other reasons that cannot be categorized into the preceding types. For example, the switch rebooted after joining a stack.

Example

Display the device reset information.

```
<HUAWEI> display reboot-info
Slot ID   Times        Reboot Type         Reboot Time(DST)
================================================================================
0           1        POWER              2013/07/18 19:19:56
0           2        SCHEDU             2013/07/18 18:51:04
0           3        SOFTWARE            2013/07/18 18:41:22
0           4        EXCEPTION           2013/07/18 17:38:26
0           5        MANUAL              2013/07/18 17:31:14
0           6        MANUAL              2013/07/18 17:26:01
0           7        EXCEPTION           2013/07/18 17:03:28
================================================================================
Total   7
```

Table 2-59 Description of the display reboot-info command output

Item	Description
Slot ID	Stack ID if the stacking function is enabled or the slot ID if the stacking function is not enabled.
Times	Number of board resets.
Reboot Type	Types of reset, including MANUAL, POWER, SCHEDU, FSP, EXCEPTION, VRP, SOFTWARE, OS, WATCHDOG, and OTHER.
Reboot Time(DST)	Time when a board was reset. On devices that do not support RTC, the device synchronizes the system clock on the network after the NTP function is configured. During the synchronization, the system time when the device is delivered is displayed. If synchronization fails, the system time when the device is delivered is displayed.

2.8.17 display saved-configuration

Function

The **display saved-configuration** command displays the configuration file to be used for the next startup.

Format

display saved-configuration [**last** | **time** | **configuration**]

Parameters

Parameter	Description	Value
last	Displays the system configurations saved last time.	-

Parameter	Description	Value
time	Displays the recent time when the configurations are saved manually or automatically.	-
configuration	Displays the parameters of the automatic save function.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

If the device has been started and is not working properly, run the **display saved-configuration** command to check the device startup configuration in the file specified by running the **startup saved-configuration** command.

Run the **display saved-configuration last** command to check the system configurations saved last time in the configuration file loaded during the current startup.

Run the **display saved-configuration time** command to check the last time when the system configurations are saved.

Run the **display saved-configuration configuration** command to check the automatic save function parameters including the automatic save interval and CPU usage.

The command output is relevant to user configuration.

Example

Display the configuration file for the next startup.

```
<HUAWEI> display saved-configuration
#
 sysname Switch
...
#
 vlan batch 10 20
#
interface Vlanif10
 ip address 192.168.1.3 255.255.255.0
#
interface Vlanif20
 ip address 192.168.4.3 255.255.255.0
...
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
...
```



```
#
user-interface maximum-vty 15
user-interface con 0
user-interface vty 0 14
 idle-timeout 0 0
#
return
```

2.8.18 display schedule reboot

Function

The **display schedule reboot** command displays the configuration of the scheduled restart of the device.

Format

display schedule reboot

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

After using the **schedule reboot** command to configure a scheduled restart, you can use this command to view the configuration of the scheduled restart.

Example

Display the configuration of the scheduled restart of the device.

```
<HUAWEI> display schedule reboot
Info:System will reboot at 22:00:00 2013/09/17 (in 1 hours and 43 minutes).
```

Table 2-60 Description of the display schedule reboot command output

Item	Description
System will reboot at	Specific restart time.
in hours and minutes	Time span between the restart time and the current time.

2.8.19 display startup

Function

The **display startup** command displays the system software and configuration files for the current and next startup.

Format

display startup [**slot** *slot-id*]

NOTE

Devices that do not support the stack function or do not have the stack function enabled do not support the **slot** *slot-id* parameters.

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies a member device in a stack.	The value is an integer. The range of the integer is dependent on the specific device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before upgrading or degrading a device, run this command to check whether the files for next startup have been loaded. If the files have been loaded, the device can be upgraded or degraded successfully after it is restarted. You can also run the command to view the system software and files for current startup.

The **display cli command-tree** command output shows that the **chassis** parameter is registered on the device. Fixed devices do not support this parameter.

Example

Display the names of system software for current and next startup.

```
<HUAWEI> display startup
MainBoard:
  Configured startup system software:       flash:/basicsoftware.cc
  Startup system software:                  flash:/basicsoftware.cc
  Next startup system software:             flash:/basicsoftware.cc
  Startup saved-configuration file:         flash:/vrpcfg.zip
  Next startup saved-configuration file:    flash:/vrpcfg.zip
  Startup paf file:                         NULL
  Next startup paf file:                    NULL
```

```
Startup license file:              NULL
Next startup license file:           NULL
Startup patch package:               NULL
Next startup patch package:            NULL
```

Table 2-61 Description of the display startup command output

Item	Description
Configured startup system software	System software that is configured for the current startup by running the **startup system-software** command before the system starts.
Startup system software	System software that is used in the current startup.
Next startup system software	System software that is configured for the next startup by running the **startup system-software** command. If no system software for the next startup is configured, the system software used in the current startup is displayed.
Startup saved-configuration file	Configuration file that is used in the current startup.
Next startup saved-configuration file	Configuration file that is configured for the next startup by running the **startup saved-configuration** command. If no configuration file for the next startup is configured, the configuration file used in the current startup is displayed.
Startup paf file	PAF file that is used in the current startup. **default** indicates that no PAF file is specified or the PAF file does not take effect. **NULL** indicates that no PAF file exists on the device.
Next startup paf file	PAF file that is configured for the next startup. If no PAF file is configured, **default** is displayed. **NULL** indicates that no PAF file exists on the device.

Item	Description
Startup license file	License file that is used in the current startup. **default** indicates that no license file is specified or the license file does not take effect. **NULL** indicates that no license file exists on the device.
Next startup license file	License file that is configured for the next startup. If no license file is configured, **default** is displayed. **NULL** indicates that no license file exists on the device.
Startup patch package	Patch package file that is used in the current startup. **NULL** indicates that no patch package file is specified or the patch package file does not take effect.
Next startup patch package	Patch package file that is configured for the next startup by running the **startup patch** command. If no patch package file is configured, **NULL** is displayed.

2.8.20 factory-configuration prohibit

Function

The **factory-configuration prohibit** command disables the function of restoring the factory settings of a device by holding down **reset**.

The **undo factory-configuration prohibit** command enables the function of restoring the factory settings of a device by holding down **reset**.

By default, you can hold down **reset** to restore the factory configuration.

NOTE

Only SS1720GW-E, S1720GWR-E, and support this command.

Format

factory-configuration prohibit

undo factory-configuration prohibit

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

If you hold down **reset** on a device for more than 5 seconds, the device restarts with the factory settings and all user-defined configurations are lost after the restart. To retain user-defined configurations after you hold down **reset**, run the **factory-configuration prohibit** command to disable this function.

If you want to restore the factory settings of a device by holding down **reset**, run the **undo factory-configuration prohibit** command to enable this function.

Example

Disable the function of restoring the factory configuration of a device by holding down **reset**.

```
<HUAWEI> system-view
[HUAWEI] factory-configuration prohibit
```

2.8.21 pnp-button mode reset-system

Function

The **pnp-button mode reset-system** command configures all member switches in a stack to restore to the default settings and restart after the PNP button is pressed and held.

The **undo pnp-button mode reset-system** command restores the default settings.

By default, a switch in a stack restores to the default settings and automatically restarts after the PNP button is pressed and held on the switch.

Format

pnp-button mode reset-system

undo pnp-button mode reset-system

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To clear all service configurations and data files, press and hold the PNP button for more than 6 seconds to restore the default settings and automatically restart the device. By default, holding the PNP button on any device in a stack will restore the device to the default settings and automatically restart the device. To clear the service configurations and data files of the stack, run the **pnp-button mode reset-system** command to configure the device behavior after the PNP button is pressed and held.

Example

Configure all member switches in a stack to restore to the default settings and automatically restart after the PNP button is pressed and held.

```
<HUAWEI> system-view
[HUAWEI] pnp-button mode reset-system
```

2.8.22 pnp-button disable

Function

The **pnp-button disable** command disables the PNP button function of a device.

The **undo pnp-button disable** command enables the PNP button function of a device.

By default, the PNP button function is enabled on a device.

Format

pnp-button disable

undo pnp-button disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If you do not want anyone to use the PNP button to reset the device configuration or restart the device, run the **pnp-button disable** command to disable the PNP button function of the device.

Example

Disable the PNP button function of the device.

```
<HUAWEI> system-view
[HUAWEI] pnp-button disable
```

2.8.23 reboot

Function

The **reboot** command restarts the device.

Format

reboot [**fast** | **save diagnostic-information**]

Parameters

Parameter	Description	Value
fast	Fast restarts the device. In fast restart mode, the configuration file is not saved.	-
save diagnostic-information	Saves the diagnostic information before the restart.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command functions in the same way as a power recycle operation (power off and then restart the device). The command enables you to restart the device remotely.

- If the configuration file for next startup (new configuration file) is the same as the configuration file saved on the device after the **reboot** command is run, the system will not ask you whether to save the configuration before the restart. If the configuration file for next startup (new configuration file)

differs from the configuration file saved on the device, the system asks you whether to save the configuration before the restart, and unsaved configuration information will be lost after the restart.

- When the **reboot fast** command is run, the system restart quickly without displaying any message and the configuration is lost.
- After the **reboot save diagnostic-information** command is run, the system will save the diagnostic information to root directory of the storage device before restarting.

Precautions

- If you do not respond to the displayed message within the timeout period after running this command, the system will return to the user view and the device will not be restarted.
- To avoid loss of diagnostic information after a restart, configure the device to save the diagnostic information before restarting.
- This command interrupts services on the entire device. Therefore, do not use this command when the device is running properly.
- Before restarting the device, ensure that the configuration file has been saved.
- If you upgrade the system software to V200R009C00 or a later version and the configuration file contains WLAN configurations, the system displays a message indicating that the configuration file conflicts with the system software for next startup when the device restarts. The system software upgrade fails. If a conflict occurs, you need to use the eDesk tool to convert configurations in the configuration file, and specify the converted configuration file as the configuration file for next startup. If the configuration file is not converted, the configurations will be lost after the system is restarted and upgraded.
- If multiple users run the **reboot save diagnostic-information** command at the same time, a message indicating that the command is locked by another user is displayed.
- If a user runs the **display diagnostic-information** command when another user is running the **reboot save diagnostic-information** command, a message indicating that the command is locked by another user is displayed.
- The S2730S-S, S5735-L-I, S5735-L1,S300, S5735-L, S5735S-L, S5735S-L1, S5735S-L-M, S5735-S, S500, and S5735S-S support the stacking function since V200R019C10. S5735-L-I supports the stacking function since V200R021C00. If multiple switches set up a stack and the system software package for the next startup is earlier than V200R019C10, the stack will split after the **reboot** command is executed to restart any stack member. If the stacking function is enabled on a single switch, the system software package for the next startup is earlier than V200R019C10, and the **stack slot renumber** command is executed to change the stack ID of the switch to a non-zero value, then the stack configuration of the switch will be cleared and the slot-ID-related configuration cannot be restored after the **reboot** command is executed to restart the switch.
- Due to the component upgrade of some device models, some devices cannot be downgraded. If the message "Error: The hardware version VER.B of slot %u does not support the configured system software package." (%u indicates the actual slot number) is displayed after the command is run, you can solve this problem by installing the patch that matches the version. For details about

the first supported version of the device and matching patch version, see the device overview in the "Hardware Description"..

NOTE

After converting configurations in the configuration file using the **eDesk pro** tool, restart the switch without saving the configurations. If the configurations are saved, the converted configuration file is invalid.

Example

Restart the device.

```
<HUAWEI> reboot
Info: The system is now comparing the configuration, please wait.....
Warning: The configuration has been modified, and it will be saved to the next s
tartup saved-configuration file flash:/204.cfg. Continue? [Y/N]:y
Info: If want to reboot with saving diagnostic information, input 'N' and then e
xecute 'reboot save diagnostic-information'.
System will reboot! Continue?[Y/N]:y
```

Restart the device quickly.

```
<HUAWEI> reboot fast
Info: If want to reboot with saving diagnostic information, input 'N' and then execute 'reboot save
diagnostic-information'.
System will reboot! Continue?[Y/N]:y
```

2.8.24 reset factory-configuration

Function

The **reset factory-configuration** command restores the factory settings of the device.

Format

reset factory-configuration

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To clear all service configurations and data files, run the **reset factory-configuration** command to restore the factory settings.

Precautions

After you run the **reset factory-configuration** command, the system asks you whether to restart the device. After you enter **y**, the device restarts and clears the service configurations and data files on the device. The configurations and files to be cleared include:

- Configurations in the configuration file
- Configurations in the flash memory, such as the stackconfigurations.
- Database files in NETCONF
- Data files in the file system

NOTE

- The next-startup system software package, patch, module, and license file will not be deleted.
- This command will not delete the protected directory and the $_default.cfg file in the protected directory.

NOTICE

Exercise caution and use this command under the supervision of technical support personnel.

