Hewlett Packard Enterprise

HPE FlexFabric 5945 Switch Series

Fundamentals Command Reference

Part number: 5200-7082
Software version: Release 6607 and later
Document version: 6W100-20200402

© Copyright 2020 Hewlett Packard Enterprise Development LP

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

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

Acknowledgments

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

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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

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

UNIX® is a registered trademark of The Open Group.

Contents

Basic CLI commands ····· 1

alias ····· 1
display [| [by-linenum] { begin | exclude | include }] ····· 2
display > ····· 4
display >> ····· 5
display alias ····· 6
display history-command ····· 6
display history-command all ····· 7
display hotkey ····· 8
hotkey ····· 9
quit ····· 11
repeat ····· 11
return ····· 13
screen-length disable ····· 13
system-view ····· 14

RBAC commands ····· 15

description ····· 15
display role ····· 15
display role feature ····· 22
display role feature-group ····· 25
feature ····· 27
interface policy deny ····· 28
permit interface ····· 29
permit vlan ····· 31
permit vpn-instance ····· 32
role ····· 34
role default-role enable ····· 34
role feature-group ····· 35
rule ····· 36
super ····· 40
super authentication-mode ····· 41
super default role ····· 42
super password ····· 42
super use-login-username ····· 44
vlan policy deny ····· 44
vpn-instance policy deny ····· 45

Login management commands ····· 47

activation-key ····· 47
authentication-mode ····· 49
auto-execute command ····· 51
command accounting ····· 52
command authorization ····· 53
databits ····· 54
display line ····· 54
display telnet client ····· 56
display user-interface ····· 56
display users ····· 58
escape-key ····· 59
flow-control ····· 60
free line ····· 61
free user-interface ····· 62
history-command max-size ····· 62
http acl ····· 63
https acl ····· 64
idle-timeout ····· 65

line ····· 66
line class ····· 66
lock ····· 68
lock reauthentication ····· 69
lock-key ····· 69
parity ····· 70
protocol inbound ····· 71
restful http enable ····· 73
restful http port ····· 74
restful https enable ····· 74
restful https port ····· 75
screen-length ····· 75
send ····· 76
set authentication password ····· 77
shell ····· 78
speed ····· 79
stopbits ····· 79
telnet ····· 80
telnet client source ····· 81
telnet ipv6 ····· 82
telnet server acl ····· 83
telnet server acl-deny-log enable ····· 84
telnet server dscp ····· 84
telnet server enable ····· 85
telnet server ipv6 acl ····· 85
telnet server ipv6 dscp ····· 86
telnet server ipv6 port ····· 87
telnet server port ····· 87
terminal type ····· 88
user-interface ····· 89
user-interface class ····· 90
user-role ····· 91
FTP commands ····· 93
FTP server commands ····· 93
display ftp-server ····· 93
display ftp-user ····· 93
free ftp user ····· 94
free ftp user-ip ····· 95
free ftp user-ip ipv6 ····· 95
ftp server acl ····· 96
ftp server acl-deny-log enable ····· 97
ftp server dscp ····· 97
ftp server enable ····· 98
ftp server ipv6 dscp ····· 98
ftp server ssl-server-policy ····· 99
ftp timeout ····· 99
FTP client commands ····· 100
? ····· 100
append ····· 101
ascii ····· 102
binary ····· 102
bye ····· 103
cd ····· 103
cdup ····· 104
close ····· 105
debug ····· 105
delete ····· 106
dir ····· 106
disconnect ····· 107
display ftp client source ····· 108
ftp ····· 108

ftp client ipv6 source ····· 110
ftp client source ····· 111
ftp ipv6 ····· 111
get ····· 113
help ····· 114
lcd ····· 115
ls ····· 115
mkdir ····· 117
newer ····· 117
open ····· 118
passive ····· 118
put ····· 119
pwd ····· 120
quit ····· 120
reget ····· 121
rename ····· 121
reset ····· 122
restart ····· 123
rhelp ····· 123
rmdir ····· 125
rstatus ····· 125
status ····· 127
system ····· 128
user ····· 128
verbose ····· 129
TFTP commands ····· 131
tftp ····· 131
tftp client ipv6 source ····· 133
tftp client source ····· 133
tftp ipv6 ····· 134
tftp-server acl ····· 136
tftp-server ipv6 acl ····· 136
File system management commands ····· 138
cd ····· 138
copy ····· 139
delete ····· 142
dir ····· 143
execute ····· 144
fdisk ····· 144
file prompt ····· 146
fixdisk ····· 147
format ····· 147
gunzip ····· 148
gzip ····· 149
md5sum ····· 150
mkdir ····· 150
more ····· 151
mount ····· 151
move ····· 152
pwd ····· 153
rename ····· 153
reset recycle-bin ····· 153
rmdir ····· 154
sha256sum ····· 155
tar create ····· 155
tar extract ····· 156
tar list ····· 157
umount ····· 158
undelete ····· 159

Configuration file management commands ····· 160
archive configuration ····· 160
archive configuration interval ····· 161
archive configuration location ····· 162
archive configuration max ····· 163
archive configuration server ····· 164
archive configuration server password ····· 166
archive configuration server user ····· 166
backup startup-configuration ····· 167
configuration commit ····· 168
configuration commit delay ····· 169
configuration encrypt ····· 170
configuration replace file ····· 170
display archive configuration ····· 171
display current-configuration ····· 172
display current-configuration diff ····· 174
display default-configuration ····· 175
display diff ····· 176
display saved-configuration ····· 177
display startup ····· 178
display this ····· 179
reset saved-configuration ····· 180
restore startup-configuration ····· 181
save ····· 182
standby auto-update config ····· 185
startup saved-configuration ····· 185
Software upgrade commands ····· 187
boot-loader file ····· 187
boot-loader update ····· 189
display boot-loader ····· 190
ISSU commands ····· 192
display install active ····· 192
display install backup ····· 193
display install committed ····· 195
display install inactive ····· 196
display install ipe-info ····· 197
display install job ····· 198
display install log ····· 198
display install package ····· 200
display install rollback ····· 201
display install which ····· 201
display issu rollback-timer ····· 203
display issu state ····· 203
display version comp-matrix ····· 206
install abort ····· 207
install activate ····· 208
install add ····· 210
install commit ····· 211
install deactivate ····· 212
install remove ····· 213
install rollback to ····· 213
install verify ····· 215
issu accept ····· 216
issu commit ····· 216
issu load ····· 218
issu one-step ····· 221
issu quit ····· 223
issu rollback ····· 223
issu rollback-timer ····· 224

issu run switchover ····· 225
reset install log-history oldest ····· 227
reset install rollback oldest ····· 227
Preprovisioning commands ····· 229
display provision failed-config ····· 229
provision ····· 229
reset provision failed-config ····· 230
slot ····· 231
Device management commands ····· 232
clock datetime ····· 232
clock protocol ····· 233
clock summer-time ····· 233
clock timezone ····· 235
command ····· 236
copyright-info enable ····· 237
display alarm ····· 237
display clock ····· 238
display copyright ····· 239
display cpu-usage ····· 239
display cpu-usage configuration ····· 240
display cpu-usage history ····· 241
display device ····· 243
display device manuinfo ····· 244
display device manuinfo fan ····· 244
display device manuinfo power ····· 245
display diagnostic-information ····· 245
display environment ····· 247
display fan ····· 248
display hardware-failure-detection ····· 249
display hardware-resource switch-mode ····· 250
display memory ····· 251
display memory-threshold ····· 252
display power ····· 254
display resource-monitor ····· 255
display scheduler job ····· 256
display scheduler logfile ····· 257
display scheduler reboot ····· 258
display scheduler schedule ····· 258
display system stable state ····· 259
display system-working-mode ····· 261
display transceiver alarm ····· 261
display transceiver diagnosis ····· 263
display transceiver interface ····· 264
display transceiver manuinfo ····· 264
display version ····· 264
display version-update-record ····· 265
download manuinfo fan ····· 266
fan prefer-direction ····· 267
hardware-failure-detection ····· 267
hardware-resource switch-mode ····· 268
header ····· 269
job ····· 270
locator blink ····· 271
memory-threshold ····· 271
memory-threshold usage ····· 273
monitor cpu-usage enable ····· 273
monitor cpu-usage interval ····· 274
monitor cpu-usage threshold ····· 275
monitor resend cpu-usage ····· 276
monitor resend memory-threshold ····· 277

parity-error consistency-check log enable ... 278
parity-error consistency-check period ... 279
parity-error consistency-check threshold ... 280
parity-error monitor log enable ... 280
parity-error monitor period ... 281
parity-error monitor threshold ... 282
password-recovery enable ... 282
reboot ... 283
reset scheduler logfile ... 284
reset version-update-record ... 285
resource-monitor minor resend enable ... 285
resource-monitor output ... 286
resource-monitor resource ... 287
restore factory-default ... 289
scheduler job ... 289
scheduler logfile size ... 290
scheduler reboot at ... 291
scheduler reboot delay ... 292
scheduler schedule ... 292
shutdown-interval ... 293
sysname ... 294
system-working-mode ... 295
temperature-limit ... 295
time at ... 296
time once ... 297
time repeating ... 298
user-role ... 300
Tcl commands ... 301
cli ... 301
tclquit ... 301
tclsh ... 302
Python commands ... 303
exit() ... 303
python ... 303
python *filename* ... 304
Document conventions and icons ... 305
Conventions ... 305
Network topology icons ... 306
Support and other resources ... 307
Accessing Hewlett Packard Enterprise Support ... 307
Accessing updates ... 307
Websites ... 308
Customer self repair ... 308
Remote support ... 308
Documentation feedback ... 308
Index ... 310

Basic CLI commands

alias

Use **alias** to configure a command alias.

Use **undo alias** to delete a command alias.

Syntax

alias *alias command*

undo alias *alias*

Default

The device has a set of system-defined command aliases, as listed in Table 1.

Table 1 System-defined command aliases

Command alias	Command or command keyword
access-list	**acl**
end	**return**
erase	**delete**
exit	**quit**
hostname	**sysname**
logging	**info-center**
no	**undo**
show	**display**
write	**save**

Views

System view

Predefined user roles

network-admin

Parameters

alias: Specifies an alias, a case-sensitive string of 1 to 20 characters. An alias cannot be **alias** or contain spaces or double quotation marks (").

command: Specifies a command string. Make sure the command string meets the syntax requirements.

Usage guidelines

System-defined command aliases cannot be deleted.

You can configure one or more aliases for a command or the starting keywords of commands. Then, you can use the aliases to execute the command or commands. If the command or commands have **undo** forms, you can also use the aliases to execute the **undo** command or commands.

For example, if you configure the alias **shiprt** for **display ip routing-table**, you can enter **shiprt** to execute the **display ip routing-table** command. If you configure the alias **ship** for **display ip**, you can use **ship** to execute all commands that start with **display ip**:

- Enter **ship routing-table** to execute the **display ip routing-table** command.
- Enter **ship interface** to execute the **display ip interface** command.

The command string can include up to nine parameters. Each parameter starts with the dollar sign ($) and a sequence number in the range of 1 to 9. For example, you can configure the alias **shinc** for the **display ip $1 | include $2** command. Then, to execute the **display ip routing-table | include Static** command, you only need to enter **shinc routing-table Static**. To execute the **display ip interface | include Twenty-FiveGigE1/0/1** command, you only need to enter **shinc interface Twenty-FiveGigE1/0/1**.

Examples

Configure **shiprt** as the alias for the **display ip routing-table** command and verify the configuration.

```
<Sysname> system-view
[Sysname] alias shiprt display ip routing-table
[Sysname] shiprt
Destinations : 13        Routes : 13
Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
3.3.3.3/32         Static  60  0           192.168.1.62    Vlan1
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
169.254.0.0/24     Direct  0   0           169.254.0.188   Vlan1
169.254.0.0/32     Direct  0   0           169.254.0.188   Vlan1
169.254.0.188/32   Direct  0   0           127.0.0.1       InLoop0
169.254.0.255/32   Direct  0   0           169.254.0.188   Vlan1
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

Configure **shinc** as the alias for **display ip $1 | include $2**.

```
[Sysname] alias shinc display ip $1 | include $2
```

Use alias **shinc** to display all static routes.

```
[Sysname] shinc routing-table Static
3.3.3.3/32         Static  60  0           192.168.1.62    Vlan1
```

Related commands

display alias

display [| [by-linenum] { begin | exclude | include }]

Use **display** [**|** [**by-linenum**] { **begin** | **exclude** | **include** }] to filter the output from a **display** command with regular expressions.

Syntax

display *command* [**|** [**by-linenum**] { **begin** | **exclude** | **include** } *regular-expression*]&<1-128>

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

command: Specifies the keywords and arguments of a **display** command. To display available keywords and arguments, enter **display ?**.

[**|** [**by-linenum**] { **begin** | **exclude** | **include** } *regular-expression*]&<1-128>: Specifies a maximum of 128 filter conditions.

- **by-linenum**: Numbers the output lines. You need to specify this keyword in only one filter condition.
- **begin**: Displays the first line matching the specified regular expression and all subsequent lines.
- **exclude**: Displays all lines not matching the specified regular expression.
- **include**: Displays all lines matching the specified regular expression.
- *regular-expression*: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

Usage guidelines

To quickly locate certain lines in the output from a **display** command, you can use regular expressions to filter the output, and display a number before each output line. For more information about regular expressions, see *Fundamentals Configuration Guide*.

If you specify multiple filter conditions, the system displays the output lines that meet all the conditions.

A line number is a 5-character string and is typically followed by a colon (:). If you specify both the **by-linenum** and **begin** *regular-expression* options, a line number might be followed by a colon or a hyphen (-).

- **Colon**—The line matches the regular expression.
- **Hyphen**—The line does not match the regular expression.

Examples

Display the lines that contain **vlan** in the running configuration.

```
<Sysname> display current-configuration | include vlan
vlan 1
vlan 999
 port access vlan 999
```

Display log entries in the log buffer that contain both **SHELL** and **VTY**.

```
<Sysname> display logbuffer | include SHELL | include VTY
%Sep  6 10:38:12:320 2018 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from 169.254.100.171.
%Sep  6 10:52:32:576 2018 Sysname SHELL/5/SHELL_LOGOUT: VTY logged out from
169.254.100.171.
%Sep  6 16:03:27:100 2018 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from 169.254.100.171.
```

```
%Sep  6 16:44:18:113 2018 Sysname SHELL/5/SHELL_LOGOUT: VTY logged out from
169.254.100.171.
```

Display the running configuration, starting from the first line that contains **user-group** and numbering the output lines.

```
<Sysname> display current-configuration | by-linenum begin user-group
  114:  user-group system
  115-  #
  116-  return
```

display >

Use **display >** to save the output from a **display** command to a separate file.

Syntax

display *command* **>** *filename*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

command: Specifies the keywords and arguments of a **display** command. To display available keywords and arguments, enter **display ?**.

filename: Specifies the name of the file that is used to save the output, a string of 1 to 63 characters.

Usage guidelines

The **display** commands show the configuration, statistics, and states of the device. You can use the **display >** command to save the output to a file.

If the specified file does not exist, the system creates the file and saves the output to the file. If the file already exists, the system overwrites the file.

Examples

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

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

Check the content of the **vlan.txt** file.

```
<Sysname> more vlan.txt
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:   None
 Untagged ports:
    Twenty-FiveGigE1/0/2
```

display >>

Use **display >>** to append the output from a **display** command to the end of a file.

Syntax

display *command* **>>** *filename*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

command: Specifies the keywords and arguments of a **display** command. To display available keywords and arguments, enter **display ?**.

filename: Specifies the name of the file that is used to save the output, a string of 1 to 63 characters.

Usage guidelines

The **display** commands show the configuration, statistics, and states of the device. You can use **display >>** to save the output to a file.

If the specified file does not exist, the system creates the file and saves the output to the file. If the file already exists, the system appends the output to the end of the file.

Examples

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

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

Check the content of the **vlan.txt** file.

```
<Sysname> more vlan.txt
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:   None
 Untagged ports:
    Twenty-FiveGigE1/0/2

 VLAN ID: 999
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 192.168.2.1
 IPv4 subnet mask: 255.255.255.0
 Description: For LAN Access
 Name: VLAN 0999
 Tagged ports:   None
 Untagged ports:
```

```
Twenty-FiveGigE1/0/2
```

display alias

Use **display alias** to display command aliases.

Syntax

display alias [*alias*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

alias: Specifies a command alias. If you do not specify this argument, the command displays all command aliases.

Examples

Display all command aliases.