Example

Restore the device to factory settings.

```
Warning: The command will delete all the configurations and files (except the startup, patch, module, and
license files) from the de
vice. Continue? [Y/N]:y
Warning: The system will reboot after configurations and files are deleted. Continue? [Y/
N]:y
```

2.8.25 reset saved-configuration

Function

The **reset saved-configuration** command clears the next startup configuration file and cancels the configuration file used for next startup.

Format

reset saved-configuration

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

- If the configuration file on the device is incompatible with the upgraded software, run the **reset saved-configuration** command to clear the configuration file and run the **startup saved-configuration** command to specify a new configuration file.
- If the device in use is applied to another scenario and the original configuration file of the device does not meet requirements in the scenario, run the **reset saved-configuration** command to clear the existing configuration file and restart the device to restore its factory configurations.

Precautions

- After you run the **reset saved-configuration** command, the next startup configuration file is cleared and the file is not used for next startup. If the current startup configuration file is the same as the next startup configuration file, the current startup configuration file is also cleared.
- If you do not use the **startup saved-configuration** command to specify a new configuration file or do not save the configuration file after the file is not used for next startup, the device uses default factory configurations for startup.
- If the current configuration file is empty, and the configuration file for the next startup is not empty, running the **reset saved-configuration** command clears the settings for the configuration file for the next startup.
- If the configuration file for the next startup is empty, and the current configuration file is not empty, after the **reset saved-configuration** command is run, the system prompts an error and no settings are cleared.
- Exercise caution when you run the **reset saved-configuration** command.
- Running the **reset saved-configuration** command will clear the content in the configuration file used for the next device startup but not clear the database information on the device. In NETCONF mode, run the **reset netconf db-configuration** command to clear the configuration and database file to prevent the configuration delivery failures caused by residual database files.
- After the **reset netconf db-configuration** or **reset saved-configuration** command is run, the **assign trunk** command configuration is cleared, that is, the default configuration is restored.

Example

Clear the next startup configuration file in the storage device and cancel the configuration file used for next startup.

```
<HUAWEI> reset saved-configuration
Warning: The action will delete the saved configuration in the device.
The configuration will be erased to reconfigure. Continue? [Y/N]:y
Warning: Now clearing the configuration in the device.
Info: Succeeded in clearing the configuration in the device.
```


2.8.26 reset reboot-info

Function

The **reset reboot-info** command resets the device reset information.

Format

reset reboot-info [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	• Specifies the slot ID if stacking is not configured. • Specifies the stack ID if stacking is configured.	The value is 0 if stacking is not configured; the value ranges from 0 to 8 if stacking is configured.

Views

User view

Default Level

3: Management level

Usage Guidelines

The device records information about every restart, including the number of restart events, restart type, and restart time. Run the **display reboot-info** command to view restart information. You can run the **reset reboot-info** command to clear restart information.

Example

Reset the device reset information.

```
<HUAWEI> reset reboot-info
```

2.8.27 save

Function

The **save** command saves the configurations to the default directory.

Format

save [**all**] [**force**] [*configuration-file*]

Parameters

Parameter	Description	Value
all	Saves all configurations to the next startup configuration file of the system. **NOTE** All configurations are saved, including those of the boards that are not running, no matter whether **all** is specified.	-
force	Forcibly saves configurations.	-
configuration-file	Specifies the name of a configuration file.	The value is a string of case-insensitive characters. The absolute path length ranges from 5 to 64 characters. The value cannot contain spaces and the following characters: < > \ ? , : `. Left and right square brackets cannot be used in pairs. The forward slash (/) and period (.) cannot be used together.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run commands to modify the current configuration of the device, but the modified configuration will be lost after the device restarts. To enable the new configuration to take effect after a restart, save the current configuration in the configuration file before restarting the device.

When a series of configurations are complete and take effect, you must save the current configuration file to the storage device.

- If the *configuration-file* parameter is not specified, the **save** [**all**] command saves the current configuration to the next startup configuration file in the storage device. The "Next startup saved-configuration file:" field displayed in the **display startup** command output indicates the next startup configuration file.

- The **save** [**all**] *configuration-file* command saves the current configuration to the specified directory of the storage device. Generally, the command does not affect the current startup configuration file. Only if the *configuration-file* parameter is the same as the directory and name of the configuration file for the next startup, this command can be used as the same as the **save** command without the *configuration-file* parameter.
- The **save** [**all**] **force** *configuration-file* command saves the current configurations to a file specified by the *configuration-file* parameter on a storage device without user confirmation.

All configurations are saved, no matter whether **all** is specified.

If you do not specify *configuration-file* when saving the configuration file for the first time, the system asks you whether to save the configuration file as **vrpcfg.zip**. The **vrpcfg.zip** file is the default system configuration file with empty configurations in initial state.

Precautions

- If the configuration file to be saved using this command has the same name with the existing configuration file, the existing configuration file is rewritten.
- The configuration file name extension must be .zip or .cfg.
  - .cfg: The file is saved in plain text mode. After the file is specified as the configuration file, all commands in the file are recovered one by one during startup.
  - .zip: The .cfg file is compressed to a .zip file that occupies less space. After being specified as the configuration file, the .zip file is decompressed to the .cfg file and all commands in the .cfg file are recovered one by one during startup.
- When the system is saving configuration files, other users are not allowed to perform configuration. When the current user is performing configuration, other users are not allowed to save configuration files.
- When the controller delivers configurations, the configuration cannot be saved on the device side.
- If you run the **authentication-mode none** command to change the authentication mode of the console port to none authentication, security risks exist. When you save the configuration file, the system displays a message indicating security risks.
- If you run the **undo authentication-mode** command to change the authentication mode of the console port to none authentication, security risks exist. When you save the configuration file, the system displays a message indicating security risks.

Example

Save the current configuration to the default directory when the next startup configuration file is not specified.

```
<HUAWEI> save
The current configuration will be written to the device.
Are you sure to continue?[Y/N]y
Now saving the current configuration to the slot 0.
Save the configuration successfully.
```


Save the current configuration to the next startup configuration file specified.

```
<HUAWEI> save
The current configuration will be written to flash:/vrpcfg.zip.
Are you sure to continue?[Y/N]y
Now saving the current configuration to the slot 0.
Info: Save the configuration successfully.
```

2.8.28 schedule reboot

Function

The **schedule reboot** command configures the scheduled restart of a device and sets the specific time when the device restarts or the delay time before the device restarts.

The **undo schedule reboot** command disables the scheduled restart function.

By default, the scheduled restart is disabled.

Format

schedule reboot { **at** *time* | **delay** *interval* [**force**] }

undo schedule reboot

Parameters

Parameter	Description	Value
at *time*	Specifies the device restart time.	The format of *time* is *hh:mm YYYY/MM/DD*. The restart time must be later than the current device time by less than 720 hours. *YYYY/MM/DD* indicates year, month, and date and is optional. • *hh* indicates hour and the value ranges from 0 to 23. • *mm* indicates minute and the value ranges from 0 to 59. • *YYYY* indicates year and the value ranges from 2000 to 2099. • *MM* indicates month and the value ranges from 1 to 12. • *DD* indicates date and the value ranges from 1 to 31.

Parameter	Description	Value
delay *interval*	Specifies the delay time before the device restarts.	The format of *interval* is *hh:mm* or *mm*. The delay time must be no more than 720 hours. ● In *hh:mm*, *hh* indicates hour and the value ranges from 0 to 720 and *mm* indicates minute and the value ranges from 0 to 59. ● *mm* indicates minute and the value ranges from 0 to 43200.
force	Specifies forcible scheduled restart.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When upgrading or restarting the device, you can configure the device to restart at time when few services are running to minimize the impact on services.

Precautions

- If the **schedule reboot at** command is used to set a specific date (*YYYY/MM/DD*) and the date is a future date, the device restarts at the specified time. If no date is set, two situations occur: If the specified time is later than the current time, the device restarts at the specified time of the day. If the specified time is earlier than the current time, the device restarts at the set time next day.
- Note that the gap between the specified date and current date must be shorter than or equal to 720 hours. If the scheduled restart has been configured, the latest configuration overrides the previous one.
- Run the **schedule reboot delay** *interval* command to set the delay time before the device restarts. If the **force** parameter is not specified, the system compares the configuration file with the current configuration. If the current configuration is different from the configuration file, the system asks you whether to save the current configuration. After you complete the selection, the system prompts you to confirm the configured restart time. Enter **Y** or **y** to make the configured restart time take effect. If the **force** parameter is specified, the system does not display any message, and the restart time takes effect directly. The current configuration is not compared or saved.
- The scheduled restart function becomes invalid when you use the **clock datetime** command to set the system time to over 10 minutes later than the

restart time set by the **schedule reboot** command. If the time difference is equal to or less than ten minutes, the device immediately restarts and does not save the configuration.

- This command restarts the device at the specified time, interrupting all services on the device. Therefore, do not use this command when the device is running properly.
- Before restarting the device, ensure that the configuration file has been saved.

Example

Configure the device to restart at 22:00.

```
<HUAWEI> schedule reboot at 22:00
Info: The system is now comparing the configuration, please wait.
Warning: The configuration has been modified, and it will be saved to the next startup saved-configuration
file flash:/vrpcfg.zip. C
ontinue? [Y/N]:y
Now saving the current configuration to the slot 0...
Save the configuration successfully.
Info: Reboot system at 22:00:00 2012/06/12 UTC-05:13(in 2 hours and 0 minutes)
confirm?[Y/N]:y
```

2.8.29 set factory-configuration operate-mode

Function

The **set factory-configuration operate-mode** command determines whether to reserve or delete the existing configuration when restoring the factory configuration.

The **undo set factory-configuration operate-mode** command enables the device to reserve the existing configuration when you restore the factory configuration.

By default, the system reserves the previous configuration when restoring the factory configuration.

NOTE

Only SS1720GW-E, and S1720GWR-E support this command.

Format

set factory-configuration operate-mode { **reserve-configuration** | **delete-configuration** }

undo set factory-configuration operate-mode

Parameters

Parameter	Description	Value
reserve-configuration	Reserves current configuration file after factory settings are restored.	-

Parameter	Description	Value
delete-configuration	Deletes current configuration file after factory settings are restored.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Run the **set factory-configuration operate-mode delete-configuration** command to specify the operation as **delete-configuration** for restoring factory settings. This prevents user information leak when the device is lost.

Example

Set the mode of restoring the factory configuration to **delete**.

```
<HUAWEI> system-view
[HUAWEI] set factory-configuration operate-mode delete-configuration
Warning: It may delete your configuration file when executing factory configuration, continue?[Y/N]:y
```

2.8.30 set save-configuration

Function

The **set save-configuration** command enables the function of saving system configurations periodically.

The **undo set save-configuration** command disables the function of saving system configurations periodically.

By default, the system does not periodically save configurations.

Format

set save-configuration [**interval** *interval* | **cpu-limit** *cpu-usage* | **delay** *delay-interval*] *

undo set save-configuration [**interval** | **cpu-limit** | **delay**] *

undo set save-configuration [**interval** *interval* | **cpu-limit** *cpu-usage* | **delay** *delay-interval*] *

Parameters

Parameter	Description	Value
interval *interval*	Specifies the interval for saving configurations.	The value is an integer that ranges from 30 to 43200, in minutes. The default value is 30.
cpu-limit *cpu-usage*	Specifies the threshold of the CPU usage during the periodic save operation.	The value is an integer that ranges from 1 to 60. The default value is 50.
delay *delay-interval*	Specifies the delay in automatic backup after the configuration changes. **NOTE** If a configuration change occurs within the configured delay time, the device restarts the timer.	The value is an integer that ranges from 1 to 60, in minutes. The default value is five minutes. The value of *delay-interval* must be less than the value of *interval*.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After this command enables the function of saving system configurations periodically, the configuration file will not be lost if the device is powered off or restarts.

If the **set save-configuration** command is not executed, the system does not enable the function of saving system configurations periodically.

If the **set save-configuration** command is executed, the system compares the configuration files before saving configurations. If the configurations do not change, the system does not save the configurations.

- You can specify **interval** *interval* to set the interval for periodically saving configurations. The system saves the current configurations only when the configurations have been changed and are not saved. The default interval is 0 seconds, indicating that the system does not save the configurations. After the automatic save function is enabled, the default interval is 30 minutes if *interval* is not specified.
- If **cpu-limit** *cpu-usage* is specified, the automatic save function does not affect system performance. After the automatic save timer is triggered, the system cancels the current automatic save operation if the system CPU usage

is detected to be higher than the upper limit. The default upper limit of the CPU usage is 50% for the automatic save function.

- After **delay** *delay-interval* is specified, the system saves the changed configurations after the specified delay. The default value is 5 minutes.

The **undo set save-configuration** command disables the automatic save function. The **undo set save-configuration** command with a parameter specified restores the default value of the parameter and the automatic save function still takes effect.

Follow-up Procedure

Run the **display saved-configuration configuration** command to check the configurations about the periodic save function.

Precautions

Before saving configurations, the system compares the configurations with those in the configuration file. Automatic saving of configurations is triggered in the following scenarios:

- The configurations are inconsistent with those saved last time.
- The configurations are the same as those saved last time, but changes have been made. For example, if a command is run and then its configurations are deleted, automatic saving of configurations will still be triggered although configurations are the same as those saved last time.

After the automatic save function is enabled, the configurations are saved in the configuration file for the next startup. The content in the configuration file changes when the configuration changes. The system cancels the automatic save operation when:

- Content is being written into the configuration file.
- The configurations are being recovered.
- The CPU usage is excessively high.

Example

Set the automatic save interval to 60 minutes.

```
<HUAWEI> system-view
[HUAWEI] set save-configuration interval 60
```

Configure the system to save the new configuration 3 minutes after the configuration changes at an interval of 10 hours when the upper limit of the CPU usage is 60%.

```
<HUAWEI> system-view
[HUAWEI] set save-configuration interval 600 delay 3 cpu-limit 60
```

2.8.31 set save-configuration backup-to-server server

Function

The **set save-configuration backup-to-server server** command specifies the server where the system periodically saves the configuration file.

The **undo set save-configuration backup-to-server server** command cancels the server where the system periodically saves the configuration file.

By default, the system does not periodically save configurations to the server.

Format

set save-configuration backup-to-server server *server-ip* [**vpn-instance** *vpn-instance-name*] **transport-type** { **ftp** | **sftp** } [**port** *port-number*] **user** *user-name* **password** *password* [**path** *path*]

set save-configuration backup-to-server server *server-ip* [**vpn-instance** *vpn-instance-name*] **transport-type tftp** [**path** *path*]

undo set save-configuration backup-to-server server [*server-ip* [**vpn-instance** *vpn-instance-name*]]

Parameters

Parameter	Description	Value
server *server-ip*	Specifies the IP address of the server where the system periodically saves the configuration file.	-
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance.	The value must be an existing VPN instance name.
port *port-number*	Specifies the port number of a server.	The value is an integer ranging from 1 to 65535. By default, the port number of the FTP server is 21, and that of the SFTP server is 22.
transport-type	Specifies the mode in which the configuration file is transmitted to the server.	The value can be **ftp**, **sftp**, or **tftp**. To ensure file transfer security, use the SFTP method.
user *user-name*	Specifies the name of the user who saves the configuration file on the server.	The value is a string of 1 to 64 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
password *password*	Specifies the password of the user who saves the configuration file on the server.	The value is a case-sensitive string without spaces. The value of a simple text password is a string of 1 to 16 characters. The value of a ciphertext password is a string of 24, 32 or 48 characters. When double quotation marks are used around the string, spaces are allowed in the string.
path *path*	Specifies the relative save path on the server. If this parameter is not specified, the FTP, SFTP, or TFTP root path is enabled by default.	The value is a string of 1 to 64 case-sensitive characters without spaces. The path should use forward slashes. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Run this command to periodically save the configuration file to the server.

Before periodically saving configurations, the system compares the configuration files. If the configurations do not change, the system does not periodically save them.

Precautions

If the specified path on the server does not exist, configuration files cannot be sent to the server. The system then sends an alarm message indicating the transmission failure to the NMS, and the transmission failure is recorded as a log message on the device.

The user name and password must be the same as those used in FTP or SFTP login mode.

NOTE

- When you run this command to save configuration files to a server, the system supports only the binary transmission mode. Therefore, the server must support the binary transmission mode.
- Before running this command, run the **set save-configuration** command to start the periodic configuration saving function. Otherwise, configuration files are not saved to the server.
- FTP or TFTP is insecure. Therefore, configuring SFTP is recommended.
- A server IP address can be bound to multiple VPN instances. To delete the configurations of a specified VPN instance, you must set *vpn-instance-name*. Otherwise, configurations irrelevant to the VPN instance will be deleted.
- The configuration file saved by running this command is named in the format of yyyy-mm-dd.hh-mm-ss.sysname.zip, where yyyy indicates the year, the first mm indicates the month, dd indicates the day, hh indicates the hour, the second mm indicates the minute, ss indicates the second, and sysname indicates the host name, for example, **2022-07-02.17-23-17.HUAWEI.zip**.

Example

Specify the server to which the system periodically sends the configuration file, and set the transmission mode to SFTP.

```
<HUAWEI> system-view
[HUAWEI] set save-configuration backup-to-server server 10.1.1.1 transport-type sftp user admin1234 password Helloworld@6789
```

Specify the server to which the system periodically sends the configuration file, and set the transmission mode to SFTP, port number to 88, and save path to **d:/sftp**.

```
<HUAWEI> system-view
[HUAWEI] set save-configuration backup-to-server server 10.1.1.1 transport-type sftp port 88 user admin1234 password Helloworld@6789 path d:/sftp
```

2.8.32 startup saved-configuration

Function

The **startup saved-configuration** command specifies the system configuration file for next startup.

The **undo startup saved-configuration** command deletes the system configuration for next startup.

Format

startup saved-configuration *configuration-file* [**slot** *slot-id*]

undo startup saved-configuration

NOTE

Devices that do not support the stack function or do not have the stack function enabled do not support the **slot** *slot-id* parameters.

Parameters

Parameter	Description	Value
configuration-file	Specifies the name of a configuration file. Make sure that the file exists.	The value is a string of 5 to 64 case-insensitive characters without spaces. The file name extension can be .zip or .cfg. The file name must not contain %.
slot *slot-id*	Specifies a member device in a stack.	The value is an integer. The range of the integer is dependent on the specific device.

Views

startup saved-configuration: User view

undo startup saved-configuration: System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the original configuration file cannot be used due to the software upgrade, run the **startup saved-configuration** command to specify another configuration file for next startup. The startup configuration file must be saved in the root directory of the storage device.

Follow-up Procedure

Run the **reboot** or the **schedule reboot** command to restart the device.

Precautions

- The configuration file specified for the next startup must exist.
- The configuration file name extension must be .zip or .cfg.
  - A configuration file with the file name extension .cfg is a text file, and you can view the file content in the text file. After the file is specified as the configuration file for next startup, the system restores all commands in the file one by one during a startup.
  - A .cfg file is compressed to a .zip file that occupies less space. After being specified as the configuration file, the .zip file is decompressed to the .cfg file and the system restores all commands in the .cfg file one by one during startup.
- If the EasyDeploy function is configured, run the **undo startup saved-configuration** command to clear the configuration file for next startup and delete all the configuration files in the storage device. When the device

restarts, it finds no configuration file available and downloads a configuration file from the file server.

If the EasyDeploy function is not configured, run the **undo startup saved-configuration** command to clear the configuration file for next startup. After the command is run, the device uses empty configuration in next startup.

- The **display cli command-tree** command output shows that the **chassis** parameter is registered on the device. Fixed devices do not support this parameter.
- Do not change the configuration file manually and specify the configuration file for next startup. Otherwise, the device may not start normally.
- Users at level 3 or higher can change the configuration file used for the next startup.
- If the configuration file used for the next startup contains the **authentication-mode none** command that changes the authentication mode of the console port to none authentication, security risks exist. When you configure the configuration file used for the next startup, the system displays a message indicating security risks.
- If the configuration file used for the next startup contains the **undo authentication-mode** command that changes the authentication mode of the console port to none authentication, security risks exist. When you configure the configuration file used for the next startup, the system displays a message indicating security risks.

Example

Cancel the specified configuration file for next startup in the system view.

```
<HUAWEI> system-view
[HUAWEI] undo startup saved-configuration
```

Specify the system configuration file for the next startup.

```
<HUAWEI> startup saved-configuration vrpcfg.cfg
Info: Succeeded in setting the configuration for booting system.
```

2.8.33 startup system-software

Function

The **startup system-software** command specifies the system software for next startup.

Format

startup system-software *system-file* [**all** | **slave-board** | **slot** *slot-id*]

NOTE

Devices that do not support the stack function or do not have the stack function enabled do not support the **all**, **slave-board**, or **slot** *slot-id* parameters.

Parameters

Parameter	Description	Value
system-file	Specifies the name of the system software file.	The value is a string of 4 to 64 case-sensitive characters without spaces and %. It is in the format of [*drive-name*] [*file-name*]. If *drive-name* is not specified, the name of the default storage device is used.
all	Specifies all member devices in a stack.	-
slave-board	Specifies the system software for next startup on the slave switch.	-
slot *slot-id*	Specifies a member device in a stack.	The value is an integer. The range of the integer is dependent on the specific device.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In system software upgrade or downgrade, run this command to specify the system software for next startup.

Follow-up Procedure

Run the **reboot** or the **schedule reboot** command to restart the device.

Precautions

- When the **startup system-software** command is run, the system displays a prompt and the current password is cleared only after the user confirms the operation.
- The system software package must use .cc as the file name extension and be saved to the root directory of the storage device.
- When the system software for next startup is configured using the **startup system-software** command, the system checks the system software integrity. If the digital signature of the system software is invalid, the configuration fails. Therefore, ensure the system software validity.

- If the upgrade or downgrade cannot be performed between versions, the system displays a message, prompting you to perform operations as prompted.
- The **display cli command-tree** command output shows that the **chassis** parameter is registered on the device. Fixed devices do not support this parameter.
- During system software upgrade of fixed PoE switches, powered devices (PDs) will be powered off.
- During the downgrade to an earlier version, the system checks whether the software package of the earlier version contains a complete signature file. If the software package does not contain a complete signature file, the system prompts you whether to continue the downgrade. After confirming that the software package is correct, the downgrade does not affect functions. However, you are advised to upgrade to a more secure version.

NOTE

The system file is authenticated when you configure the file name of the system software used in the next startup. Wait for a while.

Table 2-62 lists the possible causes and troubleshooting methods for failures to load the system software package to the device.

Table 2-62 Possible causes and troubleshooting methods for failures to load the system software package

Failure Cause		Troubleshooting Method
CRC check fails.	The system software package is damaged. Please upload again.	Upload the system software package again.
Version check fails.	The %s only supports the system software package of %s and later versions.	Upload the system software package of the version supported by the device.
Signature verification fails.	Software package verification failed. Please upload again.	Upload the system software package again.
The system software package is corrupted.	The system software package is damaged. Please upload again.	Upload the system software package again.
The system software package is not supported on the device.	The system software package does not match the device.	Upload the system software package that matches the device.
The name of the system software package is incorrect.	The system software package does not exist.	Change the name of the system software package and upload the package again.

Failure Cause		Troubleshooting Method
The name of the system software package is too long.	The file name is too long.	Change the name of the system software package and upload the package again.
Stacking is not supported.	The target version does not support CSS card stacking. Disable this stacking function and try later.	Disable the stacking function and upload the system software package again.
The system software package does not match the MPU.	The system software package does not include the MPU software package.	Upload the system software package that matches the MPU.
Failed to set the system software package.	Failed in setting the software for booting system.	Check whether the system software package matches the device type.
The directory where the system software package is uploaded is incorrect.	The file flash:/%.cc doesn't exist in the main board. (Default directory is flash:/)	Upload the system software package to the root directory of the flash memory.
The flash version does not support the system software package to be uploaded.	The flash chip version xxx does not support the new startup system software package. This file cannot be specified as the startup system software package.	Upload the system software package of the version supported by the flash.
The PHY version does not support the system software package to be uploaded.	The PHY chip version xxx does not support the new startup system software package. This file cannot be specified as the startup system software package.	Upload the system software package of the version supported by the PHY.
The LSW version does not support the system software package to be uploaded.	The LSW chip version xxx does not support the new startup system software package. This file cannot be specified as the startup system software package.	Upload the system software package of the version supported by the LSW.

Failure Cause		Troubleshooting Method
The hardware version VER.B does not support the new system software package.	The hardware VER.B does not support the startup software package. You need to configure the matching patch first.	Configure the matching patch first. For details, see the reference document or upgrade guide.

Example

Specify the system software to be loaded for next startup.

```
<HUAWEI> startup system-software basicsoft.cc
```

2.8.34 startup patch

Function

The **startup patch** command specifies the patch file for next startup.

Format

startup patch *patch-name* [**slave-board** | **slot** *slot-id*]

NOTE

Devices that do not support the stack function or do not have the stack function enabled do not support the **slave-board** parameters.

Parameters

Parameter	Description	Value
patch-name	Specifies the name of the patch file for next startup.	The value is a string of 5 to 64 case-insensitive characters without spaces. It is in the format of [*drive-name*] [*path*] [*file-name*]. If *drive-name* is not specified, the name of the default storage device is used.
slave-board	Specifies the patch file for next startup on slave switch.	-
slot *slot-id*	Specifies a member device in a stack.	The value is an integer. The range of the integer is dependent on the specific device.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To make the patch file take effect after the device restarts, run this command to specify the patch file for next startup.

Follow-up Procedure

Run the **reboot** or the **schedule reboot** command to restart the device.