```
<Sysname> display alias
Index     Alias               Command key
1         access-list         acl
2         end                 return
3         erase               delete
4         exit                quit
5         hostname            sysname
6         logging             info-center
7         no                  undo
8         shinc               display $1 | include $2
9         show                display
10        sirt                display ip routing-table
11        write               save
```

Display the command alias **shinc**.

```
<Sysname> display alias shinc
Alias               Command key
shinc               display ip $1 | include $2
```

Related commands

alias

display history-command

Use **display history-command** to display all commands that are saved in the command history buffer for the current CLI session.

Syntax

display history-command

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

The system automatically saves commands you have successfully executed to the command history buffer for the current CLI session. You can view them and execute them again.

By default, the system can save up to 10 commands in the buffer. You can use the **history-command max-size** command to change the buffer size. To buffer a new command when the buffer is full, the system deletes the oldest command entry in the buffer.

All commands in the command history buffer for the current CLI session will be cleared when you log out.

The system displays passwords as asterisks (*) to ensure device security if the command history buffer has password configuration commands.

Examples

Display all commands saved in the command history buffer for the current CLI session.

```
<Sysname> display history-command
  system-view
  vlan 2
  quit
```

Related commands

history-command max-size

display history-command all

Use **display history-command all** to display all commands that are saved in the command history buffer for all CLI sessions.

Syntax

display history-command all

Views

Any view

Predefined user roles

network-admin

Usage guidelines

The system automatically saves commands successfully executed by users to the command history buffer for all CLI sessions. Users can view them but cannot recall them from the buffer.

Up to 1024 commands can be saved in the command history buffer. To buffer a new command when the buffer is full, the system deletes the oldest command entry in the buffer.

A user logout does not cause the system to delete commands from the history buffer for all CLI sessions.

The system displays passwords as asterisks (*) to ensure device security if the command history buffer has password configuration commands.

Examples

Display all commands saved in the command history buffer for all CLI sessions.

```
<Sysname> display history-command all
  Date       Time     Terminal   Ip              User
  03/16/2017 20:03:33 vty0       192.168.1.26    **
  Cmd:dis his all

  03/16/2017 20:03:29 vty0       192.168.1.26    **
  Cmd:sys
```

Table 2 Command output

Field	Description
Date	Date when the command was executed.
Time	Time when the command was executed.
Terminal	User line used by the user.
Ip	IP address of the terminal used by the user.
User	Username used by the user if the user login authentication mode is **scheme**. If the login authentication mode is **none** or **password**, this field displays ******.
Cmd	Command string entered by the user.

Related commands

display history-command

display hotkey

Use **display hotkey** to display hotkey information.

Syntax

display hotkey

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display hotkey information.

```
<Sysname> display hotkey
----------------- Hotkeys -----------------
           -Defined function hotkeys-
CTRL_A  Move the cursor to the beginning of the line.
CTRL_B  Move the cursor one character to the left.
CTRL_C  Stop the current command.
CTRL_D  Erase the character at the cursor.
CTRL_E  Move the cursor to the end of the line.
```

```
CTRL_F  Move the cursor one character to the right.
CTRL_H  Erase the character to the left of the cursor.
CTRL_N  Display the next command in the history buffer.
CTRL_P  Display the previous command in the history buffer.
CTRL_R  Redisplay the current line.
CTRL_W  Delete the word to the left of the cursor.
CTRL_X  Delete all characters from the beginning of the line to the cursor.
CTRL_Y  Delete all characters from the cursor to the end of the line.
CTRL_Z  Return to the User View.
CTRL_]  Kill incoming connection or redirect connection.
ESC_B   Move the cursor back one word.
ESC_D   Delete all characters from the cursor to the end of the word.
ESC_F   Move the cursor forward one word.
           -Defined command hotkeys-
CTRL_G  display current-configuration
CTRL_L  display ip routing-table
CTRL_O  undo debugging all
           -Undefined hotkeys-
CTRL_T  NULL
CTRL_U  NULL
```

Related commands

hotkey

hotkey

Use **hotkey** to configure a hotkey.

Use **undo hotkey** to restore the default.

Syntax

hotkey *hotkey* { *command* | **function** *function* | **none** }

undo hotkey *hotkey*

Default

Table 3 shows the default definitions for hotkeys.

Table 3 Default definitions for hotkeys

Hotkey	Function or command
Ctrl+A	**move_the_cursor_to_the_beginning_of_the_line**: Moves the cursor to the beginning of a line.
Ctrl+B	**move_the_cursor_one_character_to_the_left**: Moves the cursor one character to the left.
Ctrl+C	**stop_the_current_command**: Stops the current command.
Ctrl+D	**erase_the_character_at_the_cursor**: Deletes the character at the cursor.
Ctrl+E	**move_the_cursor_to_the_end_of_the_line**: Moves the cursor to the end of a line.
Ctrl+F	**move_the_cursor_one_character_to_the_right**: Moves the cursor one character to the right.

Hotkey	Function or command
Ctrl+G	**`display current-configuration`**: Displays the running configuration.
Ctrl+H	**erase_the_character_to_the_left_of_the_cursor**: Deletes the character to the left of the cursor.
Ctrl+L	**`display ip routing-table`**: Displays the IPv4 routing table information.
Ctrl+N	**display_the_next_command_in_the_history_buffer**: Displays the next command in the history buffer. Password configuration commands, if any, are skipped.
Ctrl+O	**`undo debugging all`**: Displays all debugging functions.
Ctrl+P	**display_the_previous_command_in_the_history_buffer**: Displays the previous command in the history buffer. Password configuration commands, if any, are skipped.
Ctrl+R	**redisplay_the_current_line**: Redisplays the current line.
Ctrl+T	N/A
Ctrl+U	N/A
Ctrl+W	**delete_the_word_to_the_left_of_the_cursor**: Deletes the word to the left of the cursor.
Ctrl+X	**delete_all_characters_from_the_beginning_of_the_line_to_the_cursor**: Deletes all characters to the left of the cursor.
Ctrl+Y	**delete_all_characters_from_the_cursor_to_the_end_of_the_line**: Deletes all characters from the cursor to the end of the line.
Ctrl+Z	**return_to_the_User_View**: Returns to user view.
Ctrl+]	**kill_incoming_connection_or_redirect_connection**: Terminates the current connection.
Esc+B	**move_the_cursor_back_one_word**: Moves the cursor back one word.
Esc+D	**delete_all_characters_from_the_cursor_to_the_end_of_the_word**: Deletes all characters from the cursor to the end of the word.
Esc+F	**move_the_cursor_forward_one_word**: Moves the cursor forward one word.

Views

System view

Predefined user roles

network-admin

Parameters

`hotkey`: Specifies a hotkey. To display the supported hotkeys, enter **`hotkey ?`** or see Table 3.

`command`: Specifies the command to be assigned to the hotkey.

`function` *`function`*: Specifies the function to be assigned to the hotkey. To display the supported functions, enter **`hotkey`** *`hotkey`* **`function ?`** or see Table 3.

none: Removes the command or function assignment for the hotkey. After you remove the assignment for a hotkey, pressing the hotkey does not execute any command or function.

Usage guidelines

The device supports a set of hotkeys. Pressing a hotkey executes the command or function assigned to the hotkey. You can configure all the hotkeys except **Ctrl+]**.

A hotkey can correspond to only one command or function. If you assign multiple commands or functions to the same hotkey, the most recently assigned command or function takes effect.

A command or function can be assigned to multiple hotkeys. You can use any of those hotkeys to execute the command or function.

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

Examples

Assign the **display tcp statistics** command to hotkey **Ctrl+T**.

```
<Sysname> system-view
[Sysname] hotkey ctrl_t display tcp statistics
```

Assign move_the_cursor_to_the_beginning_of_the_line function to hotkey **Ctrl+U**.

```
<Sysname> system-view
[Sysname] hotkey ctrl_u function move_the_cursor_to_the_beginning_of_the_line
```

Disable the configurable command or function assigned to hotkey **Ctrl+A**.

```
<Sysname> system-view
[Sysname] hotkey ctrl_a none
```

Related commands

display hotkey

quit

Use **quit** to return to the upper-level view.

Syntax

quit

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Executing this command in user view disconnects you from the device.

Examples

Return from Twenty-FiveGigE 1/0/1 interface view to system view and then to user view.

```
[Sysname-Twenty-FiveGigE1/0/1] quit
[Sysname] quit
<Sysname>
```

repeat

Use **repeat** to repeat commands in the command history buffer for the current CLI session.

Syntax

repeat [*number*] [**count** *times*] [**delay** *seconds*]

Views

Any view

Predefined user roles

network-admin

Parameters

number: Specifies the number of the most recently executed commands in the command history buffer for the current CLI session that you want to execute. The value range is 1 to 10. The default is 1.

count *times*: Specifies the number of times that you want to execute the commands. The value range is 0 to 4294967295. The default is 0. If you do not specify this option, the system keeps executing the commands until you press the escape key to terminate the execution.

delay *seconds*: Specifies the time (in seconds) for the system to wait before executing the commands again. The value range is 0 to 4294967295. The default is 1.

Usage guidelines

To repeat a command, first enter the view for the command. To repeat multiple commands, first enter the view for the first command.

The **repeat** command executes commands in the order they were executed.

The system starts a timer and waits for your interaction when it repeats an interactive command. If you do not provide the required information at prompt before the timer expires, the system skips the interactive command.

The system skips all password configuration commands.

Examples

Configure the system to execute the two most recently executed commands (**display cpu-usage** and **display clock**) three times at an interval of 10 seconds.

```
<Sysname> repeat 2 count 3 delay 10
<Sysname> display cpu
Slot 1 CPU 0 CPU usage:
      33% in last 5 seconds
      32% in last 1 minute
      33% in last 5 minutes
<Sysname> display clock
07:02:18.230 UTC Thu 06/19/2017
<Sysname> display cpu-usage
Slot 1 CPU 0 CPU usage:
      33% in last 5 seconds
      32% in last 1 minute
      33% in last 5 minutes
<Sysname> display clock
07:02:28.263 UTC Thu 06/19/2017
<Sysname> display cpu-usage
Slot 1 CPU 0 CPU usage:
      33% in last 5 seconds
      32% in last 1 minute
      33% in last 5 minutes
<Sysname> display clock
07:02:38.293 UTC Thu 06/19/2017
```

Related commands

display history-command

escape-key

history-command max-size

return

Use **return** to return to user view from any other view.

Syntax

return

Views

Any view except user view

Predefined user roles

network-admin

network-operator

Usage guidelines

Pressing **Ctrl+Z** has the same effect as the **return** command.

Examples

Return to user view from Twenty-FiveGigE 1/0/1 interface view.

```
[Sysname-Twenty-FiveGigE1/0/1] return
<Sysname>
```

screen-length disable

Use **screen-length disable** to disable pausing between screens of output for the current CLI session.

Use **undo screen-length disable** to enable pausing between screens of output for the current CLI session.

Syntax

screen-length disable

undo screen-length disable

Default

The default depends on the configuration of the **screen-length** command in user line view.

The following are the default settings for the **screen-length** command:

- Pausing between screens of output.
- Displaying up to 24 lines on a screen.

Views

User view

Predefined user roles

network-admin

Usage guidelines

If you disable pausing between screens of output, all output is displayed. The screen is refreshed continuously until the final screen is displayed.

This command takes effect only for the current CLI session. When you are logged out, the default is restored.

Examples

Disable pausing between screens of output for the current CLI session.

```
<Sysname> screen-length disable
```

Related commands

screen-length

system-view

Use **system-view** to enter system view from user view.

Syntax

system-view

Views

User view

Predefined user roles

network-admin

network-operator

Examples

Enter system view from user view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname]
```

RBAC commands

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

description

Use **description** to configure a description for a user role for easy identification.

Use **undo description** to restore the default.

Syntax

description *text*

undo description

Default

A user role does not have a description.

Views

User role view

Predefined user roles

network-admin

Parameters

text: Specifies a description, a case-sensitive string of 1 to 128 characters.

Examples

Configure the description as **labVIP** for user role **role1**.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] description labVIP
```

Related commands

display role

role

display role

Use **display role** to display user role information.

Syntax

display role [**name** *role-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *role-name*: Specifies a user role name, a case-sensitive string of 1 to 63 characters. If you do not specify a user role name, the command displays information about all user roles, including the predefined user roles.

Examples

Display information about user role **123**.

```
<Sysname> display role name 123
Role: 123
  Description: new role
  VLAN policy: deny
  Permitted VLANs: 1 to 5, 7 to 8
  Interface policy: deny
  Permitted interfaces: Twenty-FiveGigE1/0/1 to Twenty-FiveGigE1/0/3, Vlan-interface1 to
Vlan-interface20
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  1       permit RWX   feature-group abc
  2       deny   -W-   feature       ldap
  3       permit       command       system ; radius sc *
  4       permit R--   xml-element   -
  5       permit RW-   oid           1.2.1
  R:Read W:Write X:Execute
```

Display information about all user roles.

```
<Sysname> display role
Role: network-admin
  Description: Predefined network admin role has access to all commands on the device
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       *
  sys-2   permit RWX   web-menu      -
  sys-3   permit RWX   xml-element   -
  sys-4   deny         command       display security-logfile summary
  sys-5   deny         command       display security-logfile buffer
  sys-6   deny         command       system-view ; info-center
                                     security-logfile directory *
  sys-7   deny         command       security-logfile save
  sys-8   permit RW-   oid           1
  R:Read W:Write X:Execute

Role: network-operator
  Description: Predefined network operator role has access to all read commands
on the device
```

```
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       display *
  sys-2   permit       command       xml
  sys-3   permit       command       system-view ; probe ; display *
  sys-4   deny         command       display history-command all
  sys-5   deny         command       display exception *
  sys-6   deny         command       display cpu-usage configuration
                                     *
  sys-7   deny         command       display kernel exception *
  sys-8   deny         command       display kernel deadloop *
  sys-9   deny         command       display kernel starvation *
  sys-10  deny         command       display kernel reboot *
  sys-13  permit       command       system-view ; local-user *
  sys-16  permit R--   web-menu      -
  sys-17  permit RW-   web-menu      m_device/m_maintenance/
                                     m_changepassword
  sys-18  permit R--   xml-element   -
  sys-19  deny         command       display security-logfile summary
  sys-20  deny         command       display security-logfile buffer
  sys-21  deny         command       system-view ; info-center
                                     security-logfile directory *
  sys-22  deny         command       security-logfile save
  sys-23  deny         command       system-view ; local-user-import
                                     *
  sys-24  deny         command       system-view ; local-user-export
                                     *
  sys-25  permit R--   oid           1
  R:Read W:Write X:Execute

Role: level-0
  Description: Predefined level-0 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       tracert *
  sys-2   permit       command       telnet *
  sys-3   permit       command       ping *
  sys-4   permit       command       ssh2 *
  sys-5   permit       command       super *
  sys-6   permit       command       mtrace *
```

```
  R:Read W:Write X:Execute

Role: level-1
  Description: Predefined level-1 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       tracert *
  sys-2   permit       command       telnet *
  sys-3   permit       command       ping *
  sys-4   permit       command       ssh2 *
  sys-5   permit       command       display *
  sys-6   permit       command       super *
  sys-7   deny         command       display history-command all
  sys-8   permit       command       mtrace *
  R:Read W:Write X:Execute

Role: level-2
  Description: Predefined level-2 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-3
  Description: Predefined level-3 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-4
  Description: Predefined level-4 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-5
  Description: Predefined level-5 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-6
  Description: Predefined level-6 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
```

```
  VPN instance policy: permit (default)

Role: level-7
  Description: Predefined level-7 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-8
  Description: Predefined level-8 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-9
  Description: Predefined level-9 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ------------------------------------------------------------------
  sys-1   permit RWX   feature       -
  sys-2   deny   RWX   feature       device
  sys-3   deny   RWX   feature       filesystem
  sys-4   permit       command       display *
  sys-5   deny         command       display history-command all
  R:Read W:Write X:Execute

Role: level-10
  Description: Predefined level-10 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-11
  Description: Predefined level-11 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-12
  Description: Predefined level-12 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-13
```