Precautions

- A patch file uses .pat as the file name extension and must be saved in the root directory.
- If you use this command to specify another patch for next startup, the previous patch will be overridden.
- After the patch file is specified for next startup, run the **display patch-information** command to view the patch file.
  - If the patch file for next startup is not empty, the device load the patch automatically after next startup.
  - If the patch file for next startup is empty, the device cannot load the patch after next startup.
- After the device restarts, the system loads and runs the patch. If you do not want the system to load the patch file after startup, use either of the following methods to delete the patch file:
  - Run the **patch delete all** command to delete the current patch.
  - Run the **reset patch-configure** [**next-startup**] command to delete the patch file already loaded on the system after startup.
- The **display cli command-tree** command output shows that the **chassis** parameter is registered on the device. Fixed devices do not support this parameter.

Example

Specify the patch file for next startup.

```
<HUAWEI> startup patch patch.pat.....
.....
Info: Succeeded in setting main board resource file for system.
```

2.9 Smart Upgrade Commands

2.9.1 Command Support

All models of S300, S500, S2700, S5700, and S6700 series switches (except the S5731-L and S5731S-L) support Smart Upgrade.

Only the following switch models support Smart AP Upgrade:

S5731-H, S5731S-H, S5732-H, S6730-H, S6730S-H

2.9.2 display smart-upgrade information

Function

The **display smart-upgrade information** command displays details about smart upgrade.

Format

display smart-upgrade information

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After smart upgrade is enabled, you can run the **display smart-upgrade information** command to check network connectivity with the HOUP and check whether a new version of software or patch is available for upgrade.

Precautions

This command triggers information exchange between the switch and HOUP. If this command is used frequently, smart upgrade may be affected.

Example

Display details about smart switch or AP upgrade.

```
<HUAWEI> display smart-upgrade information
Info: Loading the information, please wait .

Configuration:
  URL                  : s.houp.huawei.com
  HTTPS port           : 443
  Bind SSL policy      : houp
```



```
  Verify HTTPS server          : true
Version information:
  Refresh time                 : 2019-01-23 12:24:06
  Check version result         : needUpdate
  Recommended software version : V200R023C00
  Recommended patch version    : V200R020SPH001
  Upgrade description          :
  Firmware and Patch Description in English:1)description:2)CC+SPH

  Software package name        : S5732-H-V200R023C00.cc
  Software package size(B)     : 120101636
  Patch package name           : S5732-H-V200R020SPH001.pat
  Patch package size(B)        : 14910

Upgrade information:
  Upgrade Time                 : 2019-01-23 11:13
  Upgrade status               : success
  Cancellation status          : -
  Software download time       : -
  Software download progress(%): -
  Software download speed(KB/s): -
  Patch download time          : -
  Patch download progress(%)   : -
  Patch download speed(KB/s)   : -
  Last upgrade time            : 2019-01-23 11:13
  Last upgrade result          : success

Local information:
  Device name                  : S5732-H24UM2CC
  ESN                          : 2102351XFR1*********
  Software version             : V200R020C00
  Patch version                : V200R020SPH

Schedule Upgrade Information:
  Download time                : 2020-2-13 20:01:24
  Download triggered           : yes
  Download pre-check result    : succeeded
  Reboot time                  : 2020-2-13 20:01:24
  Reboot triggered             : yes
  Reboot triggered result      : failed
<HUAWEI> display smart-upgrade information
Info: Loading the information, please wait .

Configuration:
  URL                          : s.houp.huawei.com
  HTTPS port                   : 443
  Bind SSL policy              : houp
  Verify HTTPS server          : true
Version information:
  Refresh time                 : 2020-07-23 12:24:06
  Check version result         : needUpdate
  Recommended software version : V200R023C00
  Recommended patch version    : -
  Upgrade description          : -
  Firmware and Patch Description in English: -

  Software package name        : AirEngineX760_V200R023C00.bin
  Software package size(B)     : 120101636
  Patch package name           : xxx.pat
  Patch package size(B)        : 14910

Upgrade information:
  Upgrade Time                 : 2020-01-23 11:13
  Upgrade status               : success
  Cancellation status          : -
  Software download time       : -
  Software download progress(%): -
  Software download speed(KB/s): -
  Patch download time          : -
```



```
  Patch download progress(%)   : -
  Patch download speed(KB/s)   : -
  Last upgrade time            : 2020-01-23 11:13
  Last upgrade result          : success

Local information:
  Device name                  : AirEngine 8760-X1-PRO
  ESN                        : 2102351XFR1*********
  Software version             : V200R019C10
  Patch version                : -

AP information:
  Device Type                  : AirEngine 8760-X1-
PRO

Schedule Upgrade Information:
  Download time                : -
  Download triggered           : no
  Download pre-check result    : -
  Reboot time                  : -
  Reboot triggered             : no
  Reboot triggered result      : -
```

Table 2-63 Description of the **display smart-upgrade information** command output

Item	Description
Configuration	Configuration information.
URL	Configured proxy server.
HTTPS port	HTTPS port number of the proxy server. The default port number is 443.
Bind SSL policy	Name of the bound SSL policy.
Verify HTTPS server	Whether to verify the HTTPS server. ● true: The HTTPS server is verified. ● false: The HTTPS server is not verified.
Version information	Version information.
Refresh time	Time when version information is obtained. Each time the command is run, the time is updated.
Check version result	Version check result. ● needUpdate: An upgrade is required. ● netError: The network is unavailable. ● versionOptimal: The version is optimal.
Recommended software version	Recommended software package version.
Recommended patch version	Recommended patch version.
Upgrade description	Upgrade description.

Item	Description
Firmware and Patch Description in English	Hardware and patch description in English.
Software package name	Software package name.
Software package size(B)	Software package size.
Patch package name	Patch package name.
Patch package size(B)	Patch package size.
Upgrade information	Upgrade information.
Upgrade Time	Upgrade time.
Upgrade status	Upgrade status: • success: The upgrade succeeds. • running: The upgrade is ongoing. • netError: Network error. • serverSpecUpLimit: The server specification reached the upper limit of the connection. • CertOutDate: The certificate has expired. • writeFlashFailed: The system file fails to be saved in the flash memory. • fileCheckFailed: The file verification fails. • upgradeCancelled: The upgrade is canceled. • abnormalReset: The switch is restarted or an active/standby switchover is performed during an upgrade. • fileNotMatch: The file does not match. • systemError: System error. • other: Other status.
Cancellation status	Upgrade cancellation status: • Initial: The initialization is generally performed when the loading starts. • Cancelling: The upgrade is being canceled. • Successful: The upgrade is successfully canceled. • Failed: The upgrade fails to be canceled.

Item	Description
Software download time	Time when the software package is downloaded to a device.
Software download progress(%)	Software package download progress, in percentage.
Software download speed(KB/s)	Software package download rate.
Patch download time	Time when a patch is downloaded to a device.
Patch download progress(%)	Patch download progress, in percentage.
Patch download speed(KB/s)	Patch download rate.
Last upgrade time	Last upgrade time.
Last upgrade result	Last upgrade result.
Local information	Local device information.
Device name	Device name.
ESN	Device ESN.
Software version	Software version.
Patch version	Patch version.
AP information	AP information.
Device Type	AP type.
Schedule Upgrade Information	Scheduled upgrade information.
Download time	Scheduled time when system files will be downloaded.
Download triggered	Whether system file download is triggered: ● yes: System file download is triggered. ● no: System file download is not triggered.
Download pre-check result	Result of the device status pre-check before system files are downloaded: ● failed: The check fails. ● succeeded: The check is successful.
Reboot time	Scheduled time for a reboot following an upgrade.

Item	Description
Reboot triggered	Check whether the reboot following an upgrade is triggered. • yes: The reboot following an upgrade is triggered. • no: The reboot following an upgrade is not triggered.
Reboot triggered result	Result of the device status pre-check before a restart is performed: • failed: The check fails. • succeeded: The check is successful.

2.9.3 smart-upgrade { url | https-port }

Function

The **smart-upgrade** { **url** | **https-port** } command configures the URL and HTTPS port number of a proxy server.

The **undo smart-upgrade** { **url** | **https-port** } command cancels the configured URL and HTTPS port number of a proxy server.

By default, the URL and HTTPS port number of a proxy server for connecting to a device are s.houp.huawei.com and 443, respectively.

Format

smart-upgrade { **url** *host* | **https-port** *https-port* }

undo smart-upgrade { **url** | **https-port** }

Parameters

Parameter	Description	Value
host	Specifies the URL or IP address of a proxy server.	The value is a string of 1 to 127 characters.
https-port	Specifies the HTTPS port number of a proxy server.	The value is an integer ranging from 1 to 65535.

Views

System view

Default Level

3: Management level

Usage Guidelines

When a device resides on an intranet, it cannot directly access the HOUP (s.houp.huawei.com). You can run this command to configure the URL and HTTPS port number of a proxy server, so that the device can access public networks through the proxy server.

When the device resides on a public network, it cannot directly access the HOUP (s.houp.huawei.com). You can run this command to configure s.houp.huawei.cn as the URL for connecting to the public network.

Example

Configure the URL and HTTPS port number of a proxy server.

```
<HUAWEI> system-view
[HUAWEI] smart-upgrade url 10.10.10.20
[HUAWEI] smart-upgrade https-port 10020
```

2.9.4 smart-upgrade download

Function

The **smart-upgrade download** command configures a smart upgrade-enabled switch to download the system file from the HOUP.

Format

smart-upgrade download

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the smart upgrade status of the switch or AP is displayed as **needUpdate**, you can run the **smart-upgrade download** command to configure the switch or AP to download the system file first and then run the **smart-upgrade right-now** command at the right time to implement smart upgrade.

Precautions

Resumable download is supported during system file download for smart upgrade. If the system file fails to be downloaded due to a network exception, run the **smart-upgrade download** command to enable the switch to start downloading the system file from the breakpoint.

During the smart upgrade of an AP, if the upgrade file version of the AP does not match the software version of the switch, the system displays an error message.

Example

Configure a smart upgrade-enabled switch to download the system file from the HOUP.

```
<HUAWEI> system-view
[HUAWEI] smart-upgrade download
Info: Getting version information from houp, please wait ...
Info: If you want to stop the download, please press CTRL + C.
Info: Downloading file basic-soft.cc ...
Info: Current percent is 100%.
Info: 83148260 byte(s) received in 160.618 second(s) 505.54 Kbyte(s)/sec.
Info: Downloading file basic-soft.cc.asc ...
Info: The file already exists, check whether it can be resumed from the breakpoint.
Info: The file content is inconsistent with houp, delete and re-download...
Info: Current percent is 100%.
Info: 490 byte(s) received in 0.228 second(s) 2.10 Kbyte(s)/sec.
Info: Start verifying signature ...
Info: Signature verification passed.
Info: Start set next startup file, please wait...
Info: Set next startup file basic-soft.cc successfully.
```

2.9.5 smart-upgrade enable

Function

The **smart-upgrade enable** command enables smart upgrade.

The **undo smart-upgrade enable** command disables smart upgrade.

By default, smart upgrade is disabled on a switch.

Format

smart-upgrade enable

undo smart-upgrade enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

After the **smart-upgrade enable** command is run on a switch, the switch queries the latest version information from the HOUP every 24 hours.

Prerequisites

An SSL policy has been bound to smart upgrade using the **smart-upgrade ssl-policy** command.

Follow-up Task

After smart upgrade is enabled, perform the following operations according to the actual situation:

- Run the **display smart-upgrade information** command to check details about smart upgrade.
- Run the **smart-upgrade download** command to configure the switch to download the system file from the HOUP.
- Run the **smart-upgrade right-now** command to perform a smart upgrade immediately.

Example

Enable smart upgrade.

```
<HUAWEI> system-view
[HUAWEI] smart-upgrade enable
```

2.9.6 smart-upgrade ap enable

Function

The **smart-upgrade ap enable** command enables smart upgrade for APs.

The **undo smart-upgrade ap enable** command disables smart upgrade for APs.

By default, smart upgrade is disabled for APs.

NOTE

This command is supported only on the following models:
S5731-H, S5731S-H, S5732-H, S6730-H, S6730S-H

Format

smart-upgrade ap enable

undo smart-upgrade ap enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To upgrade APs to the latest version more conveniently, you can deploy the smart upgrade function to implement one-click upgrade. After the **smart-upgrade ap enable** command is run to enable smart upgrade for APs, the switch queries the latest version information from the HOUP every 24 hours.

Prerequisites

Smart upgrade has been enabled using the **smart-upgrade enable** command.

Follow-up Task

After the smart upgrade function is enabled for APs, perform the following operations as required:

- Run the **smart-upgrade download** command to download system files.
- Run the **smart-upgrade right-now** command to perform a smart upgrade immediately.
- Run the **display smart-upgrade information** command to check details about smart upgrade.

Example

Enable smart upgrade for APs.

```
<HUAWEI> system-view
[HUAWEI] smart-upgrade ap enable
```

2.9.7 smart-upgrade right-now

Function

The **smart-upgrade right-now** command performs smart upgrade on a switch immediately.

Format

smart-upgrade right-now

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the smart upgrade status of a switch is displayed as **needUpdate**, you can run the **smart-upgrade right-now** to implement loading of and upgrade to a new software version in one-click mode.