```
  Description: Predefined level-13 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-14
  Description: Predefined level-14 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-15
  Description: Predefined level-15 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit       command       *
  sys-2   permit RWX   web-menu      -
  sys-3   permit RWX   xml-element   -
  sys-4   deny         command       display security-logfile summary
  sys-5   deny         command       display security-logfile buffer
  sys-6   deny         command       system-view ; info-center
                                     security-logfile directory *
  sys-7   deny         command       security-logfile save
  sys-8   permit RW-   oid           1
  R:Read W:Write X:Execute

Role: security-audit
  Description: Predefined security audit role only has access to commands for the security
log administrator
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   deny         command       *
  sys-2   permit       command       display security-logfile summary
  sys-3   permit       command       display security-logfile buffer
  sys-4   permit       command       system-view ; info-center
                                     security-logfile directory *
  sys-5   permit       command       security-logfile save
  sys-6   permit       command       cd *
  sys-7   permit       command       copy *
  sys-8   permit       command       delete *
  sys-9   permit       command       dir *
```

```
  sys-10  permit       command       mkdir *
  sys-11  permit       command       more *
  sys-12  permit       command       move *
  sys-13  permit       command       rmdir *
  sys-14  permit       command       pwd
  sys-15  permit       command       rename *
  sys-16  permit       command       undelete *
  sys-17  permit       command       ftp *
  sys-18  permit       command       sftp *
  R:Read W:Write X:Execute

Role: guest-manager
  Description: Predefined guest manager role can't access to commands
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  sys-1   permit RWX   xml-element   useraccounts/approveguest/
  sys-2   permit RWX   xml-element   useraccounts/exportguestaccount/
  sys-3   permit RWX   xml-element   useraccounts/generateguestaccount/
  sys-4   permit RWX   xml-element   useraccounts/guest/
  sys-5   permit RWX   xml-element   useraccounts/guestconfigure/
  sys-6   permit RWX   xml-element   useraccounts/importguestaccount/
  sys-7   permit RWX   xml-element   useraccounts/exportguesttemplet/
  sys-8   permit RWX   xml-element   rpc/
  sys-9   deny         command       *
  R:Read W:Write X:Execute
```

Table 4 Command output

Field	Description
Role	User role name. Predefined user role names: • network-admin. • network-operator. • level-*n* (where *n* represents an integer in the range of 0 to 15). • security-audit. • guest-manager. This user role is not supported in the current software version.
Description	User role description.
VLAN policy	VLAN policy of the user role: • **deny**—Denies access to any VLANs except for permitted VLANs. • **permit (default)**—Default VLAN policy, which enables the user role to access all VLANs.
Permitted VLANs	VLANs accessible to the user role.

Field	Description
Interface policy	Interface policy of the user role: • **deny**—Denies access to any interfaces except for permitted interfaces. • **permit (default)**—Default interface policy, which enables the user role to access all interfaces.
Permitted interfaces	Interfaces accessible to the user role.
VPN instance policy	VPN instance policy of the user role: • **deny**—Denies access to any VPN instances except for permitted VPN instances. • **permit (default)**—Default VPN instance policy, which enables the user role to access all VPN instances.
Permitted VPN instances	VPN instances accessible to the user role.
Rule	User role rule number. Predefined user role rules are identified by sys-*n*, where *n* represents an integer.
Perm	Access control type: • **permit**—User role has access to the items in the **Entity** field. • **deny**—User role does not have access to the items in the **Entity** field.
Type	Controlled type: • **R**—Read-only. • **W**—Write. • **X**—Execute.
Scope	Rule control scope: • **command**—Controls access to the command or commands, as specified in the **Entity** field. • **feature**—Controls access to the commands of the feature, as specified in the **Entity** field. • **feature-group**—Controls access to the commands of the features in the feature group, as specified in the **Entity** field. • **web-menu**—Controls access to Web menus. This rule control scope is not supported in the current software version. • **xml-element**—Controls access to XML elements. • **oid**—Controls access to MIB nodes.
Entity	Command string, feature name, feature group, XML element, or OID specified in the user role rule: • An en dash (–) represents any feature. • An asterisk (*) represents zero or more characters.

Related commands

`role`

display role feature

Use **`display role feature`** to display features available in the system.

Syntax

`display role feature` [**`name`** *`feature-name`* | **`verbose`**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *feature-name*: Specifies a feature by feature name. The *feature-name* argument represents the feature name, and all letters must be in lower case.

verbose: Displays the commands of each feature.

Usage guidelines

If you do not specify any parameters, the command displays only the list of features available in the system.

Examples

Display the list of feature names.

```
<Sysname> display role feature
Feature: device          (Device configuration related commands)
Feature: interface       (Interface related commands)
Feature: syslog          (Syslog related commands)
...
```

Display the commands of each feature.

```
<Sysname> display role feature verbose
Feature: device          (Device configuration related commands)
  display clock    (R)
  debugging dev    (W)
  display debugging dev    (R)
  display device *    (R)
  display diagnostic-information *    (R)
  display environment *    (R)
  display fan *    (R)
  display alarm *    (R)
  display power *    (R)
  display system-working-mode    (R)
  display hardware-resource *    (R)
  display current-configuration *    (R)
  display saved-configuration *    (R)
  display default-configuration *    (R)
  display startup    (R)
  display this *    (R)
...
```

Display the commands of feature **aaa**.

```
<Sysname> display role feature name aaa
Feature: aaa             (AAA related commands)
  system-view ; domain *    (W)
  system-view ; header *    (W)
  system-view ; aaa *    (W)
```

```
  system-view ; ita *    (W)
  system-view ; probe ; display system internal aaa *    (R)
  display domain *    (R)
  display aaa *    (R)
  system-view ; user-group *    (W)
  system-view ; local-user *    (W)
  display local-user *    (R)
  display user-group *    (R)
  display debugging local-server    (R)
  debugging local-server *    (W)
  super *    (X)
...
```

Table 5 Command output (display role feature name aaa)

Field	Description
Feature	Displays the name and brief function description of the feature.
system-view ; domain *	All commands that start with the **domain** keyword in system view, and all commands in ISP domain view.
system-view ; header *	All commands that start with the **header** keyword in system view.
system-view ; aaa *	All commands that start with the **aaa** keyword in system view.
system-view ; ita *	This field is not supported in the current software version. All commands that start with the **ita** keyword in system view.
display domain *	All commands that start with the **display domain** keywords in user view.
system-view ; user-group *	All commands that start with the **user-group** keyword in system view, and all commands in user group view.
system-view ; local-user *	All commands that start with the **local-user** keyword in system view, and all commands in local user view.
display user-group *	All commands that start with the **display user-group** keywords in user view.
display debugging local-server	All commands that start with the **display debugging local-server** keywords in user view.
debugging local-server *	All commands that start with the **debugging local-server** keywords in user view.
super *	All commands that start with the **super** keyword in user view.
display password-control *	All commands that start with the **display password-control** keywords in user view.
reset password-control *	All commands that start with the **reset password-control** keywords in user view.
system-view ; password-control *	All commands that start with the **password-control** keyword in system view.
(W)	Command type is Write. A write command configures the system.
(R)	Command type is Read. A read command displays configuration or maintenance information.

Field	Description
(X)	Command type is Execute. An execute command executes a specific function.

Related commands

feature

display role feature-group

Use **display role feature-group** to display feature group information.

Syntax

display role feature-group [**name** *feature-group-name*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *feature-group-name*: Specifies a feature group. The *feature-group-name* argument represents the feature group name, a case-sensitive string of 1 to 31 characters. If you do not specify a feature group, the command displays information about all feature groups.

verbose: Displays the commands of each feature in feature groups. If you do not specify this keyword, the command displays only the feature lists of feature groups.

Usage guidelines

Feature groups **L2** and **L3** are predefined feature groups.

Examples

Display the feature lists of feature groups.

```
<Sysname> display role feature-group
Feature group: L2
Feature: igmp-snooping   (IGMP-Snooping related commands)
Feature: mld-snooping    (MLD-Snooping related commands)
Feature: lacp            (LACP related commands)
Feature: stp             (STP related commands)
Feature: lldp            (LLDP related commands)
Feature: dldp            (DLDP related commands)
Feature: cfm             (CFM related commands)
Feature: eoam            (EOAM related commands)
Feature: smart-link      (Smart-link related commands)
Feature: monitor-link    (Monitor-link related commands)
Feature: loopbk-detect   (Loopback-detection related commands)
Feature: vlan            (Virtual LAN related commands)
Feature: mvrp            (MVRP related commands )
Feature: rrpp            (RRPP related commands)
Feature: erps            (ERPS related commands)
```

```
Feature: ptp             (PTP related commands)
Feature: ofp             (OFP related commands)
Feature: port-security   (Port-security related commands)
Feature: macsec          (MACSEC related commands)
Feature: l2pt            (L2PT related commands)
Feature: drni            (DRNI related commands)

Feature group: L3
Feature: route           (Route management related commands)
Feature: staticrt        (Unicast static route related commands)
Feature: ospf            (Open Shortest Path First protocol related commands)
Feature: rip             (Routing Information Protocol related commands)
Feature: isis            (ISIS protocol related commands)
Feature: lisp            (LISP protocol related commands)
Feature: bgp             (Border Gateway Protocol related commands)
Feature: l3vpn           (Layer 3 Virtual Private Network related commands)
Feature: route-policy    (Routing Policy related commands)
Feature: mt              (Multiple-topology related commands)
Feature: multicast       (Multicast related commands)
Feature: pim             (Protocol Independent Multicast related commands)
Feature: igmp            (Internet Group Management Protocol related commands)
Feature: mld             (Multicast Listener Discovery related commands)
Feature: mcast-domain    (Multicast VPN related commands)
Feature: msdp            (Multicast Source Discovery Protocol related commands)
```

Display the commands in each feature group. For more information about the wildcards and marks used in the command list, see Table 5.

```
<Sysname> display role feature-group verbose
Feature group: L2
Feature: igmp-snooping   (IGMP-Snooping related commands)
  system-view ; igmp-snooping *    (W)
  system-view ; multicast-vlan *    (W)
  system-view ; user-profile * ; igmp-snooping *    (W)
  system-view ; vlan * ; igmp-snooping *    (W)
  system-view ; vlan * ; pim-snooping *    (W)
  system-view ; vsi * ; igmp-snooping *    (W)
  system-view ; vsi * ; pim-snooping *    (W)
  system-view ; interface * ; igmp-snooping *    (W)
  system-view ; interface * ; port multicast-vlan *    (W)
  display igmp-snooping *    (R)
  display pim-snooping *    (R)
  display multicast-vlan *    (R)
  display l2-multicast *    (R)
  system-view ; probe ; display system internal l2-multicast *    (R)
  system-view ; probe ; display system internal multicast-vlan *    (R)
  reset igmp-snooping *    (W)
  reset pim-snooping *    (W)
  reset multicast-vlan *    (W)
  reset l2-multicast *    (W)
```

```
  debugging igmp-snooping *    (W)
  display debugging igmp-snooping *    (R)
  system-view ; probe ; debugging system internal igmp-snooping *    (W)
Feature: mld-snooping    (MLD-Snooping related commands)
  system-view ; mld-snooping *    (W)
  system-view ; ipv6 multicast-vlan *    (W)
  system-view ; user-profile * ; mld-snooping *    (W)
  system-view ; vlan * ; mld-snooping *    (W)
  system-view ; vlan * ; ipv6 pim-snooping *    (W)
  system-view ; vsi * ; mld-snooping *    (W)
  system-view ; vsi * ; ipv6 pim-snooping *    (W)
  system-view ; interface * ; mld-snooping *    (W)
  system-view ; interface * ; ipv6 port multicast-vlan *    (W)
  display mld-snooping *    (R)
...
```

Display the feature list of the **L3** feature group.

```
<Sysname> display role feature-group name L3
Feature group: L3
Feature: route           (Route management related commands)
Feature: staticrt        (Unicast static route related commands)
Feature: ospf            (Open Shortest Path First protocol related commands)
Feature: rip             (Routing Information Protocol related commands)
Feature: isis            (ISIS protocol related commands)
Feature: lisp            (LISP protocol related commands)
Feature: bgp             (Border Gateway Protocol related commands)
Feature: l3vpn           (Layer 3 Virtual Private Network related commands)
Feature: route-policy    (Routing Policy related commands)
Feature: mt              (Multiple-topology related commands)
Feature: multicast       (Multicast related commands)
Feature: pim             (Protocol Independent Multicast related commands)
Feature: igmp            (Internet Group Management Protocol related commands)
Feature: mld             (Multicast Listener Discovery related commands)
Feature: mcast-domain    (Multicast VPN related commands)
Feature: msdp            (Multicast Source Discovery Protocol related commands)
```

Related commands

feature

role feature-group

feature

Use **feature** to add a feature to a feature group.

Use **undo feature** to remove a feature from a feature group.

Syntax

feature *feature-name*

undo feature *feature-name*

Default

A user-defined feature group does not have any features.

Views

Feature group view

Predefined user roles

network-admin

Parameters

feature-name: Specifies a feature name. You must enter the feature name in lower case.

Usage guidelines

Repeat the **feature** command to add multiple features to a feature group.

Examples

Add the AAA and ACL features to feature group **security-features**.

```
<Sysname> system-view
[Sysname] role feature-group name security-features
[Sysname-featuregrp-security-features] feature aaa
[Sysname-featuregrp-security-features] feature acl
```

Related commands

display role feature

display role feature-group

role feature-group

interface policy deny

Use **interface policy deny** to enter user role interface policy view.

Use **undo interface policy deny** to restore the default.

Syntax

interface policy deny

undo interface policy deny

Default

A user role has access to all interfaces.

Views

User role view

Predefined user roles

network-admin

Usage guidelines

To restrict the interface access of a user role to a set of interfaces, perform the following tasks:

1. Use **interface policy deny** to enter user role interface policy view.
2. Use **permit interface** to specify accessible interfaces.

NOTE:

The **interface policy deny** command denies the access of the user role to any interfaces if the **permit interface** command is not configured.

To configure an interface, make sure the interface is permitted by the user role interface policy in use. You can perform the following tasks on an accessible interface:

- Create, remove, or configure the interface.
- Enter interface view.
- Specify the interface in feature commands.

The create and remove operations are available only for logical interfaces.

Any change to a user role interface policy takes effect only on users who log in with the user role after the change.

Examples

Enter user role interface policy view of **role1**, and deny **role1** to access any interfaces.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] interface policy deny
[Sysname-role-role1-ifpolicy] quit
```

Enter user role interface policy view of **role1**, and deny **role1** to access any interfaces except for Twenty-FiveGigE 1/0/1 to Twenty-FiveGigE 1/0/4.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] interface policy deny
[Sysname-role-role1-ifpolicy] permit interface twenty-fivegige 1/0/1 to twenty-fivegige
1/0/4
```

Related commands

display role

permit interface

role

permit interface

Use **permit interface** to configure a list of interfaces accessible to a user role.

Use **undo permit interface** to disable the access of a user role to specific interfaces.

Syntax

permit interface *interface-list*

undo permit interface [*interface-list*]

Default

No permitted interfaces are configured in user role interface policy view.

Views

User role interface policy view

Predefined user roles

network-admin

Parameters

interface-list: Specifies a space-separated list of up to 10 interface items. Each interface item specifies one interface in the *interface-type interface-number* form or a range of interfaces in the *interface-type interface-number* **to** *interface-type interface-number* form. If you specify an interface range, the end interface must meet the following requirements:

- Be the same type as the start interface.
- Have a higher interface number than the start interface.

Usage guidelines

To permit a user role to access an interface after you configure the **interface policy deny** command, you must add the interface to the permitted interface list of the policy. With the user role, you can perform the following tasks to the interfaces in the permitted interface list:

- Create, remove, or configure the interfaces.
- Enter the interface views.
- Specify the interfaces in feature commands.

The create and remove operations are available only for logical interfaces.

You can repeat the **permit interface** command to add multiple permitted interfaces to a user role interface policy.

The **undo permit interface** command removes the entire list of permitted interfaces if you do not specify an interface.

Any change to a user role interface policy takes effect only on users who log in with the user role after the change.

Examples

1. Configure user role **role1**:

Permit user role **role1** to execute all commands available in interface view and VLAN view.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] rule 1 permit command system-view ; interface *
[Sysname-role-role1] rule 2 permit command system-view ; vlan *
```

Permit the user role to access Twenty-FiveGigE 1/0/1, and Twenty-FiveGigE 1/0/3 to Twenty-FiveGigE 1/0/5.

```
[Sysname-role-role1] interface policy deny
[Sysname-role-role1-ifpolicy] permit interface twenty-fivegige 1/0/1
twenty-fivegige 1/0/3 to twenty-fivegige 1/0/5
[Sysname-role-role1-ifpolicy] quit
[Sysname-role-role1] quit
```

2. Verify that you cannot use user role **role1** to work on any interfaces except for Twenty-FiveGigE 1/0/1 and Twenty-FiveGigE 1/0/3 to Twenty-FiveGigE 1/0/5:

Verify that you can enter Twenty-FiveGigE 1/0/1 interface view.

```
[Sysname] interface twenty-fivegige 1/0/1
[Sysname-Twenty-FiveGigE1/0/1] quit
```

Verify that you can assign Twenty-FiveGigE 1/0/5 to VLAN 10. In this example, the user role can access all VLANs because the default VLAN policy of the user role is used.

```
[Sysname] vlan 10
[Sysname-vlan10] port twenty-fivegige 1/0/5
[Sysname-vlan10] quit
```

Verify that you cannot enter interface view of Twenty-FiveGigE 1/0/2.

```
[Sysname] interface twenty-fivegige 1/0/2
Permission denied.
```

Related commands

display role

interface policy deny

role

permit vlan

Use **permit vlan** to configure a list of VLANs accessible to a user role.

Use **undo permit vlan** to remove the permission for a user role to access specific VLANs.

Syntax

permit vlan *vlan-id-list*

undo permit vlan [*vlan-id-list*]

Default

No permitted VLANs are configured in user role VLAN policy view.

Views

User role VLAN policy view

Predefined user roles

network-admin

Parameters

vlan-id-list: Specifies a space-separated list of up to 10 VLAN items. Each VLAN item specifies a VLAN by VLAN ID or specifies a range of VLANs in the form of *vlan-id1* **to** *vlan-id2*. The value range for the VLAN IDs is 1 to 4094. If you specify a VLAN range, the value for the *vlan-id2* argument must be greater than the value for the *vlan-id1* argument.

Usage guidelines

To permit a user role to access a VLAN after you configure the **vlan policy deny** command, you must add the VLAN to the permitted VLAN list of the policy. With the user role, you can perform the following tasks on the VLANs in the permitted VLAN list:

- Create, remove, or configure the VLANs.
- Enter the VLAN views.
- Specify the VLANs in feature commands.

You can repeat the **permit vlan** command to add multiple permitted VLANs to a user role VLAN policy.

The **undo permit vlan** command removes the entire list of permitted VLANs if you do not specify a VLAN.

Any change to a user role VLAN policy takes effect only on users who log in with the user role after the change.

By default, all access ports belong to VLAN 1. To assign an access port to any other VLAN by using the **port access vlan** command, make sure you have a user role that can access both VLAN 1 and the new VLAN.

Examples

1. Configure user role **role1**:

   # Permit user role **role1** to execute all commands available in interface view and VLAN view.

   ```
   <Sysname> system-view
   [Sysname] role name role1
   [Sysname-role-role1] rule 1 permit command system-view ; interface *
   [Sysname-role-role1] rule 2 permit command system-view ; vlan *
   ```

   # Permit user role **role1** to access VLANs 1, 2, 4, and 50 to 100.

   ```
   [Sysname-role-role1] vlan policy deny
   [Sysname-role-role1-vlanpolicy] permit vlan 1 2 4 50 to 100
   [Sysname-role-role1-vlanpolicy] quit
   [Sysname-role-role1] quit
   ```

2. Verify that you cannot use user role **role1** to work on any VLANs except for VLANs 1, 2, 4, and 50 to 100:

   # Verify that you can create VLAN 100 and enter VLAN view.

   ```
   [Sysname] vlan 100
   [Sysname-vlan100] quit
   ```

   # Verify that you can add Twenty-FiveGigE 1/0/1 to VLAN 100 as an access port.

   ```
   [Sysname] interface twenty-fivegige 1/0/1
   [Sysname-Twenty-FiveGigE1/0/1] port access vlan 100
   [Sysname-Twenty-FiveGigE1/0/1] quit
   ```

   # Verify that you cannot create VLAN 101 or enter VLAN view.

   ```
   [Sysname] vlan 101
   Permission denied.
   ```

Related commands

display role

role

vlan policy deny

permit vpn-instance

Use **permit vpn-instance** to configure a list of MPLS L3VPN instances accessible to a user role.

Use **undo permit vpn-instance** to disable the access of a user role to specific MPLS L3VPN instances.

Syntax

permit vpn-instance *vpn-instance-name*&<1-10>

undo permit vpn-instance [*vpn-instance-name*&<1-10>]

Default

No permitted VPN instances are configured in user role VPN instance policy.

Views

User role VPN instance policy view

Predefined user roles

network-admin

Parameters

vpn-instance-name&<1-10>: Specifies a space-separated list of up to 10 MPLS L3VPN instance names. Each name is a case-sensitive string of 1 to 31 characters.

Usage guidelines

To permit a user role to access a VPN instance after you configure the **vpn-instance policy deny** command, you must add the VPN instance to the permitted VPN instance list of the policy. With the user role, you can perform the following tasks on the VPN instances in the permitted VPN instance list:

- Create, remove, or configure the VPN instances.
- Enter the VPN instance views.
- Specify the VPN instances in feature commands.

You can repeat the **permit vpn-instance** command to add multiple permitted VPN instances to a user role VPN instance policy.

The **undo permit vpn-instance** command removes the entire list of permitted VPN instances if you do not specify a VPN instance.

Any change to a user role VPN instance policy takes effect only on users who log in with the user role after the change.

Examples

1. Configure user role **role1**:

Permit the user role to execute all commands available in system view and in the child views of system view.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] rule 1 permit command system-view ; *
```

Permit the user role to access VPN instance **vpn1**.

```
[Sysname-role-role1] vpn policy deny
[Sysname-role-role1-vpnpolicy] permit vpn-instance vpn1
[Sysname-role-role1-vpnpolicy] quit
[Sysname-role-role1] quit
```

2. Verify that you cannot use user role **role1** to work on any VPN instances except for **vpn1**:

Verify that you can enter the view of **vpn1**.

```
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] quit
```

Verify that you can specify the primary accounting server at 10.110.1.2 in VPN instance **vpn1** for RADIUS scheme **radius1**.

```
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary accounting 10.110.1.2 vpn-instance vpn1
[Sysname-radius-radius1] quit
```

Verify that you cannot create VPN instance **vpn2** or enter VPN instance view.

```
[Sysname] ip vpn-instance vpn2
Permission denied.
```

Related commands

display role

role

vpn-instance policy deny

role

Use **role** to create a user role and enter its view, or enter the view of an existing user role.

Use **undo role** to delete a user role.

Syntax

role name *role-name*

undo role name *role-name*

Default

The system has the following predefined user roles: network-admin, network-operator, level-*n* (where *n* represents an integer in the range of 0 to 15), and security-audit.

Views

System view

Predefined user roles

network-admin

Parameters

name *role-name*: Specifies a username. The *role-name* argument is a case-sensitive string of 1 to 63 characters.

Usage guidelines

You can create a maximum of 64 user roles in addition to the predefined user roles.

You cannot delete the predefined user roles or change the permissions assigned to network-admin, network-operator, level-15, or security-audit.

You cannot assign the security-audit user role to non-AAA authentication users.

The access permissions of the level-0 to level-14 user roles can be modified through user role rules and resource access policies. However, you cannot make changes on the predefined access permissions of these user roles. For example, you cannot change the access permission of these user roles to the **display history-command all** command.

Examples

Create user role **role1** and enter its view.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1]
```

Related commands

display role

interface policy deny

rule

vlan policy deny

vpn-instance policy deny

role default-role enable

Use **role default-role enable** to enable the default user role feature for remote AAA users.

Use **undo role default-role enable** to restore the default.

Syntax

role default-role enable [*role-name*]

undo role default-role enable

Default

The default user role feature is disabled. AAA users who do not have a user role cannot log in to the device.

Views

System view

Predefined user roles

network-admin

Parameters

role-name: Specifies a user role by its name for the default user role. The user role must already exist. The argument is a case-sensitive string of 1 to 63 characters. If you do not specify the *role-name* argument, the default user role is network-operator.

Usage guidelines

The default user role feature assigns the default user role to AAA-authenticated users if the authentication server (local or remote) does not assign any user roles to the users. These users are allowed to access the system with the default user role.

For local authorization, this command is required if you do not use the **authorization-attribute user role** command to assign user roles to local users.

If AAA users have been assigned user roles, they log in with the user roles.

Examples

Enable the default user role feature.

```
<Sysname> system-view
[Sysname] role default-role enable
```

Related commands

role

role feature-group

Use **role feature-group** to create a user role feature group and enter its view, or enter the view of an existing user role feature group.

Use **undo role feature-group** to delete a user role feature group.

Syntax

role feature-group name *feature-group-name*

undo role feature-group name *feature-group-name*

Default

Two user role feature groups **L2** and **L3** exist.

Views

System view

Predefined user roles

network-admin

Parameters

name *feature-group-name*: Specifies a feature group name. The *feature-group-name* argument is a case-sensitive string of 1 to 31 characters.

Usage guidelines

The **L2** feature group includes all Layer 2 feature commands, and the **L3** feature group includes all Layer 3 feature commands. These predefined feature groups are not user configurable.

In addition to the predefined feature groups **L2** and **L3**, you can create a maximum of 64 user role feature groups.

Examples

Create feature group **security-features** and enter its view.

```
<Sysname> system-view
[Sysname] role feature-group name security-features
[Sysname-featuregrp-security-features]
```

Related commands

display role feature

display role feature-group

feature

rule

Use **rule** to create or change a user role rule.

Use **undo rule** to delete user role rules.

Syntax

rule *number* { **deny** | **permit** } { **command** *command-string* | { **execute** | **read** | **write** } * { **feature** [*feature-name*] | **feature-group** *feature-group-name* | **oid** *oid-string* | **xml-element** [*xml-string*] } }

undo rule { *number* | **all** }

Default

A user-defined user role does not have any rules and cannot access any resources.

Views

User role view

Predefined user roles

network-admin

Parameters

number: Specifies a rule number in the range of 1 to 256.

deny: Denies access to the specified commands, XML elements, or MIB nodes.

permit: Permits access to the specified commands, XML elements, or MIB nodes.

command *command-string*: Specifies a command string. The command string can represent a command or a group of commands. The *command-string* argument is a case-sensitive string of 1 to 128 characters, including the following characters:

- The wildcard asterisk (*).
- The delimiters space and tab.

- All printable characters.

execute: Specifies the execute commands, XML elements, or MIB nodes to execute a specific function or program. The **ping** command is an example of execute commands.

read: Specifies the read commands, XML elements, or MIB nodes to display configuration or maintenance information. The **display**, **dir**, **more**, and **pwd** commands are examples of read commands.

write: Specifies the write commands, XML elements, or MIB nodes to configure the system. The **ssh server enable** command is an example of write commands.

feature [*feature-name*]: Specifies one or all features. The *feature-name* argument is a case-sensitive character string. If you do not specify a feature name, you specify all the features in the system.

feature-group *feature-group-name*: Specifies a user-defined or predefined feature group. The *feature-group-name* argument represents the feature group name, a case-sensitive string of 1 to 31 characters. If the feature group has not been created, the rule takes effect after the group is created. To display the feature groups that have been created, use the **display role feature-group** command.

oid *oid-string*: Specifies an OID of a MIB node. The *oid-string* argument represents the OID, a case-insensitive string of 1 to 255 characters. The OID is a dotted numeric string that uniquely identifies the path from the root node to this node. For example, 1.3.6.1.4.1.25506.8.35.14.19.1.1.

xml-element [*xml-string*]: Specifies an XML element. The *xml-string* argument represents the XPath of the XML element, a case-insensitive string of 1 to 255 characters. Use the forward slash (/) to separate Xpath items, for example, Interfaces/Index/Name. If you do not specify an XML element, the rule applies to all XML elements.

all: Specifies all the user role rules.

Usage guidelines

You can define the following types of rules for different access control granularities:

- **Command rule**—Controls access to a command or a set of commands that match a regular expression.
- **Feature rule**—Controls access to the commands of a feature by command type.
- **Feature group rule**—Controls access to the commands of a group of features by command type.
- **XML element rule**—Controls access to XML elements by element type.
- **OID rule**—Controls access to the specified MIB node and its child nodes by node type.

A user role can access the set of permitted resources specified in the user role rules. User role rules include predefined (identified by sys-n) and user-defined user role rules.

You can configure a maximum of 256 user-defined rules for a user role. The total number of user-defined user role rules cannot exceed 1024.

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

Access to the file system commands is controlled by both the file system command rules and the file system feature rule.

A command with output redirection to the file system is permitted only when the command type write is assigned to the file system feature.

The following guidelines apply to non-OID rules:

- If two user-defined rules of the same type conflict, the rule with the higher ID takes effect. For example, a user role can use the **tracert** command but not the **ping** command if the user role contains rules configured by using the following commands:

    - **rule** *1* **permit command** *ping*
    - **rule** *2* **permit command** *tracert*
    - **rule** *3* **deny command** *ping*
- If a predefined user role rule and a user-defined user role rule conflict, the user-defined user role rule takes effect.

The following guidelines apply to OID rules:

- The system compares an OID with the OIDs specified in rules, and it uses the longest match principle to select a rule for the OID. For example, a user role cannot access the MIB node with OID 1.3.6.1.4.1.25506.141.3.0.1 if the user role contains rules configured by using the following commands:
    - **rule** *1* **permit read write oid** *1.3.6*
    - **rule** *2* **deny read write oid** *1.3.6.1.4.1*
    - **rule** *3* **permit read write oid** *1.3.6.1.4*
- If the same OID is specified in multiple rules, the rule with the higher ID takes effect. For example, a user role can access the MIB node with OID 1.3.6.1.4.1.25506.141.3.0.1 if the user role contains rules configured by using the following commands:
    - **rule** *1* **permit read write oid** *1.3.6*
    - **rule** *2* **deny read write oid** *1.3.6.1.4.1*
    - **rule** *3* **permit read write oid** *1.3.6.1.4.1*

When you specify a command string, follow the guidelines in Table 6.

Table 6 Command string configuration rules

Rule	Guidelines
Semicolon (;) is the delimiter.	Use a semicolon to separate the command of each view that you must enter before you access a command or a set of commands. However, do not use a semicolon to separate commands available in user view or any view, for example, **display** and **dir**. Each semicolon-separated segment must have a minimum of one printable character. To specify the commands in a view but not the commands in the view's subviews, use a semicolon as the last printable character in the last segment. To specify the commands in a view and the view's subviews, the last printable character in the last segment must not be a semicolon. For example, you must enter system view before you enter interface view. To specify all commands starting with the **ip** keyword in any interface view, you must use the "system ; interface * ; ip * ;" command string. For another example, the "system ; radius scheme * ;" command string represents all commands that start with the **radius scheme** keywords in system view. The "system ; radius scheme *" command string represents all commands that start with the **radius scheme** keywords in system view and all commands in RADIUS scheme view.

Rule	Guidelines
Asterisk (*) is the wildcard.	An asterisk represents zero or multiple characters. In a non-last segment, you can use an asterisk only at the end of the segment. In the last segment, you can use an asterisk in any position of the segment. If the asterisk appears at the beginning, you cannot specify a printable character behind the asterisk. For example, the "system ; *" command string represents all commands available in system view and all subviews of the system view. The "debugging * event" command string represents all event debugging commands available in user view.
Keyword abbreviation is allowed.	You can specify a keyword by entering the first few characters of the keyword. Any command that starts with this character string matches the rule. For example, "rule 1 deny command dis arp source *" denies access to the commands **display arp source-mac interface** and **display arp source-suppression**.
To control the access to a command, you must specify the command immediately after the view that has the command.	To control access to a command, you must specify the command immediately behind the view to which the command is assigned. The rules that control command access for any subview do not apply to the command. For example, the "rule 1 deny command system ; interface * ; *" command string disables access to any command that is assigned to interface view. However, you can still execute the **acl advanced** command in interface view, because this command is assigned to system view rather than interface view. To disable access to this command, use "rule 1 deny command system ; acl *;".
Do not include the vertical bar (|), greater-than sign (>), or double greater-than sign (>>) when you specify **display** commands in a user role command rule.	The system does not treat the redirect signs and the parameters that follow the signs as part of command lines. However, in user role command rules, these redirect signs and parameters are handled as part of command lines. As a result, no rule that includes any of these signs can find a match. For example, "rule 1 permit command display debugging > log" can never find a match. This is because the system has a **display debugging** command but not a **display debugging > log** command.