Before this command is run, you can also run the **smart-upgrade download** command to configure the switch to download the system file from the HOUP first and then run the **smart-upgrade right-now** command at the right time to implement smart upgrade. The wait time in this method is shorter than that when the **smart-upgrade right-now** command is run.

Precautions

Switches cannot be added to or removed from a stack during smart upgrade.

Resumable download is supported during system file download for smart upgrade. If the download is interrupted due to a network exception, run the **smart-upgrade right-now** command to enable the switch to continue the download from the breakpoint.

During the smart upgrade of an AP, if the upgrade file version of the AP does not match the software version of the switch, the system displays an error message.

Example

Perform smart upgrade on a switch immediately.

```
<HUAWEI> system-view
[HUAWEI] smart-upgrade right-now
Info: Getting version information from houp, please wait ...
Info: If you want to stop the upgrade, please press CTRL + C.
Info: Downloading file basic-soft.cc ...
Info: The file already exists, check whether it can be resumed from the breakpoint.
Info: Resume from the 15728640 bytes breakpoint.
Info: Current percent is 100%.
Info: 104372996 byte(s) received in 197.329 second(s) 516.53 Kbyte(s)/sec.
Info: Downloading file basic-soft.cc.asc ...
Info: Current percent is 100%.
Info: 490 byte(s) received in 0.201 second(s) 2.38 Kbyte(s)/sec.
Info: Downloading file basic-patch.pat ...
Info: The file already exists, check whether it can be resumed from the breakpoint.
Info: The file size is OK and the content is consistent.
Info: Downloading file basic-patch.pat.asc ...
Info: The file already exists, check whether it can be resumed from the breakpoint.
Info: The file size is OK and the content is consistent.
```



```
Info: Start verifying signature ...
Info: Signature verification passed.
Info: Set next startup patch basic-patch.pat successfully.
Info: Start set next startup file, please wait...
Info: Set next startup file basic-soft.cc successfully.
Info: System will rebooting for upgrade...
```

2.9.8 smart-upgrade ssl-policy

Function

The **smart-upgrade ssl-policy** command binds an SSL policy to smart upgrade.

The **undo smart-upgrade ssl-policy** command unbinds an SSL policy from smart upgrade.

By default, no SSL policy is bound to smart upgrade.

Format

smart-upgrade ssl-policy *policy-name*

undo smart-upgrade ssl-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an SSL policy.	The value is a string of 1 to 23 case-insensitive characters without spaces. The value can contain digits, letters, and underscores (_).

Views

System view

Default Level

3: Management level

Usage Guidelines

Because a switch where smart upgrade is to be enabled is connected to the HOUP using HTTPS, an SSL policy must be bound to smart upgrade for the switch to establish HTTPS connection with the HOUP before smart upgrade is enabled on the switch.

Example

Bind an SSL policy named **houp** to smart upgrade.

```
<HUAWEI> system-view
[HUAWEI] smart-upgrade ssl-policy houp
```


2.9.9 smart-upgrade schedule

Function

The **smart-upgrade schedule** command configures the scheduled smart upgrade function on a switch.

The **undo smart-upgrade schedule** command disables the scheduled smart upgrade function on a switch.

By default, the scheduled smart upgrade function is disabled on a switch.

Format

smart-upgrade schedule download at *download-time* [**reboot at** *reboot-time*]

undo smart-upgrade schedule

Parameters

Parameter	Description	Value
download at *download-time*	Specifies the time when a switch downloads system files.	The format is YYYY-MM-DD HH:MM:SS. • YYYY indicates the year. The value is an integer in the range from 2000 to 2099. • MM indicates the month. The value is an integer in the range from 1 to 12. • DD indicates the day. The value is an integer in the range from 1 to 31. • HH specifies the hour. The value is an integer in the range from 0 to 23. • MM indicates the minute. The value is an integer in the range from 0 to 59. • SS indicates the second. The value is an integer in the range from 0 to 59. **NOTE** The time when a switch downloads system files must be later than the current time of the switch.

Parameter	Description	Value
reboot at *reboot-time*	Specifies the time when a switch restarts after an upgrade.	The format is YYYY-MM-DD HH:MM:SS. ● YYYY indicates the year. The value is an integer in the range from 2000 to 2099. ● MM indicates the month. The value is an integer in the range from 1 to 12. ● DD indicates the day. The value is an integer in the range from 1 to 31. ● HH specifies the hour. The value is an integer in the range from 0 to 23. ● MM indicates the minute. The value is an integer in the range from 0 to 59. ● SS indicates the second. The value is an integer in the range from 0 to 59. **NOTE** ● The time when a switch restarts after an upgrade must be later than the time when the switch downloads system files. ● If you do not specify the time when a switch restarts after an upgrade, the switch only downloads system files. In this case, you need to manually restart the switch to complete the upgrade.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a switch requires a smart upgrade, you can run the **smart-upgrade schedule** command on the switch to configure it to perform a smart upgrade at an off-peak time. This configuration will prevent the upgrade from affecting services running on the switch.

Precautions

- This command takes effect only for smart upgrade of switches instead of APs.
- During a scheduled smart upgrade, if the switch fails to download system files at the scheduled time due to network problems, the switch attempts to download system files again when the scheduled restart time arrives. If the upgrade still fails, the scheduled smart upgrade fails.
- The following operations will disable the scheduled smart upgrade function:

- Resets a switch.
- Run the **undo smart-upgrade enable** command to disable smart upgrade.
- Run the **smart-upgrade download** command to download system files.
- Run the **smart-upgrade right-now** command to perform a smart upgrade immediately.
- Download system files immediately through the web system.
- Perform a smart upgrade immediately through the web system.

Example

Configure the scheduled smart upgrade function.

```
<HUAWEI> system-view
[HUAWEI] smart-upgrade schedule download at 2020-12-01 00:00:00
```

2.9.10 smart-upgrade verify-server disable

Function

The **smart-upgrade verify-server disable** command disables the server certificate verification function before a switch is connected to a proxy server for smart upgrade.

The **undo smart-upgrade verify-server disable** command enables the server certificate verification function before a switch is connected to a proxy server for smart upgrade.

By default, the server certificate verification function is enabled before a switch is connected to a proxy server for smart upgrade.

Format

smart-upgrade verify-server disable

undo smart-upgrade verify-server disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

When the certificate for smart upgrade is invalid or no certificate for smart upgrade is available, you can run the **smart-upgrade verify-server disable** command to temporarily disable the certificate verification function.

Although the certificate verification function is manually disabled, an SSL policy still needs to be bound to smart upgrade. Therefore, after the certificate verification function is disabled, run the **ssl policy** *policy-name* command to create an empty SSL policy and run the **smart-upgrade ssl-policy** command to bind the SSL policy to smart upgrade.

Example

Disable the function of verifying the HTTPS certificate of the server.

```
<HUAWEI> system-view
[HUAWEI] smart-upgrade verify-server disable
```

2.9.11 smart-upgrade web-prompt disable

Function

The **smart-upgrade web-prompt disable** command disables web prompt for smart upgrade.

The **undo smart-upgrade web-prompt disable** command enables web prompt for smart upgrade.

By default, web prompt for smart upgrade is enabled.

Format

smart-upgrade web-prompt disable

undo smart-upgrade web-prompt disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

By default, when smart upgrade is disabled on a switch, the web system prompts the user that this function is disabled. After smart upgrade is enabled on the switch and a new software version is available, the web system prompts the user

to upgrade the switch to the new version. If such information is not required, you can run this command to disable web prompt for smart upgrade.

Example

Disable web prompt for smart upgrade.

```
<HUAWEI> system-view
[HUAWEI] smart-upgrade web-prompt disable
```

2.10 Upgrade Commands

2.10.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models (except the S5731-L and S5731S-L), unless otherwise specified. For details, see specific commands.

2.10.2 check startup

Function

The **check startup** command checks the correctness of various resource files, including the PAF file, the patch package, the startup software, and the configuration file.

Format

check startup [**crc**] [**next**]

Parameters

Parameter	Description	Value
crc	Performs a CRC check on various resource files.	-
next	Checks various resource files used for next startup.	-

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

After configuring the resource files for next startup, you can run this command to check whether the resource files are complete and whether the formats and versions of the resource files are correct.

Example

Check the correctness of the resource files.

```
<HUAWEI> check startup
Main board:
Check startup software.....ok
Check configuration file.....ok
Check PAF.....ok
Check Patch.....ok
PAF is fitted with startup software
Info: Slave board is not existing.
```

Performs a CRC check on various resource files.

```
<HUAWEI> check startup crc
Warning: This operation will take several minutes! Continue?[Y/N]:y
Check startup software CRC.....
ok
Info: Slave board is not existing.
```

2.10.3 display device group-speed license-usage

Function

The **display device group-speed license-usage** command displays the usage of license control items.

NOTE

This command takes effect only on the following devices that have license control items loaded:

S5732-H24UM2CC, S5732-H48UM2CC, and S5736-S24UM4XC

Format

display device group-speed license-usage

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the usage of license control items, run the **display device group-speed license-usage** command.

For details about license control items, see **License Control Items**.

Example

Display the usage of license control items.

```
<HUAWEI> display device group-speed license-usage
Slot LicenseItem       ResourceCount ResourceUsed
-----------------------------------------------------
 0   1G->2.5G          4             0
     1G->5G            4             0
     1G->10G           4             3
     2.5G->5G          1             0
     2.5G->10G         1             0
     5G->10G           1             0
```

Table 2-64 Description of the **display device group-speed license-usage** command output

Item	Description
Slot	Slot ID.
LicenseItem	Control item name.
ResourceCount	Number of control Items.
ResourceUsed	Number of used control items.

2.10.4 display last startup information

Function

The **display last startup information** command displays the version of the system software used for the last startup.

Format

display last startup information slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the version of the system software used for the last startup in the MPU slot.	The value must be set according to the device configuration.

Views

All view

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display last startup information** command to check the version of the system software used for the last startup.

Precautions

- If the device is upgraded from V200R020C10SPC100 or an earlier version to V200R020C10SPC500 or a later version, because the source version does not support this command, the system displays a message "Info: The file that records information about the last startup system software is empty." after this command is executed.
- If the device version is V200R020C10SPC500 or later and the system software remains unchanged, the system displays a message "Info: The file that records information about the last startup system software is empty." after this command is executed.

Example

Display the version of the system software used for the last startup.

```
<HUAWEI> system-view
[HUAWEI] display last startup information slot 0
Startup system software : flash:/basicsoft.cc
Software version       : V200R021C01SPC100B236
Software compile time  : Oct 30 2021, 19:32:02
```

2.10.5 display license

Function

The **display license** command displays information about the license file in the system.

NOTE

This command takes effect only on the device that loads the license control item.

Format

display license [*file-name* | **verbose**]

Parameters

Parameter	Description	Value
file-name	Displays summary information about the license file with a specified file name. *file-name* supports file name association. The disk where the file resides can be automatically associated. ● Full help: All the disks of the device can be associated and displayed. ● Partial help: The related disk and file can be associated and displayed after you enter a specified character string.	The value is a string of 5 to 64 case-insensitive characters without spaces.
verbose	Displays detailed information about the current active license file.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

A license file dynamically controls the availability of some features. Only one license file is active in the system. Run this command to view detailed information about the active license in the system, including license file name, version, validity period, and control item. Based on the information, you can determine whether to upgrade the system version to support more features.

Precautions

The license of an N1 software package is activated on iMaster NCE-Campus. Therefore, you cannot view the license control items of the N1 software package by running this command on the device.

On the S5732-H24UM2CC, S5732-H48UM2CC, and S5736-S24UM4XC, if these devices set up a stack and the master and non-master devices have inconsistent license control items, run the **display device group-speed license-usage** command to check the usage of license control items in the stack.

Example

Display information about the active license file of the device.

```
<HUAWEI> display license
 Active license    : flash:/LICORTF163673-554BEF51E8.dat
```



```
License state     : Trial
Revoke ticket     : No ticket

RD of Huawei Technologies Co., Ltd.

Product name      : S5700
Product version   : V200R0012
License Serial No : LIC20210401UV9K50
Creator           : Huawei Technologies Co., Ltd.
Created Time      : 2021-04-01 21:22:06
Sns End Data      : 2021-07-01
Feature name      : EHFEA1
Authorize type    : DEMO
Expired date      : PERMANENT
Trial days        : 60

Item name          Item type  Value    Description
-------------------------------------------------------------
ES5SF4512K00       Resource   2        FIB512K
ES5SF4128K00       Resource   6        FIB128K
ES5SWL16AP00       Resource   64       WL16AP
ES5SWL64AP00       Resource   16       WL64AP
ES5SWL128AP0       Resource   8        WL128AP
ES5SWL512AP0       Resource   2        WL512AP

 Master board license state: Trial. The trial days remains 60 days. Apply for authentic license before the
current license expires.
```

Table 2-65 Description of the **display license** command output

Item	Description
Active license	Name and path of the active license file.