Examples

Permit user role **role1** to execute the **display acl** command.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] rule 1 permit command display acl
```

Permit user role **role1** to execute all commands that start with the **display** keyword.

```
[Sysname-role-role1] rule 2 permit command display *
```

Permit user role **role1** to execute the **radius scheme aaa** command in system view and use all commands assigned to RADIUS scheme view.

```
[Sysname-role-role1] rule 3 permit command system ; radius scheme aaa
```

Deny the access of **role1** to the read or write commands of any features.

```
[Sysname-role-role1] rule 4 deny read write feature
```

Deny the access of **role1** to the read commands of the **aaa** feature.

```
[Sysname-role-role1] rule 5 deny read feature aaa
```

Permit **role1** to access all read, write, and execute commands of feature group **security-features**.

```
[Sysname-role-role1] rule 6 permit read write execute feature-group security-features
```

Permit **role1** to access all read and write MIB nodes starting from the node with OID 1.1.2.

```
[Sysname-role-role1] rule 7 permit read write oid 1.1.2
```

Related commands

display role

display role feature

display role feature-group

role

super

Use **super** to obtain another user role without reconnecting to the device.

Syntax

super [*role-name*]

Views

User view

Predefined user roles

network-admin

Parameters

role-name: Specifies a user role, a case-sensitive string of 1 to 63 characters. The user role must exist in the system and cannot be security-audit. If you do not specify a user role, you obtain the default target user role which is set by using the **super default role** command.

Usage guidelines

The obtained user role is a temporary user role, because this command is effective only on the current login. The next time you are logged in with the user account, the original user role settings take effect.

To enable a user to obtain another user role without reconnecting to the device, you must configure user role authentication.

- If no local password is configured in the local password authentication (**local**), an AUX user can obtain the user role by either entering a string or not entering anything.
- If no local password is configured in the local-then-remote authentication (**local scheme**), the following rules apply:
  - A VTY user performs remote authentication.
  - An AUX user can obtain user role authorization by either entering a string or not entering anything.

Examples

Obtain the user role network-operator.

```
<Sysname> super network-operator
Password:
User privilege role is network-operator, and only those commands that authorized to the role can be used.
```

Related commands

authentication super (*Security Command Reference*)

super authentication-mode

super password

super authentication-mode

Use **super authentication-mode** to set an authentication mode for temporary user role authorization.

Use **undo super authentication-mode** to restore the default.

Syntax

super authentication-mode { **local** | **scheme** } *

undo super authentication-mode

Default

Local password authentication applies.

Views

System view

Predefined user roles

network-admin

Parameters

local: Enables local password authentication.

scheme: Enables remote AAA authentication.

Usage guidelines

For local password authentication, use the **super password** command to set a password.

For remote AAA authentication, set the username and password on the RADIUS or HWTACACS server.

If you specify both **local** and **scheme** keywords, the keyword first entered in the command takes precedence.

- **scheme local**—Enables remote-then-local authentication mode. The device first performs AAA authentication to obtain a temporary user role. Local password authentication is performed if the remote HWTACACS or RADIUS server does not respond, or if the AAA configuration on the device is invalid.
- **local scheme**—Enables local-then-remote authentication mode. The device first performs local password authentication. If no password is configured for the user role, the device performs remote authentication for VTY users. An AUX user can obtain another user role by either entering a string or not entering anything.

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

Examples

Enable local-only authentication for temporary user role authorization.

```
<Sysname> system-view
[Sysname] super authentication-mode local
```

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

```
<Sysname> system-view
[Sysname] super authentication-mode scheme local
```

Related commands

authentication super (*Security Command Reference*)

super password

super default role

Use **super default role** to specify the default target user role for temporary user role authorization.

Use **undo super default role** to restore the default.

Syntax

super default role *role-name*

undo super default role

Default

The default target user role is network-admin.

Views

System view

Predefined user roles

network-admin

Parameters

role-name: Specifies the name of the default target user role, a case-sensitive string of 1 to 63 characters. The user role must exist in the system and cannot be security-audit.

Usage guidelines

The default target user role is applied to the **super** or **super password** command when you do not specify a user role for the command.

Examples

Specify **network-operator** as the default target user role for temporary user role authorization.

```
<Sysname> system-view
[Sysname] super default role network-operator
```

Related commands

super

super password

super password

Use **super password** to set a password for a user role.

Use **undo super password** to delete the password for a user role.

Syntax

In non-FIPS mode:

super password [**role** *role-name*] [{ **hash** | **simple** } *string*]

undo super password [**role** *role-name*]

In FIPS mode:

super password [**role** *role-name*]

undo super password [**role** *role-name*]

Default

No password is set for a user role.

Views

System view

Predefined user roles

network-admin

Parameters

role *role-name*: Specifies a user role, a case-sensitive string of 1 to 63 characters. The user role must exist in the system and cannot be security-audit. If you do not specify a user role, the command sets a password for the default target user role which is set by using the **super default role** command.

hash: Specifies a password in hashed form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in hashed form.

string: Specifies the password. In non-FIPS mode, the plaintext form of the password is a case-sensitive string of 1 to 63 characters. The hashed form of the password is a case-sensitive string of 1 to 110 characters. In FIPS mode, the password must be a case-sensitive plaintext string of 15 to 63 characters. The string must contain four character types including digits, uppercase letters, lowercase letters, and special characters.

Usage guidelines

If you do not specify any parameters, you specify a plaintext password in the interactive mode.

The FIPS mode supports only the interactive mode for setting a password.

Set a password if you configure local password authentication for temporary user role authorization.

It is a good practice to specify different passwords for different user roles.

When the global password control feature is enabled, all history super passwords are stored in hashed form.

- If you set a new super password in plaintext form, make sure the new super password is different from the current one and those stored in the history super password records.
- If you set a new super password in hashed form, the system does not compare the new super password with the current one or those stored in the history super password records.

Examples

Set the password to **123456TESTplat&!** in plaintext form for user role network-operator.

```
<Sysname> system-view
[Sysname] super password role network-operator simple 123456TESTplat&!
```

Set the password to **123456TESTplat&!** in the interactive mode for user role network-operator.

```
<Sysname> system-view
[Sysname] super password role network-operator
Password:
Confirm :
Updating user information. Please wait... ...
```

Related commands

super authentication-mode

super default role

super use-login-username

Use **super use-login-username** to enable the device to automatically obtain the login username when a login user requests temporary user role authorization from a remote authentication server.

Use **undo super use-login-username** to restore the default.

Syntax

super use-login-username

undo super use-login-username

Default

The device prompts for a username when a login user requests temporary user role authorization from a remote authentication server.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command is applicable only to the login from a user line that uses scheme authentication, which requires a username for login.

If the user was logged in from a user line that uses password authentication or no authentication, the device cannot obtain the login username. The request for temporary user role authorization from a remote authentication server will fail.

This command does not take effect on local password authentication for temporary user role authorization.

Examples

Enable the device to automatically obtain the login username when a login user requests temporary user role authorization from a remote authentication server.

```
<Sysname> system-view
[Sysname] super use-login-username
```

Related commands

authentication super (*Security Command Reference*)

super authentication-mode

super password

vlan policy deny

Use **vlan policy deny** to enter user role VLAN policy view.

Use **undo vlan policy deny** to restore the default.

Syntax

vlan policy deny

undo vlan policy deny

Default

A user role has access to all VLANs.

Views

User role view

Predefined user roles

network-admin

Usage guidelines

To restrict the VLAN access of a user role to a set of VLANs, perform the following tasks:

1. Use **vlan policy deny** to enter user role VLAN policy view.
2. Use **permit vlan** to specify accessible VLANs.

NOTE:

The **vlan policy deny** command denies the access of the user role to any VLANs if the **permit vlan** command is not configured.

To configure a VLAN, make sure the VLAN is permitted by the user role VLAN policy in use. You can perform the following tasks on an accessible VLAN:

- Create, remove, or configure the VLAN.
- Enter VLAN view.
- Specify the VLAN in feature commands.

Any change to a user role VLAN policy takes effect only on users who log in with the user role after the change.

Examples

Enter user role VLAN policy view of **role1**, and deny the access of **role1** to any VLANs.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] vlan policy deny
[Sysname-role-role1-vlanpolicy] quit
```

Enter user role VLAN policy view of **role1**, and deny the access of **role1** to any VLANs except for VLANs 50 to 100.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] vlan policy deny
[Sysname-role-role1-vlanpolicy] permit vlan 50 to 100
```

Related commands

display role

permit vlan

role

vpn-instance policy deny

Use **vpn-instance policy deny** to enter user role VPN instance policy view.

Use **undo vpn-instance policy deny** to restore the default.

Syntax

vpn-instance policy deny

undo vpn-instance policy deny

Default

A user role has access to all VPN instances.

Views

User role view

Predefined user roles

network-admin

Usage guidelines

To restrict the VPN instance access of a user role to a set of VPN instances, perform the following tasks:

1. Use **vpn-instance policy deny** to enter user role VPN instance policy view.
2. Use **permit vpn-instance** to specify accessible VPN instances.

NOTE:

The **vpn-instance policy deny** command denies the access of the user role to any VPN instances if the **permit vpn-instance** command is not configured.

To configure a VPN instance, make sure the VPN instance is permitted by the user role VPN instance policy in use. You can perform the following tasks on an accessible VPN instance:

- Create, remove, or configure the VPN instance.
- Enter VPN instance view.
- Specify the VPN instance in feature commands.

Any change to a user role VPN instance policy takes effect only on users who log in with the user role after the change.

Examples

Enter user role VPN instance policy view of **role1**, and deny the access of **role1** to any VPN instances.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] vpn-instance policy deny
[Sysname-role-role1-vpnpolicy] quit
```

Enter user role VPN instance policy view of **role1**, and deny the access of **role1** to any VPN instances except for **vpn2**.

```
<Sysname> system-view
[Sysname] role name role1
[Sysname-role-role1] vpn-instance policy deny
[Sysname-role-role1-vpnpolicy] permit vpn-instance vpn2
```

Related commands

display role

permit vpn-instance

role

Login management commands

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

Some login management commands are available in both user line view and user line class view. For these commands, the device uses the following rules to determine the settings to be activated:

- A setting in user line view applies only to the user line. A setting in user line class view applies to all user lines of the class.
- A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.
- A setting in user line class view takes effect on login sessions that are established after the setting is configured.

activation-key

Use **activation-key** to set the terminal session activation key. Pressing this shortcut key starts a terminal session.

Use **undo activation-key** to restore the default.

Syntax

activation-key *key-string*

undo activation-key

Default

The terminal session activation key is **Enter**.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

key-string: Specifies a shortcut key. It can be a character (case sensitive), or an ASCII code value in the range of 0 to 127. For example, if you configure **activation-key 1**, the shortcut key is **Ctrl+A**. If you configure **activation-key a**, the shortcut key is **a**. For information about ASCII code values of individual characters, see the standard ASCII code chart. For information about ASCII code values of combined keys that use the **Ctrl** key, see Table 7.

Usage guidelines

This command is not supported in VTY line view or VTY line class view.

This command takes effect immediately.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

You can use only the specified terminal session activation key to start a terminal session. To display the current terminal session activation key, use the **`display current-configuration | include activation-key`** command.

Table 7 ASCII code values for combined keys that use the Ctrl key

Combined key	ASCII code value
Ctrl+A	1
Ctrl+B	2
Ctrl+C	3
Ctrl+D	4
Ctrl+E	5
Ctrl+F	6
Ctrl+G	7
Ctrl+H	8
Ctrl+I	9
Ctrl+J	10
Ctrl+K	11
Ctrl+L	12
Ctrl+M	13
Ctrl+N	14
Ctrl+O	15
Ctrl+P	16
Ctrl+Q	17
Ctrl+R	18
Ctrl+S	19
Ctrl+T	20
Ctrl+U	21
Ctrl+V	22
Ctrl+W	23
Ctrl+X	24
Ctrl+Y	25
Ctrl+Z	26
CTRL+ [	27
CTRL+\	28
CTRL+]	29
CTRL+^	30
CTRL+_	31

Examples

Configure character **s** as the terminal session activation key for AUX line 0.

```
<Sysname> system-view
[Sysname] line aux 0
[Sysname-line-aux0] activation-key s
```

To verify the configuration:

1. Exit the AUX session.

   ```
   [Sysname-line-aux0] return
   <Sysname> quit
   ```

2. Log in again through the AUX line.

   The following message appears:

   ```
   Press ENTER to get started.
   ```

3. Press **Enter**.

   Pressing **Enter** does not start a session.

4. Press **s**.

   A terminal session is started.

   ```
   <Sysname>
   ```

authentication-mode

Use **authentication-mode** to set the authentication mode for a user line.

Use **undo authentication-mode** to restore the default.

Syntax

In non-FIPS mode:

authentication-mode { **none** | **password** | **scheme** }

undo authentication-mode

In FIPS mode:

authentication-mode scheme

undo authentication-mode

Default

In non-FIPS mode:

The authentication mode is **password** for the VTY line.

The authentication mode for the AUX line is as follows:

- If the device starts up with empty configuration, authentication is disabled. To improve device security, configure password or scheme authentication for console login immediately after you log in to the device for the first time.
- If the device starts up with the factory default, scheme authentication is enabled, and the default username and password are **admin** and null, respectively. To improve device security, configure a password for console login immediately after you log in to the device for the first time.

In FIPS mode:

The authentication mode is **scheme**.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

none: Disables authentication.

password: Performs local password authentication.

scheme: Performs AAA authentication. For more information about AAA, see *Security Configuration Guide*.

Usage guidelines

Only users assigned the network-admin, or level-15 user role can execute this command. Other users cannot execute this command, even if they are granted the right to execute this command.

When the authentication mode is **none**, a user can log in without authentication. To improve device security, use the password or scheme authentication mode.

In VTY line view, this command is associated with the **protocol inbound** command.

- If the settings of the two commands in VTY line view are both the default settings, the settings for the commands in VTY line class view take effect.
- If the settings of the two commands in VTY line view are both non-default settings, the non-default settings in VTY line view take effect.
- If only one command has a non-default setting in VTY line view, the other command uses the default setting, regardless of the setting in VTY line class view.

An authentication mode change does not take effect on the current session. It takes effect on subsequent login sessions.

Examples

Enable the **none** authentication mode for VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] authentication-mode none
```

Enable password authentication for VTY line 0 and set the password to **321**.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] authentication-mode password
[Sysname-line-vty0] set authentication password simple 321
```

Enable scheme authentication for VTY line 0. Configure the local user **123** and set the password to **321**. Assign the Telnet service and the user role network-admin to the user.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] authentication-mode scheme
[Sysname-line-vty0] quit
[Sysname] local-user 123
[Sysname-luser-manage-123] password simple 321
[Sysname-luser-manage-123] service-type telnet
[Sysname-luser-manage-123] authorization-attribute user-role network-admin
```

Related commands

set authentication password

auto-execute command

Use **auto-execute command** to specify the command to be automatically executed for a login user.

Use **undo auto-execute command** to restore the default.

Syntax

auto-execute command *command*

undo auto-execute command

Default

No command is specified to be automatically executed for a login user.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

command: Specifies the command to be automatically executed.

Usage guidelines

CAUTION:

After configuring this command for a user line, you might be unable to access the CLI through the user line. Make sure you can access the CLI through a different user line before you configure this command and save the configuration.

The device will automatically execute the specified command when a user logs in through the user line, and close the user connection after the command is executed.

This command is not supported in AUX line view or AUX line class view.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

A configuration change made by this command does not take effect on the current session. It takes effect on subsequent login sessions.

Examples

Configure the device to automatically execute the **telnet 192.168.1.41** command when a user logs in through VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] auto-execute command telnet 192.168.1.41
This action will lead to configuration failure through line-vty0. Are you sure?
[Y/N]:y
[Sysname-line-vty0]
```

To verify the configuration, Telnet to the device (192.168.1.40).

The device automatically Telnets to 192.168.1.41. The following output is displayed on the configuration terminal:

```
C:\> telnet 192.168.1.40
******************************************************************************
* Copyright (c) 2010-2020 Hewlett Packard Enterprise Development LP          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************


<Sysname>
Trying 192.168.1.41 ...
Press CTRL+K to abort
Connected to 192.168.1.41 ...
******************************************************************************
* Copyright (c) 2010-2020 Hewlett Packard Enterprise Development LP          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************
<Sysname.41>
```

This operation is the same as directly logging in to the device at 192.168.1.41 through Telnet. When you close the Telnet connection to 192.168.1.41, the Telnet connection to 192.168.1.40 is closed at the same time.

command accounting

Use **command accounting** to enable command accounting.

Use **undo command accounting** to disable command accounting.

Syntax

command accounting

undo command accounting

Default

Command accounting is disabled. The accounting server does not record executed commands.

Views

User line view

User line class view

Predefined user roles

network-admin

Usage guidelines

When command accounting is enabled but command authorization is not, every executed command is recorded on the HWTACACS server. When both command accounting and command authorization are enabled, only authorized commands that are executed are recorded on the HWTACACS server.

Invalid commands are not recorded.

A configuration change made by this command does not take effect on the current session. It takes effect on subsequent login sessions.

After you configure the **command accounting** command in user line class view, you cannot configure the **undo command accounting** command in any user line views in the class.

Examples

Enable command accounting for VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] command accounting
```

Related commands

accounting command (*Security Command Reference*)

command authorization

command authorization

Use **command authorization** to enable command authorization.

Use **undo command authorization** to disable command authorization.

Syntax

command authorization

undo command authorization

Default

Command authorization is disabled. Logged-in users can execute commands without authorization.

Views

User line view

User line class view

Predefined user roles

network-admin

Usage guidelines

When command authorization is enabled, a user can only use commands that are permitted by both the AAA scheme and user role.

A configuration change made by this command does not take effect on the current session. It takes effect on subsequent login sessions.

If you configure the **command authorization** command in user line class view, command authorization is enabled for all user lines in the class. You cannot configure the **undo command authorization** command in the view of a user line in the class.

Examples

Enable command authorization for VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] command authorization
```

Related commands

authorization command (*Security Command Reference*)

command accounting

databits

Use **databits** to specify the number of data bits for a character.

Use **undo databits** to restore the default.

Syntax

databits { **7** | **8** }

undo databits

Default

Eight data bits are used for a character.

Views

User line view

Predefined user roles

network-admin

Parameters

7: Uses seven data bits for a character.

8: Uses eight data bits for a character.

Usage guidelines

This command is not supported in VTY line class view.

This setting must be the same as the setting on the configuration terminal.

Examples

Configure AUX 0 to use seven data bits for a character.

```
<Sysname> system-view
[Sysname] line aux 0
[Sysname-line-aux0] databits 7
```

display line

Use **display line** to display user line information.

Syntax

display line [*number1* | { **aux** | **vty** } *number2*] [**summary**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

number1: Specifies the absolute number of a user line. The value range is 0 to 73.

aux: Specifies the AUX line.

vty: Specifies the VTY line.

number2: Specifies the relative number of a user line. The value range is 0 to 9 for AUX lines and 0 to 63 for VTY lines.

summary: Displays summary information about user lines. If you do not specify this keyword, the command displays detailed information.

Examples

Display information about line 0.

```
<Sysname> display line 0
  Idx  Type     Tx/Rx      Modem Auth  Int        Location
F 0    AUX 0    9600       -     N     -           1/0

  +    : Line is active.
  F    : Line is active and in async mode.
  Idx  : Absolute index of line.
  Type : Type and relative index of line.
  Auth : Login authentication mode.
  Int  : Physical port of the line.
  A    : Authentication use AAA.
  N    : No authentication is required.
  P    : Password authentication.
```

Table 8 Command output

Field	Description
Modem	Whether the modem allows calling in or out. By default, this attribute is not configured and this field displays a hyphen (-). This field is not supported in the current software version.
Int	Physical port for the line. If there is no physical port for the line or the port is a console port, this field displays a hyphen (-).
Location	Physical position of the line, in the form of *slot number*/*CPU number*.

Display summary information about all user lines.

```
<Sysname> display line summary
  Line type : [AUX]
            0:XXXX XXXX XX
  Line type : [VTY]
           10:UUXX XXXX XXXX XXXX
           26:XXXX XXXX XXXX XXXX
           42:XXXX XXXX XXXX XXXX
           58:XXXX XXXX XXXX XXXX

   2 lines used.      (U)
  72 lines not used.  (X)
```

Table 9 Command output

Fields	Description
Line type	Type of the user line: • **AUX**—AUX line. • **VTY**—VTY line.
number:*status*	*number*: Absolute number of the first user line in the user line class. *status*: User line status. **X** is for unused and **U** is for used.

display telnet client

Use **display telnet client** to display the packet source setting for the Telnet client.

Syntax

display telnet client

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command displays the source IPv4 address or source interface specified for the Telnet client to use in outgoing Telnet packets, depending on the **telnet client source** command.

Examples

Display the packet source setting for the Telnet client.

```
<Sysname> display telnet client
 The source IP address is 1.1.1.1.
```

Related commands

telnet client source

display user-interface

Use **display user-interface** to display user line information.

Syntax

display user-interface [*number1* | { **aux** | **vty** } *number2*] [**summary**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

number1: Specifies the absolute number of a user line. The value range is 0 to 73.

aux: Specifies the AUX line.

vty: Specifies the VTY line.

number2: Specifies the relative number of a user line. The value range is 0 to 9 for AUX lines and 0 to 63 for VTY lines.

summary: Displays summary information about user lines. If you do not specify this keyword, the detailed information is displayed.

Usage guidelines

This command is an older version reserved for backward compatibility purposes. It has the same functionality and output as the **display line** command. As a best practice, use the **display line** command.

Examples

Display information about line 0.

```
<Sysname> display user-interface 0
  Idx  Type     Tx/Rx      Modem Auth  Int        Location
F 0    AUX 0    9600       -     N     -          1/0

  +    : Line is active.
  F    : Line is active and in async mode.
  Idx  : Absolute index of line.
  Type : Type and relative index of line.
  Auth : Login authentication mode.
  Int  : Physical port of the line.
  A    : Authentication use AAA.
  N    : No authentication is required.
  P    : Password authentication.
```

Table 10 Command output

Field	Description
Modem	Whether the modem allows calling in or out. By default, this attribute is not configured and this field displays a hyphen (-). This field is not supported in the current software version.
Int	Physical port for the line. If there is no physical port for the line or the port is a console port, this field displays a hyphen (-).
Location	Physical position of the line, in the form of *slot number*/*CPU number*.

Display summary information about all user lines.

```
<Sysname> display user-interface summary
  Line type : [AUX]
            0:XXXX XXXX XX
  Line type : [VTY]
           10:UXUX XXXX XXXX XXXX
           26:XXXX XXXX XXXX XXXX
           42:XXXX XXXX XXXX XXXX
           58:XXXX XXXX XXXX XXXX

   2 lines used.      (U)
  72 lines not used.  (X)
```

Table 11 Command output

Fields	Description
Line type	Type of the user line: • **AUX**—AUX line. • **VTY**—VTY line.
number:*status*	*number*: Absolute number of the first user line in the user line class. *status*: User line status. **X** is for unused and **U** is for used.

display users

Use **display users** to display online CLI users.

Syntax

display users [**all**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Displays all user lines supported by the device.

Examples

Display online user information.

```
<Sysname> display users
  Idx  Line     Idle       Time              Pid     Type
+ 10   VTY 0    00:00:00   Jan 01 00:33:10   484     TEL
  12   VTY 2    00:06:22   Jan 01 00:33:22   495     TEL

Following are more details.
VTY 0   :
        User role list: network-admin network-operator
        Location: 192.168.1.107
VTY 2   :
        User role list: level-0 network-admin network-operator
        Location: 192.168.1.134
 +    : Current operation user.
 F    : Current operation user works in async mode.
```

Table 12 Command output

Field	Description
Idx	Absolute number of the user line.
Line	Type and relative number of the user line.
Idle	Time elapsed after the user's most recent input, in the *hh*:*mm*:*ss* format.

Field	Description
Time	Login time of the user.
Pid	Process ID of the user session.
Type	User type: • **TEL**—Telnet user. • **SSH**—SSH user. For a user who logged in through the console port, this field does not display anything.
+	User line you are using.
User name	Username used by the user. This field is displayed only if the user provided a username and password for authentication at login.
User role list	User roles assigned to the user.
Location	IP address of the user.

escape-key

Use **escape-key** to set the escape key.

Use **undo escape-key** to disable the escape key.

Syntax

escape-key { *key-string* | **default** }

undo escape-key

Default

The escape key is **Ctrl+C**.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

key-string: Specifies a shortcut key. It can be a character (case sensitive, except for **d** and **D**), or an ASCII code value in the range of 0 to 127. For example, if you configure **escape-key 1**, the shortcut key is **Ctrl+A**. If you configure **escape-key a**, the shortcut key is **a**. If you specify the character **d** or **D** for this argument, the actual shortcut key is **Ctrl+C**. To use **d** or **D** as the shortcut key, you must specify the ASCII code value of the character for this argument. For information about ASCII code values of individual characters, see the standard ASCII code chart. For information about ASCII code values of combined keys that use the **Ctrl** key, see Table 7.

default: Restores the default escape key **Ctrl+C**.

Usage guidelines

You can press the escape key to abort a command that is being executed, for example, a **ping** or **tracert** command. Whether a command can be aborted by **Ctrl+C** by default depends on the software implementation of the command. For more information, see the usage guidelines for the command.

As a best practice, use a key sequence as the escape key. If you define a single character as the escape key, pressing the key while a command is being executed stops the command. If no command is being executed, pressing the key enters the character as a common character. If you Telnet from the device to a remote device, pressing the key enters the character as a common character on the remote device. The key acts as the escape key on the remote device only when the following conditions are met:

- You define the same character as the escape key on the remote device.
- You press the key while a command is being executed on the remote device.

The **undo escape-key** command disables the current escape key. After you execute this **undo** command, no escape key is available.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

The setting in user line view takes effect immediately on the current session. The setting in user line class view takes effect on login sessions that are established after the setting is configured.

To display the current escape key, use the **display current-configuration | include escape-key** command.

Examples

Configure character **a** as the escape key for VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] escape-key a
```

To verify the configuration:

1. Ping IP address 192.168.1.49, specifying the **-c** keyword to set the number of ICMP echo request packets to 20.

```
<Sysname> ping -c 20 192.168.1.49
  PING 192.168.1.49: 56  data bytes, press 'a' to break
    Reply from 192.168.1.49: bytes=56 Sequence=1 ttl=255 time=3 ms
    Reply from 192.168.1.49: bytes=56 Sequence=2 ttl=255 time=3 ms
```

2. Press **a**.

   The system aborts the command and returns to user view.

```
  --- 192.168.1.49 ping statistics ---
    2 packet(s) transmitted
    2 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/3/3 ms
<Sysname>
```

flow-control

Use **flow-control** to configure the flow control mode.

Use **undo flow-control** to restore the default.

Syntax

flow-control { **none** | **software** }

undo flow-control

Default

Flow control is disabled.

Views

User line view

Predefined user roles

network-admin

Parameters

none: Disables flow control.

software: Performs software flow control.

Usage guidelines

This command is not supported in VTY line view.

The device supports flow control in both the inbound and outbound directions.

- For flow control in the inbound direction, the local device listens to flow control information from the remote device.
- For flow control in the outbound direction, the local device sends flow control information to the remote device.

The flow control setting takes effect in both directions.

To communicate, two devices must operate in the same flow control mode.

Examples

Configure software flow control in the inbound and outbound directions for AUX line 0.

```
<Sysname> system-view
[Sysname] line aux 0
[Sysname-line-aux0] flow-control software
```

free line

Use **free line** to release a user line.

Syntax

free line { *number1* | { **aux** | **vty** } *number2* }

Views

User view

Predefined user roles

network-admin

Parameters

number1: Specifies the absolute number of a user line. The value range is 0 to 73.

aux: Specifies the AUX line.

vty: Specifies the VTY line.

number2: Specifies the relative number of a user line. The value range is 0 to 9 for AUX lines and 0 to 63 for VTY lines.

Usage guidelines

This command does not release the line you are using.

Examples

Release VTY line 1.

```
<Sysname> free line vty 1
Are you sure to free line vty1? [Y/N]:y
 [OK]
```

free user-interface

Use **free user-interface** to release a user line.

Syntax

free user-interface { *number1* | { **aux** | **vty** } *number2* }

Views

User view

Predefined user roles

network-admin

Parameters

number1: Specifies the absolute number of a user line. The value range is 0 to 73.

aux: Specifies the AUX line.

vty: Specifies the VTY line.

number2: Specifies the relative number of a user line. The value range is 0 to 9 for AUX lines and 0 to 63 for VTY lines.

Usage guidelines

This command does not release the line you are using.

This command is an older version reserved for backward compatibility purposes. It has the same functionality and output as the **free line** command. As a best practice, use the **free line** command.

Examples

Release VTY line 1.

```
<Sysname> free user-interface vty 1
Are you sure to free line vty1? [Y/N]:y
 [OK]
```

history-command max-size

Use **history-command max-size** to set the size of the command history buffer for a user line.

Use **undo history-command max-size** to restore the default.

Syntax

history-command max-size *size-value*

undo history-command max-size

Default

The command history buffer for a user line stores up to 10 history commands.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

size-value: Specifies the maximum number of history commands the buffer can store, in the range of 0 to 256.

Usage guidelines

Each user line uses a separate command history buffer to store commands successfully executed by its user. The buffer size determines how many history commands the buffer can store.

To display history commands in the buffer for your session, press the up or down arrow key, or execute the **display history-command** command. For more information about the command history buffer, see *Fundamentals Configuration Guide*.

Terminating a CLI session clears the commands in the command history buffer.

The setting in user line view takes effect immediately on the current session. The setting in user line class view takes effect on login sessions that are established after the setting is configured.

Examples

Set the command history buffer size to 20 for VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] history-command max-size 20
```

http acl

Use **http acl** to control TCP connections from IPv4 HTTP clients.

Use **undo http acl** to restore the default.

Syntax

http acl { *advanced-acl-number* | *basic-acl-number* }

undo http acl

Default

The device permits TCP connections from all IPv4 HTTP clients.

Views

System view

Predefined user roles

network-admin

Parameters

advanced-acl-number: Specifies an advanced IPv4 ACL number in the range of 3000 to 3999.

basic-acl-number: Specifies a basic IPv4 ACL number in the range of 2000 to 2999.

Usage guidelines

This command does not take effect on the existing TCP connections.

To control TCP connections from IPv4 HTTP clients, specify an existing ACL that has rules. Then, only IPv4 HTTP clients permitted by the ACL can establish TCP connections to the device. If no ACL is applied or the applied ACL does not exist or does not have rules, all IPv4 HTTP clients can establish TCP connections.

Whether an IPv4 HTTP client can use a service after it establishes a TCP connection to the device depends on the configuration for the service. For example, for an IPv4 HTTP client to use the NETCONF over SOAP service, both this command and the **netconf soap acl** command must permit the IPv4 HTTP client. For more information about the **netconf soap acl** command, see NETCONF in *Network Management and Monitoring Command Reference*.

Examples

Use ACL 2001 to allow only IPv4 HTTP clients from 1.1.1.1 to establish TCP connections to the device.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] http acl 2001
```

Related commands

netconf soap acl (*Network Management and Monitoring Command Reference*)

https acl

Use **https acl** to control TCP connections from IPv4 HTTPS clients.

Use **undo https acl** to restore the default.

Syntax

https acl { *advanced-acl-number* | *basic-acl-number* }

undo https acl

Default

The device permits TCP connections from all IPv4 HTTPS clients.

Views

System view

Predefined user roles

network-admin

Parameters

advanced-acl-number: Specifies an advanced IPv4 ACL number in the range of 3000 to 3999.

basic-acl-number: Specifies a basic IPv4 ACL number in the range of 2000 to 2999.

Usage guidelines

This command does not take effect on the existing TCP connections.

To control TCP connections from IPv4 HTTPS clients, specify an existing ACL that has rules. Then, only IPv4 HTTPS clients permitted by the ACL can establish TCP connections to the device. If no ACL is applied or the applied ACL does not exist or does not have rules, all IPv4 HTTPS clients can establish TCP connections.

Whether an IPv4 HTTPS client can use a service after it establishes a TCP connection to the device depends on the configuration for the service. For example, for an IPv4 HTTPS client to use the

NETCONF over SOAP service, both this command and the **netconf soap acl** command must permit the IPv4 HTTPS client. For more information about the **netconf soap acl** command, see NETCONF in *Network Management and Monitoring Command Reference*.

Examples

Use ACL 2001 to allow only IPv4 HTTPS clients from 1.1.1.1 to establish TCP connections to the device.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] https acl 2001
```

Related commands

netconf soap acl (*Network Management and Monitoring Command Reference*)

idle-timeout

Use **idle-timeout** to set the CLI connection idle-timeout timer.