Item	Description
License state	Status of a license file: ● Normal This state value indicates that a license file is working properly. If the status of the license file on the live network is not **Normal**, check the license file. ● Trial – A license file enters the Trial state if the ESN does not match the device. A license file in Trial state can be used only for 60 days. To continue to use a license file after the Trial state, apply for a new license file using the correct ESN. – A temporary license file expires and enters the Trial state. To continue to use a license file after the Trial state, apply for a new license file and activate it. – A license file is revoked and enters the Trial state. To continue to use a license file after the Trial state, apply for a new license file based on the revocation code and activate it. ● Demo When you activate a temporary license file, it enters the Demo state. The Demo state exists only for a demo license file used for test and deployment. A license file in Demo state allows you to use normal functions within a specified period. Before the expiration of the license file in Demo state, replace it with a commercial license file. ● Emergency In emergency conditions like earthquakes, volcano explosions, and tsunamis, run the **license emergency** command to trigger a license file to enter the emergency

Item	Description
	state. The emergency state stays for seven days, and a license file can enter the emergency state three times. ● Default: No license file is activated or a license file expires. If a license file enters the Default state, services will be interrupted. If you want to use services after a license file expires or becomes invalid, apply for a new license file and activate it.
Revoke ticket	License revocation code. **no ticket** indicates that the license is permanently valid.
Product name	Name of the product that runs the license.
Product version	Product version.
License Serial No	Serial number of the license file.
Creator	Creator of the file.
Created Time	Time when the file was created.
Sns End Data	SnS end date in the N1 business model. Only the following models support this field: ● S5700 series: S300, S500, S5720-LI, S5720-SI, S5720-HI, S5720-EI, S5720I-SI, S5730-SI, S5730-HI, S5731-S, S5731-H, , S5732-H, S5735-L, S5735-L-I, S5735-L1, S5735-S, S5735-S-I, S5736-S ● S6700 series: S6720-LI, S6720-SI, S6735-S, S6720-EI, S6720-HI, S6730-S, S6730-H,
Feature name	Feature name.
Authorize type	Authorization type. ● demo: trial authorization. ● comm: commercial authorization.

Item	Description
Expired date	License expiration date. **PERMANENT** indicates that the license is permanently valid. A license file enters the trial period after it expires. This does not affect services. When the trial period expires, a license file will be invalid. The services and functions under its control revert to the default values. **NOTE** You need to apply for a new license file and activate it during the trial period. After activation, the new license file replaces the one in the trial period automatically.
Trial days	Trial period of an expired license. • For a license file in the trail state, the trial period is 60 days. The value of this field is displayed as 60. • For a license file that is not in the trail state, this field is meaningless, and its value is displayed as **--**.
Item name	Name of a control item.
Item type	Type of a control item. • Function: function items controlled by a license file • Resource: resource items controlled by a license file
Value	Value of a control item. • When **Item type** displays **Function**, **Value** displays **Yes**, indicating that this function is enabled. • When **Item type** displays **Resource**, **Value** displays a specified value, indicating the maximum number of this resource item. **NOTE** This parameter is displayed in the **display license** command output.
Control value	Values supported by a control item. **NOTE** This parameter is displayed in the **display license verbose** command output.

Item	Description
Used value	Actual used value. **NOTE** This parameter is displayed in the **display license verbose** command output.
Description	Description of a control item.

2.10.6 display license esn

Function

The **display license esn** command displays the equipment serial number (ESN) used for applying a license.

NOTE

This command takes effect only on the device that loads the license control item.

Format

display license esn

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you need to use licensed resource items or function items, apply for a license file. When applying for a license, you need to provide the device ESN.

ESN is the only identifier of device components, run the **display license esn** command to display the ESN of the current device, and then use the ESN to apply a license file for the device.

The ESN of the chassis must be the same as the ESN in the license to be activated. If they are different, the license file cannot be activated.

Example

Display the ESN used for applying a license.

```
<HUAWEI> display license esn
```



```
ESN: 2102113090P0xxxxxxxx
```

Table 2-66 Description of the **display license esn** command output

Item	Description
ESN	ESN of the device.

2.10.7 display license information

Function

The **display license information** command displays license information about the master, standby, and slave switches in a stack system.

NOTE

This command takes effect only on the device that loads the license control item.

Format

display license information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

- If the control items of the license files on the standby/slave and master switches are the same, the standby/slave switch uses its own license file and does not synchronize the license file of the master switch. You can run the **display license** command to check the license control items. An active/standby switchover has no impact on the license files loaded on the master, standby, and slave switches.
- If the control items of the license files on the standby/slave and master switches are different, the standby/slave switch synchronizes the license file of the master switch. The ESN in the synchronized license file will differ from the standby/slave switch's ESN. If so, the license changes to the Trial state and enters the trial period. After an active/standby switchover, the license on the new master switch enters the trial period. You can run the **display license**

information command on the master switch to check whether the switch's ESN is the same as the ESN in the license file.

Precautions

The **display license** command displays license information about the master switch only, whereas the **display license information** command displays license information about the master, standby, and slave switches in the stack system.

If a switch is not in a stack system, the **display license information** command displays license information about the switch only. If a stack system contains the master, standby, and slave switches, the **display license information** command displays license information about the master, standby, and slave switches.

Follow-up Procedure

If the ESN of the standby/slave switch differs from the ESN in the synchronized license file, the license enters the trial period. Apply for a new license file before the trial period expires according to the following process.

1. Run the **license revoke** command on the master switch to obtain the revocation code of the license file on the switch.
2. Run the **display esn** command on the master switch to collect ESNs of the master, standby, and slave switches.
3. Log in to license application website, and use the revocation code and ESNs of the master, standby, and slave switches to apply for a new license file for the stack system.
4. Run the **license active** *license-name* command on the master switch to activate the new license file.

Example

Display license information about the master, standby, and slave switches in a stack system.

```
<HUAWEI> display license information

Slot 0:
Current license file          : flash:/s5720-hi_slot0_full.datSynchronize from master board  : NO
Current license file esn      : 210235859810xxxxxxxx
Current slot esn              : 210235859810xxxxxxxx
License esn match with device  : YES

Slot 1:
Current license file          : flash:/s5720-hi_slot2_full.dat
Synchronize from master board  : YES
Current license file esn      : 210235859810xxxxxxxx
Current slot esn              : 210235859810xxxxxxxx
License esn match with device  : NO

Slot 2:
Current license file          : flash:/s5720-hi_slot2_full.dat
Synchronize from master board  : YES
Current license file esn      : 210235859810xxxxxxxx
Current slot esn              : 210235859810xxxxxxxx
License esn match with device  : YES
```


Table 2-67 Description of the **display license information** command output

Item	Description
Slot	Slot ID.
Current license file	Current license file.
Synchronize from master board	Whether the license file is synchronized from the master switch. For the master switch, the value is YES.
Current license file esn	ESN in the current license file.
Current slot esn	ESN of the switch.
License esn match with device	Whether the ESN in the license file matches the switch's ESN.

2.10.8 display license resource usage

Function

The **display license resource usage** command displays the usage of the resource items defined in a license file.

NOTE

This command takes effect only on the device that loads the license control item.

Format

display license resource usage

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the **display license resource usage** command to check the usage of the resource items defined in the license file, including the number of remaining licenses and the resource usage.

Resource usage refers to the percentage of resources used out of resources defined by the license file. For details about license control items, see **License Control Items**.

Example

Display the usage of licensed resources.

```
<HUAWEI> display license resource usage
Info: Active License on master board: flash:/LICORTF163673-554BEF51E8.dat
 FeatureName    | ConfigureItemName      | ResourceUsage

 ES5FEA1        ES5SF4512K00            0/2
 ES5FEA1        ES5SF4128K00            0/6
 ES5FEA1        ES5SWL16AP00             0/64
 ES5FEA1        ES5SWL64AP00             0/16
 ES5FEA1        ES5SWL128AP0             0/8
 ES5FEA1        ES5SWL512AP0             0/2
```

Table 2-68 Description of the display license resource usage command output

Item	Description
Active License on master board	File name and path of an active license name.
FeatureName	Name of the feature controlled by the license.
ConfigureItemName	Name of a control item.
ResourceUsage	Percentage of used resources.

2.10.9 display license revoke-ticket

Function

The **display license revoke-ticket** command displays the revocation code of the current license file of the device.

NOTE

This command takes effect only on the device that loads the license control item.

Format

display license revoke-ticket

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display license revoke-ticket** command enables you to check the revocation code of a license file that has become invalid on the device. This code proves that the current license file is invalid and is used to apply for a new license.

Precautions

This command displays information only when the license file in current device system is invalid. Otherwise, no command output is displayed.

Example

Display the revocation code of the current invalid license file.

```
<HUAWEI> display license revoke-ticket
 Info: The revoke ticket is: LIC20091103006100:27C1B773ED11D9F877855CDAEE74ABFE60E07126.
```

2.10.10 display license state

Function

The **display license state** command displays the license status on the device.

NOTE

This command takes effect only on the device that loads the license control item.

Format

display license state

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check the status of the running license, run this command. The command displays the current status of the license and the number of days before the license in this status will expire.

The system supports the following license states:

- Normal: normal license
- Demo: demonstration license
- Trial: trial license that has expired but is still valid during the trial period
- Emergency: emergency license
- Default: default license

This command helps you locate license problems and verify the license status on the device.

Prerequisites

A license file has been stored on the main control board of the device and has been activated. This ensures that valid entries are displayed after the execution of the command. If the license file is not activated, no command output is displayed.

Example

Display the status of the license on the device.

```
<HUAWEI> display license state
Info: Current license state is Trial. 60 days remain.
```

2.10.11 display module-information

Function

The **display module-information** command displays information about dynamically uploaded modules.

Format

display module-information [**verbose** | **next-startup**]

Parameters

Parameter	Description	Value
verbose	Displays detailed information about dynamically uploaded modules.	-
next-startup	Displays information about the module packages to be uploaded at the next startup.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

After modules are uploaded, you can run the **display module-information** command to check information about these modules.

Example

Display information about dynamically uploaded modules.

```
<HUAWEI> display module-information

                      Module Information
--------------------------------------------------------------------------------
Module     Version   InstallTime                 PackageName
--------------------------------------------------------------------------------
MACSEC     SPH       2011-01-16 16:39:18+00:00       s5720hi.mod

Total = 1
```

Display detailed information about dynamically uploaded modules.

```
<HUAWEI> display module-information verbose

                      Module Information
--------------------------------------------------------------------------------
Module     Version   InstallTime                 PackageName
--------------------------------------------------------------------------------
MACSEC     SPH       2011-01-16 16:39:18+00:00       s5720hi.mod

Total = 1
Board Info:

--------------------------------------------------------------------------------
Slot       Module        State     Count Time(YYYY-MM-DD HH:MM:SS)
--------------------------------------------------------------------------------
0          MACSEC        Using     1     2011-01-16 16:39:17+00:00

Total = 1
```

Table 2-69 Description of the **display module-information** command output

Item	Description
Module Information	Module information.
Module	Name of a dynamically uploaded module.
Version	Module package version.
PackageName	Module package name.
InstallTime	Time when the module package was uploaded to the memory.
Total	The **Total** field under **Module Information** displays the number of module packages that take effect. The **Total** field under **Board Info** displays the number of boards that have modules installed.

Item	Description
Board Info	Board information.
Slot	Slot ID of the board where a module resides.
State	Status of the module.
Count	Number of modules that take effect on the board.
Time(YYYY-MM-DD HH:MM:SS)	Time when the module took effect, that is, time when the current module was loaded to the current state.

Display information about the next startup modules configured in the system.

```
<HUAWEI> display module-information next-startup
Info: The result will be shown in several minutes. Please wait for a moment.....

                  Next startup module packages
Total = 1
--------------------------------------------------------------------------
No.  PackageName
--------------------------------------------------------------------------
1    flash:/$_install_mod/s5720hi.mod
```

Table 2-70 Description of the **display module-information next-startup** command output

Item	Description
Next startup module packages	Information about module packages to be installed at the next startup.
Total	Number of module packages to be installed at the next startup.
No.	Sequence number of a module package to be installed at the next startup.
PackageName	Name of a module package to be installed at the next startup.

2.10.12 display paf

Function

The **display paf** command displays information about the product adaptive file (PAF) in the system.

Format

display paf { **all** | { **resource** | **service** } *item-name* }

Parameters

Parameter	Description	Value
all	Displays all information about the PAF file.	-
resource	Specifies the value set for a resource item in the PAF file.	-
service	Specifies the value set for a service item in the PAF file.	-
item-name	Specifies the name of a resource item or a service item.	The value is a string of 1 to 64 characters.

Views

All views

Default Level

3: Management level

Usage Guidelines

A PAF file provides only required resources and features. This command can display all the specification information about the PAF file.