Use **undo idle-timeout** to restore the default.

Syntax

idle-timeout *minutes* [*seconds*]

undo idle-timeout

Default

The CLI connection idle-timeout timer is 10 minutes.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

minutes: Specifies the number of minutes, in the range of 0 to 35791.

seconds: Specifies the number of seconds, in the range of 0 to 59. The default is 0 seconds.

Usage guidelines

The system automatically terminates a user connection if no information interaction occurs on the connection within the idle-timeout interval.

To disable the idle-timeout feature, execute the **idle-timeout 0** command.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

The setting in user line view takes effect immediately on the current session. The setting in user line class view takes effect on login sessions that are established after the setting is configured.

Examples

Set the CLI connection idle-timeout timer to 1 minute and 30 seconds for VTY line 0.

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

```
[Sysname] line vty 0
[Sysname-line-vty0] idle-timeout 1 30
```

line

Use **line** to enter one or multiple user line views.

Syntax

line { *first-number1* [*last-number1*] | { **aux** | **vty** } *first-number2* [*last-number2*] }

Views

System view

Predefined user roles

network-admin

Parameters

first-number1: Specifies the absolute number of the first user line. The value range is 0 to 73.

last-number1: Specifies the absolute number of the last user line. The value range is 1 to 73. This number must be greater than *first-number1*.

aux: Specifies the AUX line.

vty: Specifies the VTY line.

first-number2: Specifies the relative number of the first user line. The value range is 0 to 9 for AUX lines and 0 to 63 for VTY lines.

last-number2: Specifies the relative number of the last user line. The value range is 1 to 9 for AUX lines and 1 to 63 for VTY lines. This number must be greater than *first-number2*.

Examples

Enter the view of VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0]
```

Enter the views of VTY lines 0 to 63.

```
<Sysname> system-view
[Sysname] line vty 0 63
[Sysname-line-vty0-63]
```

Related commands

line class

line class

Use **line class** to enter user line class view.

Syntax

line class { **aux** | **vty** }

Views

System view

Predefined user roles

network-admin

Parameters

aux: Specifies the AUX line class view.

vty: Specifies the VTY line class view.

Usage guidelines

To configure the same settings for all user lines of a line class, use this command to enter the user line class view.

In user line class view, you can execute the following commands:

- **activation-key**
- **auto-execute command**
- **authentication-mode**
- **command accounting**
- **command authorization**
- **escape-key**
- **history-command max-size**
- **idle-timeout**
- **protocol inbound**
- **screen-length**
- **set authentication password**
- **shell**
- **terminal type**
- **user-role**

For commands that are available in both user line view and user line class view, the device uses the following rules to determine the settings to use:

- A setting in user line view applies only to the user line. A setting in user line class view applies to all user lines of the class.
- A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.
- A setting in user line class view does not take effect on current online users. It takes effect only on new login users.

Examples

Set the CLI connection idle-timeout timer to 15 minutes in VTY line class view.

```
<Sysname> system-view
[Sysname] line class vty
[Sysname-line-class-vty] idle-timeout 15
```

In AUX line class view, configure the character **s** as the terminal session activation key.

```
<Sysname> system-view
[Sysname] line class aux
[Sysname-line-class-aux] activation-key s
[Sysname-line-class-aux] quit
```

In the view of AUX line 0, restore the default terminal session activation key.

```
[Sysname] line aux 0
[Sysname-line-aux0] undo activation-key
```

Alternatively, you can use the following command:

```
[Sysname-line-aux0] activation-key 13
```

To verify the configuration:

1. Exit the session on AUX line 0.
   ```
   [Sysname-line-aux0] return
   <Sysname> quit
   ```
2. Log in again through the user line.
   The following message appears:
   ```
   Press ENTER to get started.
   ```
3. Press **Enter**.
   Pressing **Enter** does not start a session.
4. Enter **s**.
   A terminal session is started.
   ```
   <Sysname>
   ```

Related commands

line

lock

Use **lock** to lock the current user line and set the password for unlocking the line.

Syntax

lock

Default

The system does not lock any user lines.

Views

User view

Predefined user roles

network-admin

Usage guidelines

This command is not supported in FIPS mode.

This command locks the current user line to prevent unauthorized users from using the line. You must set the password for unlocking the line as prompted. The user line is locked after you enter the password and confirm the password.

To unlock the user line, press **Enter** and enter the password you set.

Examples

Lock the current user line and set the password for unlocking the line.

```
<Sysname> lock
Please input password<1 to 16> to lock current line:
Password:
Again:
```

```
                    locked !
```

// The user line is locked. To unlock it, press **Enter** and enter the password:

```
Password:
<Sysname>
```

lock reauthentication

Use **lock reauthentication** to lock the current user line and enable unlocking authentication.

Syntax

lock reauthentication

Default

The system does not lock any user lines or initiate reauthentication.

Views

Any view

Predefined user roles

network-admin

Usage guidelines

This command locks the current user line. To unlock the user line, you must press **Enter** and provide the login password to pass reauthentication. If you have changed the login password after login, you must provide the new password. If no login password is set, the system unlocks the user line after you press **Enter**.

Examples

Lock the current user line and enable unlocking authentication.

```
<Sysname> lock reauthentication

Please press Enter to unlock the screen.
```

// The user line is locked. To unlock it, press **Enter** and enter the login password:

```
Password:

<Sysname>
```

Related commands

lock-key

lock-key

Use **lock-key** to set the user line locking key. Pressing this shortcut key locks the current user line and enables unlocking authentication.

Use **undo lock-key** to restore the default.

Syntax

lock-key *key-string*

undo lock-key

Default

No user line locking key is set.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

key-string: Specifies a shortcut key. It can be a character (case sensitive), or an ASCII code value in the range of 0 to 127. For example, if you configure **lock-key 1**, the shortcut key is **Ctrl+A**. If you configure **lock-key a**, the shortcut key is **a**. For information about ASCII code values of individual characters, see the standard ASCII code chart. For information about ASCII code values of combined keys that use the **Ctrl** key, see Table 7.

Usage guidelines

As a best practice, specify a combined key as the user line locking key. If you specify a single character as the key, the character acts only as the user line locking key. You cannot type the character for any commands, keywords, or arguments.

Pressing the user line locking key is equivalent to executing the **lock reauthentication** command.

This command takes effect immediately.

To display the current user line locking key, use the **display current-configuration | include lock-key** command.

Examples

Set the user line locking key to **Ctrl+A** for VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] lock-key 1
[Sysname-line-vty0] quit
```

To verify the configuration:

1. Press **Ctrl+A**.

```
[Sysname]

Please press Enter to unlock the screen.
```

2. Press **Enter** and enter the login password.

```
Password:

[Sysname]
```

Related commands

lock reauthentication

parity

Use **parity** to specify the parity.

Use **undo parity** to restore the default.

Syntax

parity { **even** | **mark** | **none** | **odd** | **space** }

undo parity

Default

The setting is **none**. No parity is used.

Views

User line view

Predefined user roles

network-admin

Parameters

even: Uses even parity.

mark: Uses mark parity.

none: Uses no parity.

odd: Uses odd parity.

space: Uses space parity.

Usage guidelines

This command is not supported in VTY line view.

The configuration terminal and the device must use the same parity.

Examples

Configure AUX line 0 to use odd parity.

```
<Sysname> system-view
[Sysname] line aux 0
[Sysname-line-aux0] parity odd
```

protocol inbound

Use **protocol inbound** to specify the supported protocols.

Use **undo protocol inbound** to restore the default.

Syntax

In non-FIPS mode:

protocol inbound { **all**| **ssh** | **telnet** }

undo protocol inbound

In FIPS mode:

protocol inbound ssh

undo protocol inbound

Default

In non-FIPS mode, all protocols are supported.

In FIPS mode, SSH is supported.

Views

VTY line view

VTY line class view

Predefined user roles

network-admin

Parameters

all: Supports all protocols, including SSH and Telnet.

ssh: Supports SSH only.

telnet: Supports Telnet only.

Usage guidelines

Only users assigned the network-admin, or level-15 user role can execute this command. Other users cannot execute this command, even if they are granted the right to execute this command.

A configuration change in user line view does not take effect on the current session. It takes effect on subsequent login sessions.

Before configuring a user line to support SSH, set the authentication mode to **scheme** for the user line.

In VTY line view, this command is associated with the **authentication-mode** command. If you specify a non-default value for one of the two commands, the other command uses the default setting, regardless of the setting in VTY line class view.

- If the settings of the two commands in VTY line view are both the default settings, the settings for the commands in VTY line class view take effect.
- If the settings of the two commands in VTY line view are both non-default settings, the non-default settings in VTY line view take effect.
- If only one command has a non-default setting in VTY line view, the other command uses the default setting, regardless of the setting in VTY line class view.

Examples

Enable user lines VTY 0 through VTY 4 to support only SSH.

```
<Sysname> system-view
[Sysname] line vty 0 4
[Sysname-line-vty0-4] authentication-mode scheme
[Sysname-line-vty0-4] protocol inbound ssh
```

Enable SSH support and set the authentication mode to scheme in VTY line class view. Enable user lines VTY 0 through VTY 4 to support all protocols and disable authentication for the user lines.

```
<Sysname> system-view
[Sysname] line class vty
[Sysname-line-class-vty] authentication-mode scheme
[Sysname-line-class-vty] protocol inbound ssh
[Sysname-line-class-vty] line vty 0 4
[Sysname-line-vty0-4] authentication-mode none
```

To verify the configuration:

1. Telnet to the device.

```
<Client> telnet 192.168.1.241
Trying 192.168.1.241 ...
Press CTRL+K to abort
Connected to 192.168.1.241 ...

******************************************************************************
* Copyright (c) 2010-2020 Hewlett Packard Enterprise Development LP          *
* Without the owner's prior written consent,                                 *
```

```
* no decompiling or reverse-engineering shall be allowed.                     *
******************************************************************************

<Server>
```

You are logged in without authentication.

2. Display online CLI user information.

```
<Server> display users
  Idx  Line     Idle       Time              Pid     Type
+ 50   VTY 0    00:00:00   Jan 17 15:29:27   189     TEL

Following are more details.
VTY 0   :
        User role list: network-admin network-operator
        Location: 192.168.1.186
 +    : Current operation user.
 F    : Current operation user works in async mode.
```

The output shows that you are using VTY 0. The configuration in user line view is effective.

Related commands

authentication-mode

restful http enable

Use **restful http enable** to enable RESTful access over HTTP.

Use **undo restful http enable** to disable RESTful access over HTTP.

Syntax

restful http enable

undo restful http enable

Default

RESTful access over HTTP is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command is not supported in FIPS mode.

For users to access the device through the HTTP-based RESTful API, you must enable RESTful access over HTTP.

Examples

Enable RESTful access over HTTP.

```
<Sysname> system-view
[Sysname] restful http enable
```

restful http port

Use **restful http port** to specify the service port number for RESTful access over HTTP.

Use **undo restful http port** to restore the default.

Syntax

restful http port *port-number*

undo restful http port

Default

The service port number for RESTful access over HTTP is 80.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a port number in the range of 1 to 65535.

Usage guidelines

When RESTful access over HTTP is enabled, changing the service port number re-enables the service and closes all RESTful access over HTTP connections. To log in again, users must use the new port number.

Examples

Set the service port number to 1000 for RESTful access over HTTP.

```
<Sysname> system-view
[Sysname] restful http port 1000
```

restful https enable

Use **restful https enable** to enable RESTful access over HTTPS.

Use **undo restful https enable** to disable RESTful access over HTTPS.

Syntax

restful https enable

undo restful https enable

Default

RESTful access over HTTPS is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

For users to access the device through the HTTPS-based RESTful API, you must enable RESTful access over HTTPS.

Examples

Enable RESTful access over HTTPS.

```
<Sysname> system-view
[Sysname] restful https enable
```

restful https port

Use **restful https port** to specify the service port number for RESTful access over HTTPS.

Use **undo restful https port** to restore the default.

Syntax

restful https port *port-number*

undo restful https port

Default

The service port number for RESTful access over HTTPS is 443.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a port number in the range of 1 to 65535.

Usage guidelines

When RESTful access over HTTPS is enabled, changing the service port number re-enables the service and closes all RESTful access over HTTPS connections. To log in again, users must use the new port number.

Examples

Set the service port number to 1000 for RESTful access over HTTPS.

```
<Sysname> system-view
[Sysname] restful https port 1000
```

screen-length

Use **screen-length** to set the maximum number of lines of command output to send to the terminal at a time when the screen pausing feature is enabled.

Use **undo screen-length** to restore the default.

Syntax

screen-length *screen-length*

undo screen-length

Default

A maximum of 24 lines are sent.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

screen-length: Specifies the maximum number of lines to send, in the range of 0 to 512. To send command output without pausing, set the number to 0 or execute the **screen-length disable** command.

Usage guidelines

The number of lines that can be displayed on the terminal screen is restricted by both this setting and the display specification of the terminal. For example, if this setting is 40, the device sends 40 lines to the terminal at a time. If the terminal display specification is 24 lines, only the last 24 lines are displayed on the terminal screen. To view the previous 16 lines, you must press **PgUp**.

To continue to display command output after a pause, press the space bar.

By default, pausing between screens of output is enabled.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

The setting in user line view takes effect immediately on the current session. The setting in user line class view takes effect on login sessions that are established after the setting is configured.

Examples

Set the maximum number of lines to send at a time to 30 for VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] screen-length 30
```

Related commands

screen-length disable

send

Use **send** to send messages to online login users.

Syntax

send { **all** | *number1* | { **aux** | **vty** } *number2* }

Views

User view

Predefined user roles

network-admin

Parameters

all: Specifies all user lines.

number1: Specifies the absolute number of a user line. The value range is 0 to 73.

aux: Specifies the AUX line.

vty: Specifies the VTY line.

number2: Specifies the relative number of a user line. The value range is 0 to 9 for AUX lines and 0 to 63 for VTY lines.

Usage guidelines

You can use this command to send notifications to online users before performing an operation that might affect other online users, for example, before rebooting the device.

To end a message, press **Enter**. To abort the send operation, press **Ctrl+C**.

Examples

Send a notification to the user on VTY 1.

```
<Sysname> send vty 1
Input message, end with Enter; abort with CTRL+C:
Your attention, please. I will reboot the system in 3 minutes.
Send message? [Y/N]:y
```

The message should appear on the user's terminal screen as follows:

```
[Sysname]

***
***
***Message from vty0 to vty1
***
Your attention, please. I will reboot the system in 3 minutes.
```

set authentication password

Use **set authentication password** to set the password for local password authentication.

Use **undo set authentication password** to restore the default.

Syntax

set authentication password { **hash** | **simple** } *string*

undo set authentication password

Default

No password is set for local password authentication.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

hash: Specifies a password in hashed form.

simple: Sets a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in hashed form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 16 characters. Its hashed form is a case-sensitive string of 1 to 110 characters.

Usage guidelines

This command is not supported in FIPS mode.

Only users assigned the network-admin, or level-15 user role can execute this command. Other users cannot execute this command, even if they are granted the right to execute this command.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

A password change does not take effect on the current session. It takes effect on subsequent login sessions.

Examples

Set the password to **hello** for local password authentication on VTY line 0.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] authentication-mode password
[Sysname-line-vty0] set authentication password simple hello
```

Related commands

authentication-mode

shell

Use **shell** to enable the terminal service for user lines.

Use **undo shell** to disable the terminal service for user lines.

Syntax

shell

undo shell

Default

The terminal service is enabled on all user lines.

Views

User line view

User line class view

Predefined user roles

network-admin

Usage guidelines

The **undo shell** command is not supported in AUX line view or AUX line class view.

You cannot disable the terminal service on the user line you are using.

When the device acts as a Telnet or SSH server, you cannot configure the **undo shell** command.

If the **undo shell** command is configured in user line class view, you cannot configure the **shell** command in the view of a user line in the class.

Examples

Disable the terminal service for VTY lines VTY 0 through 4 so no user can log in to the device through the user lines.

```
<Sysname> system-view
[Sysname] line vty 0 4
[Sysname-line-vty0-4] undo shell
Disable ui-vty0-4 , are you sure? [Y/N]:y
[Sysname-line-vty0-4]
```

speed

Use **speed** to set the transmission rate (also called the baud rate) on a user line.