Example

Display the value set for a resource item in the PAF file.

```
<HUAWEI> display paf resource PAF_LCS_NQA_SPECS_NUM_ENTRY
 PAF_LCS_NQA_SPECS_NUM_ENTRY = 1, 32, 32, 0
```

Display the value set for a service item in the PAF file.

```
<HUAWEI> display paf service PAF_LCS_IPV6_BASE_SPECS_ENABLED
 PAF_LCS_IPV6_BASE_SPECS_ENABLED = 1, 1
```

Table 2-71 Description of the display paf resource command output

Item	Description
PAF_LCS_NQA_SPECS_NUM_ENTRY	Resource item name in the PAF file.
1	Whether a resource item is controlled by a license. • 1: yes • 0: no

Item	Description
32	Default value of the resource item in the PAF file.
32	Maximum value of the resource item in the PAF file.
0	Minimum value of the resource item in the PAF file.

Table 2-72 Description of the display paf service command output

Item	Description
PAF_LCS_IPV6_BASE_SPECS_ENABLED	Service item name in the PAF file.
1	Whether a service item is controlled by a license. ● 1: yes ● 0: no
1	Service status. ● 1: enabled ● 0: disabled

2.10.13 display patch-information

Function

The **display patch-information** command displays information about the patch in the current system.

Format

display patch-information [**history**]

Parameters

Parameter	Description	Value
history	Displays historical information about the patch in the current system.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

After a patch is loaded or deleted, run this command to view information about the patch, including its version, name, and status.

Example

Display current information about the patch in the system.

```
<HUAWEI> display patch-information
Patch Package Name   :flash:/patch_pack.pat
Patch Package Version:V200R013SPH
The state of the patch state file is: Running
The current state is: Running

*********************************************************************
*          Information about hot patch errors is as follows:        *
*********************************************************************

   Slot           CurrentVersion
-------------------------------------------------------------

No hot patch error occurs on any board.


*********************************************************************
*              The hot patch information, as follows:               *
*********************************************************************

 Slot      Type          State     Count Time(YYYY-MM-DD HH:MM:SS)
-------------------------------------------------------------------
 3         C             Running   1     2018-12-03 18:34:25+00:00
 4         C             Running   1     2018-12-04 09:51:43+00:00


*********************************************************************
*             The Kernel patch information, as follows:             *
*********************************************************************

   Slot          Type          State         Count
-------------------------------------------------------------
   3             Kernel        Running       1
   4             Kernel        Running       1


*********************************************************************
*            The firmware patch information, as follows:            *
*********************************************************************

   Slot          Type          State         Count
-------------------------------------------------------------
   4             BOOTLOAD      Running       1
```

Display historical information about the patch in the system.

```
<HUAWEI> display patch-information history
*********************************************************************
*              The patch command history, as follows:               *
*********************************************************************

 time(Y.M.D/HH:MM:SS)   state        size     patch-package name
 -------------------------------------------------------------------
```



```
2014.01.29/14:07:39  Startup       827318      patch_all_pack.pat
2014.10.13/11:33:12  Running        8404      patch_all_pack1.pat
2014.10.13/10:48:36     Idle      827318     patch_all_pack2.pat
```

Table 2-73 Description of the display patch-information command output

Item	Description
Patch Package Name	Name of the patch file.
Patch Package Version	Version of the patch.
The state of the patch state file is	Status of the patch file.
The current state is	Current status of the patch.
Slot	Slot ID.
Type	Patch type. ● C: single-core patch. ● BOOTLOAD, CPLD, BOOTROOM, KERNEL, DTB, OSPKG, RAMDISK, FPGA, MCU_POE, or SUBCARD_CPLD: indicates a firmware patch. ● SEFU: multi-core patch type. ● ENP: indicates an ENP patch. (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this patch type.) ● Kernel: indicates a kernel patch. (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this patch type.) ● BIN: indicates a process patch. ● C-WMP: multi-core WMP patch. (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this patch type.) ● C-NAC: multi-core NAC patch. (Only the S5731-H, S5731-S, S5731S-H, S5731S-S, S5732-H, S6730-H, S6730S-H, S6730-S, and S6730S-S support this patch type.)

Item	Description
State	Running status of the patch. • Deactive • Active • Running • Idle: no patch in the system • Startup: indicates the Startup state after the patch to be loaded at the next startup is set. If the next state change is recorded, the current Startup state is overwritten.
Count	Number of patch units. For kernel patches, the number of kernel patches in **Active** and **Running** states is displayed.
Time(YYYY-MM-DD HH:MM:SS)	Time when the patch takes effect.
size	Size of the patch.

2.10.14 display rollback

Function

The **display rollback** { **information** | **result** } command displays rollback information in the system.

Format

display rollback { **information** | **result** }

Parameters

Parameter	Description	Value
information	Displays version information after the system is rolled back.	-
result	Checks whether the rollback is successful.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If an error occurs during an upgrade and you need to cancel the upgrade, run the **rollback** command to roll back the system to the previous version.

- Before performing a rollback, you can run the **display rollback information** command to preview the version status after the rollback, including the system software, configuration file, and patch file used after the rollback, as well as the remaining time for the rollback function to take effect.
- After completing the rollback, you can run the **display rollback result** command to check whether the rollback is successful.

Example

Display rollback information in the system.

```
<HUAWEI> display rollback information
------------------------------------------------------------------------
MainBoard:
 Software package:        flash:/basicsoft.cc
 Configuration file:      flash:/vrpcfg201506011523.zip
 Patch file:              NULL
 Rollback remain time:    00:16:49
------------------------------------------------------------------------
```

Table 2-74 Description of the **display rollback information** command output

Item	Description
Software package	System software used after the rollback.
Configuration file	Configuration file used after the rollback. This configuration file is the backup configuration file automatically generated by the system after the upgrade. The file name is in the format of **filenameYYYYMMDDhhmm.zip**. ● **filename**: indicates the name of the configuration file before the upgrade. ● **YYYY**: indicates the year. ● **MM**: indicates the month. ● **DD**: indicates the day. ● **hh**: indicates the hour. ● **mm**: indicates the minute. If the file name is too long, the system automatically shortens the file name length to the required length.

Item	Description
Patch file	Patch file used after the rollback.
Rollback remain time	Remaining time for the rollback function to take effect.

Check whether the rollback is successful after the rollback is complete.

```
<HUAWEI> display rollback result
Rollback result: Success.
```

Table 2-75 Description of the **display rollback result** command output

Item	Description
Rollback result	Rollback result: • Success: The rollback is successful. • Fail: The rollback fails. If the rollback fails, the system displays specific rollback failure information: – Software rollback fail: The system software fails to be rolled back. – Configuration rollback fail: The configuration file fails to be rolled back. – Patch rollback fail: The patch file fails to be rolled back.

2.10.15 display virtual license

Function

The **display virtual license** command displays information about the virtual license file in the current system.

Format

display virtual license [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	• Specifies the slot ID if stacking is not configured. • Specifies the stack ID if stacking is configured.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The controller delivers a virtual license to perform management. You do not need to load the entity license for the switch. This facilitates the management and control of the functions related to the entity license.

You can run this command to check detailed information about the virtual license file in the current system, including the name of the virtual control item, status of the virtual license, and expiration date of the virtual license.

Example

Display information about the virtual license file on the device.

```
<HUAWEI> display virtual license

Slot 0
-------------------------------------------------------------------------------
Item       Resource  License     Expired     Trial days  Item
Name       Value     Status      Date        Total       Description
-------------------------------------------------------------------------------
VXLAN      1         Demo        2019-08-16  -           VXLAN Control Function
```

Table 2-76 Description of the **display virtual license** command output

Item	Description
Slot	• Specifies the slot ID if stacking is not configured. • Specifies the stack ID if stacking is configured.

Item	Description
Item Name	Name of a control item in the virtual license. VXLAN: Control over the enhanced VXLAN functions. The enhanced VXLAN functions include the distributed VXLAN gateway function and the BGP EVPN function. **NOTE** The license does not control route exchange between devices, but controls the status of the dynamic VXLAN tunnel established using BGP EVPN. If no license is loaded or the license becomes invalid, the dynamic VXLAN tunnel cannot be established using BGP EVPN.
Resource Value	Resource value of the control item.
License Status	Status of the virtual license. ● Default: By default, no virtual license is installed on a device and the dynamic VXLAN tunnel is in Down status. ● Normal: The commercial virtual license is activated. The device status is changed to Normal after the controller delivers a commercial virtual license to the device. The status can be restored to Default only through online retrieving. ● Demo: The temporary virtual license is activated. The device status is changed to Demo after the controller delivers a temporary virtual license to the device. The status can be restored to Default through online retrieving, and trial keepalive. ● Trial: The license is in keepalive status, indicating that the device status is automatically changed to trial keepalive after the validity period for the device in Demo status expires. The keepalive period is 90 days. After the keepalive period expires, the status is restored to Default and the dynamic VXLAN tunnel is in Down status.
Expired Date	Expiration date of the virtual license.
Trial days Total	Total trial period of the virtual license.
Item Description	Description of a control item in the virtual license.

2.10.16 install-module

Function

The **install-module** command installs module packages.

By default, no module package is installed.

Format

install-module *file-name* [**next-startup**]

Parameters

Parameter	Description	Value
file-name	Specifies the name of a module package to be installed. *file-name* supports file name association. The related file can be associated and displayed after you enter a specified character string.	The value is a string of 5 to 64 case-insensitive characters without spaces.
next-startup	Specifies the name of the module package to be installed during next startup.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Software upgrade is a common method to add new services on a network. This method, however, is complex and affects services. To solve these problems, you can run the **install-module** command to install the module package of a desired function, without upgrading or powering off your device.

- Run the **install-module** *file-name* command to load a module in the module package to the device. The module directly takes effect after being loaded. If the device is in a stack, the module is loaded to all the devices in the stack, including the master, standby, and slave switches.
- Run the **install-module** *file-name* **next-startup** command to add the module package to the next startup module list. The device automatically loads the module next time it starts. Before a module package is installed dynamically, the system checks the module package validity. In the next startup module list, one module can exist in only one module package.

Precautions

- The file name extension of the module package must be .MOD, and the file must be saved in the directory **$_install_mod** on the device.
- The module package version must match the current system software version. Otherwise, the module package will fail to be installed.

- The system allows you to install up to 16 modules.

Example

Load the module package s5720hi.mod.

```
<HUAWEI> install-module s5720hi.mod
Info: Installing the module flash:/$_install_mod/s5720hi.mod..
.
Info: Succeeded in installing the module on the master board....
```

Configure the module package to be loaded during next startup.

```
<HUAWEI> install-module s5720hi.mod next-startup
Info: The result will be shown in several minutes. Please wait for a moment.....
...
Info: Succeeded in setting the next-startup module.
```

2.10.17 license active

Function

The **license active** command activates the license file saved in the storage of the device.

NOTE

This command takes effect only on the device that loads the license control item.

Format

license active *file-name*

Parameters

Parameter	Description	Value
file-name	Specifies the name of a license file. *file-name* supports file name association. The disk where the file resides can be automatically associated. • Full help: All the disks of the device can be associated and displayed. • Partial help: The related disk and file can be associated and displayed after you enter a specified character string.	The value is a string of 5 to 64 characters without spaces.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Change or upgrade the license file when the current license file is outdated or needs higher specifications and more features. The initial state of a license file is inactive and the license file does not take effect in the system. Run this command to activate the new or updated license file.

The **license active** command can be used to activate a license file in the following situations:

- The license needs to be activated for the first time.

  You can directly run this command to activate a license.
- The current license file needs to be updated.

  If the specifications of the new license file are lower than those of the current license file, the system displays a message asking you whether to continue. If you choose **No**, the system retains the current license file. If you choose **Yes**, the master switch activates the current license file and the system uses the new license file.

NOTICE

If the configuration items of the new license file are lower than those of the current license file, check whether the configuration items required by services exist in the new license file. If not, apply for a correct license file and activate it. Otherwise, services may be interrupted due to lack of dependent license configuration items after the board or the device is restarted.

Prerequisites

The new license file has been uploaded to the device.

Follow-up Procedure

When the system restarts, the system activates the license file that was activated last time to ensure the license files are the same before and after restart.

Precautions

- The license file must use .dat as file name extension and be saved to the default root directory in the storage of the device.
- If no path is specified, the license file in the working path is activated by default.
- If the specifications of the new license file are lower than those of the current license file (some functions are authorized in the current license file, but not

in the new license file, or the new license file allows fewer resources than the current one), the system displays a message asking you whether to continue.

- When the switch is stacked, if the ESN in the license file does not match the ESN of each stack member, activating the license file will prompt that the license file is abnormal. There is a risk that the license file will enter the grace period when the stack master changes.

Example

Activate **license.dat** in the storage of the device.

```
<HUAWEI> license active license.dat
```

Activate the license file **license.dat** in the storage of the stacked device.

```
<HUAWEI> license active license.dat
Verify license passed with minor errors:
  ESN is mismatched with node esn of slot 0.
  ESN is mismatched with node esn of slot 1.
Info: This operation maybe use the trial license instead of current licnese, may be reduce current resource or functions. Continue?[Y/N]:y
Warning: The ESN in board is different from that in the license file, Update the license file in time.
Continue? [Y/N]y
Info: The license is being activated. Please wait for a moment.
```

2.10.18 license emergency

Function

The **license emergency** command enables the emergency state for the license.

NOTE

This command takes effect only on the device that loads the license control item.

Format

license emergency

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The system configuration is classified into maximum configuration, authorized configuration, and minimum configuration.

- In maximum configuration, the maximum number of dynamic resource items are configured. Static resource items and function items are configured according to license configuration.
- Authorization configuration means the functions and resources of the software configured on the basis of contract or special authorization. Authorized configuration depends on feature authorization of license files.
- The minimum configuration is the default configuration when no activated license file exists in the system. The minimum configuration varies according to products.

Configurations are classified to limit the bearer capability of the system in different running status.

When you run the **license emergency** command to enable the emergency state for the license, the system is free from license control. In this case, the system can run with the maximum configuration of dynamic resources and the license-defined configuration of static resources and functions. When the validity period of the emergency state expires, dynamic resources are controlled by the license again. One version is provided with three validity periods of emergency state, each lasting for seven days.

The purpose for enabling the emergency state for the GTL license is disaster tolerance. If an earthquake takes place, for example, this mechanism protects users' services from being affected.

Precautions

- The emergency state cannot be disabled manually.
- The emergency state can only be enabled three times for each license, and the license can keep in emergency state for 7 days each time.
- The next emergency state can be enabled only on the last day when the last emergency state expires.
- After the emergency state is enabled, the device provides maximum number of resource control items contained in the loaded license. The device does not provide resource control items that are not contained in the loaded license even through the emergency state is enabled.

Example

Enable the license emergency state.

```
<HUAWEI> license emergency
Warning: This operation will cause LCS into the EMERGENCY state. Continue? [Y/N]:y
Info: Emergency started cannot be stopped.
```

2.10.19 virtual-license emergency

Function

The **virtual-license emergency** command enables the emergency state of the virtual license.

Format

virtual-license emergency

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **virtual-license emergency** command to enable the emergency state of the virtual license. After the emergency state is enabled, the VXLAN and AP cloud license control items are not controlled by the virtual license. After the validity period of the emergency state expires, the VXLAN and AP cloud license control items are controlled by the license. A version provides three validity periods of the emergency state, each of which lasts for seven days.

Precautions

- The emergency state cannot be disabled manually.
- The emergency state can only be enabled three times for each license, and the license can keep in emergency state for seven days each time.

Example

Enable the emergency state of the virtual license.

```
<HUAWEI> virtual-license emergency
```

2.10.20 license revoke

Function

The **license revoke** command revokes a license file.

NOTE

This command takes effect only on the device that loads the license control item.

Format

license revoke

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

License is an authorization file. You can apply for, upgrade, or activate the license file to get corresponding user rights.

If new devices are deployed, you can purchase new licenses as needed to enable license-controlled features and functions on the devices. This reduces purchase costs. If the capacities of the existing devices need to be expanded, you can update the licenses used on the devices to enable more license-controlled features and functions.

You can upgrade a license file to:

- Add new features.
- Optimizes device performance.
- Fix bugs in the current version.

Before updating a license file, run the **license revoke** command to revoke the existing license. The system then returns a license revocation code. This code is the evidence for license invalidation and is used to apply for a new license.

NOTE

A license revocation code is a character string generated after a license file becomes invalid. You can determine that a license file is invalid based on the corresponding revocation code.

Precautions

- When the existing license is going to expire, apply for a new license, upgrade, and activate the license. If the license has expired, the service modules are disabled and services are interrupted.
- After you run the **license revoke** command, the license file enters the Trial state and cannot be activated again regardless of how long the license file will expire.

Example

Revoke the current license file.

```
<HUAWEI> license revoke
Warning: The license will enter the Trial state and will not be activated again.
 Continue?[Y/N]: y
```


2.10.21 license verify

Function

The **license verify** command verifies the license file of the device.

NOTE

This command takes effect only on the device that loads the license control item.

Format

license verify *file-name*

Parameters

Parameter	Description	Value
file-name	Specifies the name of a license file. *file-name* supports file name association. The disk where the file resides can be automatically associated. • Full help: All the disks of the device can be associated and displayed. • Partial help: The related disk and file can be associated and displayed after you enter a specified character string.	The value is a string of characters without spaces.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before running the **license active** command to activate a license file, verify the license file.

The result of the **license verify** command can be the following:

- Major error
  The license file cannot be activated.
- Minor error
  The license file may be unable to be activated.
- Success
  The license file can be activated.

Prerequisites

The license file has been saved on the device.

Example

Verify the license file **license.dat**.

```
<HUAWEI> license verify license.dat
Info: Verify license succeeded.
```

2.10.22 patch active all

Function

The **patch active all** command activates the patches on the current system.

By default, the loaded patches on the current system are inactive.

Format

patch active all

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If you do not specify the **active** or **run** keyword when running the **patch load** command, run the **patch active all** command to activate all the loaded patches to make them effect.

Prerequisites

Patches have been loaded using the **patch load** command.

Configuration Impact

- After a non-incremental patch is loaded and the **patch active all** command is run, the patches in the current system are activated.
- If an incremental patch is loaded and the previous patch package is running, the previous patch package is still in running state after you run the **patch active all** command. The new patch package is activated.

Follow-up Procedure

After running the **patch active all** command, use the **patch run all** command to run the activated patch.

Precautions

After you run the **patch active all** command:

- If the device is restarted, all the active patches become inactive. To reactivate the patches, run the **patch active all** command.

To make the patches become active, run the **patch active all** command again.

The active state can prevent a patch error from causing continuous faults of the system. If a patch has a bug and the patch is in the active state, restart the device to prevent the patch from taking effect.

Example

Activate all patches.

```
<HUAWEI> patch active all
```

2.10.23 patch configuration-synchronize

Function

The **patch configuration-synchronize** command synchronizes the patch configuration and patch file of the master switch to other member switches in a stack.

Format

patch configuration-synchronize

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

After you replace or add a member switch in a stack and start the new member switch, run this command to synchronize the patch configuration and patch file from the master switch if the patch file of the new member switch is incorrect.

Example

Run the following commands on the new member switch to synchronize the patch configurations and patch files to the new member switch.


```
<HUAWEI> patch configuration-synchronize
Info: Finished synchronizing the patch package file and the patch configuration.
```

2.10.24 patch deactive all

Function

The **patch deactive all** command deactivates the patches on the current system.

Format

patch deactive all

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

This command does not take effect in the current version. During the operation, if a bug is detected in a patch and the system software problem cannot be solved, run the **patch delete all** command to delete the patches in the patch area in the memory.

Example

Deactivate patches on the current system.

```
<HUAWEI> patch deactive all
Warning: This function is no longer supported in the current version.
```

2.10.25 patch delete all

Function

The **patch delete all** command deletes patches on the current system.

Format

patch delete all

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

- If you find errors in patches that have been loaded to the system, run this command to delete the patches to prevent patch errors from affecting system operating.
- Before loading a non-incremental patch, run this command to delete the existing patches (if any). Otherwise, the non-incremental patch cannot be loaded.
- After the patch is deleted, it is recommended that you restart the switch.

Example

Delete all patches.

```
<HUAWEI> patch delete all
Warning: The device needs to restart after the patch is deleted.
This will delete the patch. Are you sure? [Y/N]
```

2.10.26 patch load

Function

The **patch load** command loads the patches to the patch areas in the system.

Format

patch load *filename* **all** [**active** | **run**]

Parameters

Parameter	Description	Value
filename	Specifies the path and file name of a patch package. The path can be an absolute path or a relative path. *file-name* supports file name association. The disk where the file resides can be automatically associated. ● Full help: All the disks of the device can be associated and displayed. ● Partial help: The related disk and file can be associated and displayed after you enter a specified character string.	The value is a string of 5 to 64 case-insensitive characters without spaces. The file name must have an extension of .pat.
all	Loads the patches of all member switches in a stack.	-
active	Activates loaded patches.	-
run	Runs loaded patches.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you load a patch to the current system, the system searches the patch package for a matching patch file according to the attributes of the patch file.

- If a matching patch file is found in the patch package, the system loads the patch.
- If no matching patch file is found in the patch package, the system does not load any patch.

Prerequisites

The patch package has been uploaded to the root directory of the storage device.

Before loading a patch, the system must resolve the patch package, check the validity of the patch files in the patch package, and obtain the attributes such as the patch type and version of the patch file.

Precautions

The patch file cannot be reloaded. When you reload a patch, the system displays an error message.

After this command is run, the system loads all types of patches in the patch package.

- If the **active** parameter is specified, the system activates the loaded patches directly. Then you can use the **patch run all** command to run the patches.
- If the **run** parameter is specified, the system runs the loaded patches directly.

Example

Load the patches to the patch area of the device and run the patches directly.

```
<HUAWEI> patch load patch.pat all run
```

2.10.27 patch run all

Function

The **patch run all** command runs the patches on the current system.

Format

patch run all

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the device is restarted, the active patches become deactivated and need to be activated again. To enable the active patches to retain in running start after a device restart, use this command to run these active patches.

Prerequisites

Patches have been loaded and activated on the system.

Configuration Impact

After you run this command to run patches on the current system, the patches remain in the running state if a device restart occurs.

After the **patch run all** command is run, the patches enter running state and cannot be restored to the previous state. Confirm the action before you run the command.

Example

Run active patches on the current system.

```
<HUAWEI> patch run all
```

2.10.28 reset patch-configure

Function

The **reset patch-configure** command deletes the configuration of the patch file for next startup.

Format

reset patch-configure [**next-startup**]

Parameters

Parameter	Description	Value
next-startup	Deletes the configuration of the patch file for next startup.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After you run the **startup patch** command to specify the patch file for next startup, you can use the **reset patch-configure** command to delete the configuration.

Precautions

If you run the **reset patch-configure** command, the patch file for next startup is empty. When the device restarts, the system does not load and run the patch file.

Example

Delete the configuration of the patch file for next startup.

```
<HUAWEI> reset patch-configure next-startup
Info: The result will be shown in several minutes. Please wait for a moment.....
...
Info: Succeeded in resetting the next-startup patch state.
```

2.10.29 rollback

Function

The **rollback** command rolls back the system to the previous version.

Format

rollback

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If an error occurs during an upgrade and you need to cancel the upgrade, run the **rollback** command to roll back the system to the previous version. After the rollback, the configuration of the device is the same as the previous configuration.

Precautions

- The rollback function takes effect only for an upgrade during which the **reboot** command is run to restart the device, and does not support other upgrade modes, such as the EasyDeploy upgrade and smooth stack upgrade. If the **reboot** command is run to complete an upgrade and then the system is upgraded using another mode, you can only run the **rollback** command to roll back the system to the latest version before the upgrade during which the **reboot** command is run. For example, if you run the **reboot** command to restart the device and upgrade the system from V1.0 to V1.1, and then upgrade the system to V1.2 using EasyDeploy, the system can only be rolled back to V1.0 when you run the **rollback** command to perform a system rollback.
- If a device runs continuously for more than 48 hours after being upgraded, the rollback function does not take effect. If the device runs continuously for less than 48 hours and restarts, the system sets the remaining time to zero

and the rollback function does not take effect. You can run the **display rollback information** command to check the remaining time for the rollback function to take effect.

- If the system software, configuration file, or patch file required in the rollback is deleted using the **delete (user view)** command, the system prompts that the rollback function cannot be used when you run the **rollback** command.

NOTICE

If you run the **rollback** command to roll back the system software, the current configuration of the device will be lost. Therefore, exercise caution when deciding to run this command.

Prerequisites

The device contains the system software, configuration file, and patch file that are used after the rollback and displayed in the **display rollback information** command output.

Example

Roll back the system to the previous version.

```
<HUAWEI> rollback
Info: Checking rollback version information...
Rollback software: flash:/basicsoft.cc
Rollback configuration: flash:/vrpcfg.zip
Rollback patch: NULL
Warning: The version running before the last reboot/reboot fast operation is performed will be restored,
and the current configuration will be lost. Continue? [Y/N]:y
```

2.10.30 uninstall-module

Function

The **uninstall-module** command uninstalls module packages.

Format

uninstall-module *file-name* [**next-startup**]

uninstall-module next-startup all

Parameters

Parameter	Description	Value
file-name	Specifies the name of a module package to be uninstalled.	The value is a string of 5 to 64 case-insensitive characters without spaces.
next-startup	Clears the module list for next startup.	-

Parameter	Description	Value
all	Clears the module list for next startup.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

If some services or functions are not required, run the **uninstall-module** command to uninstall the corresponding modules running in the system.

Example

Uninstall the module package s5720hi.mod from the system.

```
<HUAWEI> uninstall-module s5720hi.mod
This will uninstall the module. Are you sure? [Y/N]y....
Info: Succeeded in uninstalling the module on the master board.
```

Clear a specified module package in the next startup module list.

```
<HUAWEI> uninstall-module s5720hi.mod next-startup
Info: The result will be shown in several minutes. Please wait for a moment.....
...
Info: Succeeded in resetting the next-startup module.
```