Use **undo speed** to restore the default.

Syntax

speed *speed-value*

undo speed

Default

The transmission rate is 9600 bps on a user line.

Views

User line view

Predefined user roles

network-admin

Parameters

speed-value: Specifies the transmission rate in bps. Supported transmission rates depend on the network environment. The transmission rates for asynchronous serial interfaces might include:

- 300 bps.
- 600 bps.
- 1200 bps.
- 2400 bps.
- 4800 bps.
- 9600 bps.
- 19200 bps.
- 38400 bps.
- 57600 bps.
- 115200 bps.

Usage guidelines

This command is not supported in VTY line view.

The configuration terminal and the device must be configured with the same transmission rate to communicate.

Examples

Set the transmission rate to 19200 bps for AUX line 0.

```
<Sysname> system-view
[Sysname] line aux 0
[Sysname-line-aux0] speed 19200
```

stopbits

Use **stopbits** to specify the number of stop bits for a character.

Use **undo stopbits** to restore the default.

Syntax

stopbits { **1** | **1.5** | **2** }

undo stopbits

Default

One stop bit is used.

Views

User line view

Predefined user roles

network-admin

Parameters

1: Uses one stop bit.

1.5: Uses one and a half stop bits. The device does not support using one and a half stop bits. If you specify this keyword, two stop bits are used.

2: Uses two stop bits.

Usage guidelines

This command is not supported in VTY line view.

The configuration terminal and the device must use the same number of stop bits to communicate.

Examples

Set the number of stop bits to 1 for AUX line 0.

```
<Sysname> system-view
[Sysname] line aux 0
[Sysname-line-aux0] stopbits 1
```

telnet

Use **telnet** to Telnet to a host in an IPv4 network.

Syntax

telnet *remote-host* [*service-port*] [**vpn-instance** *vpn-instance-name*] [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* } | **dscp** *dscp-value*] *

Views

User view

Predefined user roles

network-admin

Parameters

remote-host: Specifies the IPv4 address or host name of a remote host. A host name can be a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.).

service-port: Specifies the TCP port number for the Telnet service on the remote host. The value range is 0 to 65535 and the default is 23.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the remote host belongs. The *vpn-instance-name* argument represents the VPN instance name, a

case-sensitive string of 1 to 31 characters. If the remote host belongs to the public network, do not specify this option.

source: Specifies a source IPv4 address or source interface for outgoing Telnet packets. If you do not specify this option, the device uses the primary IPv4 address of the output interface for the route to the server as the source address.

interface *interface-type interface-number*: Specifies the source interface. The primary IPv4 address of the interface will be used as the source IPv4 address for outgoing Telnet packets.

ip *ip-address*: Specifies the source IPv4 address for outgoing Telnet packets.

dscp *dscp-value*: Specifies a DSCP value for outgoing Telnet packets. The value range is 0 to 63. The default is 48.

Usage guidelines

This command is not supported in FIPS mode.

To terminate the current Telnet connection, press **Ctrl+K** or execute the **quit** command.

The source address or interface specified by this command is applied only to the Telnet connection that is being established.

Examples

Telnet to host 1.1.1.2, using 1.1.1.1 as the source IP address for outgoing Telnet packets.

```
<Sysname> telnet 1.1.1.2 source ip 1.1.1.1
```

Related commands

telnet client source

telnet client source

Use **telnet client source** to specify a source IPv4 address or source interface for the Telnet client to use for outgoing Telnet packets.

Use **undo telnet client source** to restore the default.

Syntax

telnet client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

undo telnet client source

Default

No source IPv4 address or source interface is specified. The Telnet client uses the primary IPv4 address of the output interface for the route to the server as the source IPv4 address.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies a source interface. The primary IPv4 address of the interface will be used as the source IPv4 address for outgoing Telnet packets.

ip *ip-address*: Specifies a source IPv4 address.

Usage guidelines

This command is not supported in FIPS mode.

The setting configured by this command applies to all Telnet connections but has a lower precedence than the source setting specified for the **telnet** command.

Examples

Set the source IPv4 address to 1.1.1.1 for outgoing Telnet packets.

```
<Sysname> system-view
[Sysname] telnet client source ip 1.1.1.1
```

Related commands

display telnet client configuration

telnet ipv6

Use **telnet ipv6** to Telnet to a host in an IPv6 network.

Syntax

telnet ipv6 *remote-host* [**-i** *interface-type interface-number*] [*port-number*] [**vpn-instance** *vpn-instance-name*] [**source** { **interface** *interface-type interface-number* | **ipv6** *ipv6-address* } | **dscp** *dscp-value*] *

Views

User view

Predefined user roles

network-admin

Parameters

remote-host: Specifies the IPv6 address or host name of a remote host. A host name can be a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.).

-i *interface-type interface-number*: Specifies the interface for sending Telnet packets. This option is required when the remote host address is a link-local address. When the server address is a global unicast address, you cannot specify this option.

port-number: Specifies the TCP port number for the Telnet service on the remote host. The value range is 0 to 65535 and the default is 23.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the remote host belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the remote host belongs to the public network, do not specify this option.

source: Specifies a source IPv6 address or source interface for outgoing Telnet packets. If you do not specify this option, the device uses the primary IPv6 address of the output interface for the route to the server as the source address.

interface *interface-type interface-number*: Specifies the source interface. The primary IPv6 address of the interface will be used as the source IPv6 address for outgoing Telnet packets.

ipv6 *ipv6-address*: Specifies the source IPv6 address for outgoing Telnet packets.

dscp *dscp-value*: Specifies a DSCP value for outgoing Telnet packets. The value range is 0 to 63. The default is 48.

Usage guidelines

This command is not supported in FIPS mode.

To terminate the current Telnet connection, press **Ctrl+K** or execute the **quit** command.

Examples

Telnet to the host at 5000::1.

```
<Sysname> telnet ipv6 5000::1
```

Telnet to the host at 2000::1. Use 1000::1 as the source address for outgoing Telnet packets.

```
<Sysname> telnet ipv6 2000::1 source ipv6 1000::1
```

telnet server acl

Use **telnet server acl** to apply an ACL to filter Telnet logins.

Use **undo telnet server acl** to restore the default.

Syntax

telnet server acl [**mac**] *acl-number*

undo telnet server acl

Default

No ACL is used to filter Telnet logins.

Views

System view

Predefined user roles

network-admin

Parameters

mac: Specifies a Layer 2 ACL. To specify an ACL of a different type, do not specify this keyword.

acl-number: Specifies an ACL by its number. If you specify the **mac** keyword, the value range of this argument is 4000 to 4999. If you do not specify the **mac** keyword, the value range of this argument is 2000 to 3999.

Usage guidelines

This command is not supported in FIPS mode.

You can specify an ACL that does not exist for this command. However, this command takes effect only after you create the ACL and configure rules for the ACL. For more information about ACL, see *ACL and QoS Configuration Guide*.

If you execute this command multiple times, the most recent configuration takes effect.

This command does not take effect on existing Telnet connections.

Examples

Permit only the user at 1.1.1.1 to Telnet to the device.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] telnet server acl 2001
```

telnet server acl-deny-log enable

Use **telnet server acl-deny-log enable** to enable logging for Telnet login attempts that are denied by the Telnet login control ACL.

Use **undo telnet server acl-deny-log enable** to disable logging for Telnet login attempts that are denied by the Telnet login control ACL.

Syntax

telnet server acl-deny-log enable

undo telnet server acl-deny-log enable

Default

Logging is disabled for Telnet login attempts that are denied by the Telnet login control ACL.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Only clients permitted by the Telnet login control ACL can Telnet to the device. This logging feature generates log messages for Telnet login attempts that are denied by the Telnet login control ACL.

For information about log message output, see the information center in *Network Management and Monitoring Configuration Guide*. For information about configuring a Telnet login control ACL, see the **telnet server acl** or **telnet server ipv6 acl** command.

Examples

Enable logging for Telnet login attempts that are denied by the Telnet login control ACL.

```
<Sysname> system-view
[Sysname] telnet server acl-deny-log enable
```

Related commands

telnet server acl

telnet server ipv6 acl

telnet server dscp

Use **telnet server dscp** to specify the DSCP value for IPv4 to use for Telnet packets sent to a Telnet client.

Use **undo telnet server dscp** to restore the default.

Syntax

telnet server dscp *dscp-value*

undo telnet server dscp

Default

IPv4 uses the DSCP value 48 for Telnet packets sent to a Telnet client.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Usage guidelines

This command is not supported in FIPS mode.

The DSCP value is carried in the ToS field of an IPv4 packet to indicate the packet transmission priority.

Examples

Set the DSCP value for IPv4 to use for outgoing Telnet packets to 30 on a Telnet server.

```
<Sysname> system-view
[Sysname] telnet server dscp 30
```

telnet server enable

Use **telnet server enable** to enable the Telnet server.

Use **undo telnet server enable** to disable the Telnet server.

Syntax

telnet server enable

undo telnet server enable

Default

The Telnet server is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command is not supported in FIPS mode.

Users can Telnet to the device only when the Telnet server is enabled.

Examples

Enable the Telnet server.

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

telnet server ipv6 acl

Use **telnet server ipv6 acl** to apply an IPv6 ACL to filter IPv6 Telnet logins.

Use **undo telnet server ipv6 acl** to restore the default.

Syntax

telnet server ipv6 acl { **ipv6** | **mac** } *acl-number*

undo telnet server ipv6 acl

Default

No IPv6 ACL is used to filter IPv6 Telnet logins.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6: Specifies an IPv6 ACL.

mac: Specifies a Layer 2 ACL. To specify an ACL of a different type, do not specify this keyword.

acl-number: Specifies an ACL by its number. If you specify the **ipv6** keyword, the value range of this argument is 2000 to 3999. If you specify the **mac** keyword, the value range of this argument is 4000 to 4999.

Usage guidelines

This command is not supported in FIPS mode.

You can specify an ACL that does not exist for this command. However, this command takes effect only after you create the ACL and configure rules for the ACL. For more information about ACL, see *ACL and QoS Configuration Guide*.

If you execute this command multiple times, the most recent configuration takes effect.

This command does not take effect on existing Telnet connections.

Examples

Permit only the user at 2000::1 to Telnet to the device.

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl6-ipv6-basic-2001] rule permit source 2000::1 128
[Sysname-acl6-ipv6-basic-2001] quit
[Sysname] telnet server ipv6 acl ipv6 2001
```

telnet server ipv6 dscp

Use **telnet server ipv6 dscp** to specify the DSCP value for IPv6 to use for Telnet packets sent to a Telnet client.

Use **undo telnet server ipv6 dscp** to restore the default.

Syntax

telnet server ipv6 dscp *dscp-value*

undo telnet server ipv6 dscp

Default

IPv6 uses the DSCP value 48 for Telnet packets sent to a Telnet client.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Usage guidelines

This command is not supported in FIPS mode.

The DSCP value is carried in the Traffic class field of an IPv6 packet to indicate the packet transmission priority.

Examples

Set the DSCP value for IPv6 to use for outgoing Telnet packets to 30 on a Telnet server.

```
<Sysname> system-view
[Sysname] telnet server ipv6 dscp 30
```

telnet server ipv6 port

Use **telnet server ipv6 port** to specify the IPv6 Telnet service port number.

Use **undo telnet server ipv6 port** to restore the default.

Syntax

telnet server ipv6 port *port-number*

undo telnet server ipv6 port

Default

The IPv6 Telnet service port number is 23.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a port number. The value can be 23 or in the range of 1025 to 65535.

Usage guidelines

This command terminates all existing Telnet connections to the IPv6 Telnet server. To use the Telnet service, users must reestablish Telnet connections.

Examples

Set the IPv6 Telnet service port number to 1026.

```
<Sysname> system-view
[Sysname] telnet server ipv6 port 1026
```

telnet server port

Use **telnet server port** to specify the IPv4 Telnet service port number.

Use **undo telnet server port** to restore the default.

Syntax

telnet server port *port-number*

undo telnet server port

Default

The IPv4 Telnet service port number is 23.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies a port number. The value can be 23 or in the range of 1025 to 65535.

Usage guidelines

This command terminates all existing Telnet connections to the IPv4 Telnet server. To use the Telnet service, users must reestablish Telnet connections.

Examples

Set the IPv4 Telnet service port number to 1025.

```
<Sysname> system-view
[Sysname] telnet server port 1025
```

terminal type

Use **terminal type** to specify the terminal display type.

Use **undo terminal type** to restore the default.

Syntax

terminal type { **ansi** | **vt100** }

undo terminal type

Default

The terminal display type is ANSI.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

ansi: Specifies the ANSI type.

vt100: Specifies the VT100 type.

Usage guidelines

The device supports two terminal display types: ANSI and VT100. As a best practice, specify the VT100 type on both the device and the configuration terminal. If either side uses the ANSI type, a display problem might occur when a command line has more than 80 characters. For example, a cursor positioning error might occur.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

A terminal display type change does not take effect on the current session. It takes effect on subsequent login sessions.

Examples

Set the terminal display type to VT100.

```
<Sysname> system-view
[Sysname] line vty 0
[Sysname-line-vty0] terminal type vt100
```

user-interface

Use **user-interface** to enter one or multiple user line views.

Syntax

user-interface { *first-number1* [*last-number1*] | { **aux** | **vty** } *first-number2* [*last-number2*] }

Views

System view

Predefined user roles

network-admin

Parameters

first-number1: Specifies the absolute number of the first user line. The value range is 0 to 73.

last-number1: Specifies the absolute number of the last user line. The value range is 1 to 73. This number must be greater than *first-number1*.

aux: Specifies the AUX line.

vty: Specifies the VTY line.

first-number2: Specifies the relative number of the first user line. The value range is 0 to 9 for AUX lines and 0 to 63 for VTY lines.

last-number2: Specifies the relative number of the last user line. The value range is 1 to 9 for AUX lines and 1 to 63 for VTY lines. This number must be greater than *first-number2*.

Usage guidelines

This command is an older version reserved for backward compatibility purposes. It has the same functionality and output as the **line** command. As a best practice, use the **line** command.

To configure settings for a single user line, use this command to enter the user line view.

To configure the same settings for multiple user lines, use this command to enter multiple user line views.

Examples

Enter the view of AUX line 0.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-line-aux0]
```

Enter the views of VTY lines 0 to 4.

```
<Sysname> system-view
[Sysname] user-interface vty 0 4
[Sysname-line-vty0-4]
```

Related commands

user-interface class

user-interface class

Use **user-interface class** to enter user line class view.

Syntax

user-interface class { **aux** | **vty** }

Views

System view

Predefined user roles

network-admin

Parameters

aux: Specifies the AUX line class view.

vty: Specifies the VTY line class view.

Usage guidelines

This command is an older version reserved for backward compatibility purposes. It has the same functionality and output as the **line class** command. As a best practice, use the **line class** command.

To configure the same settings for all user lines of a line class, you can use this command to enter the user line class view.

The following commands are available in user line class view:

- **activation-key**
- **auto-execute command**
- **authentication-mode**
- **command accounting**
- **command authorization**
- **escape-key**
- **history-command max-size**
- **idle-timeout**
- **protocol inbound**
- **screen-length**
- **set authentication password**
- **shell**
- **terminal type**
- **user-role**

For commands that are available in both user line view and user line class view, the device uses the following rules to determine the settings to use:

- A setting in user line view applies only to the user line. A setting in user line class view applies to all user lines of the class.

- A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.
- A setting in user line class view does not take effect on current online users. It takes effect only on new login users.

Examples

Set the CLI connection idle-timeout timer to 15 minutes in VTY line class view.

```
<Sysname> system-view
[Sysname] user-interface class vty
[Sysname-line-class-vty] idle-timeout 15
```

In AUX line class view, configure character **s** as the terminal session activation key.

```
<Sysname> system-view
[Sysname] user-interface class aux
[Sysname-line-class-aux] activation-key s
[Sysname-line-class-aux] quit
```

In the view of AUX line 0, restore the default terminal session activation key.

```
[Sysname] user-interface aux 0
[Sysname-line-aux0] undo activation-key
```

Alternatively, you can use the following command:

```
[Sysname-line-aux0] activation-key 13
```

To verify the configuration:

1. Exit the session on AUX line 0.

   ```
   [Sysname-line-aux0] return
   <Sysname> quit
   ```

2. Log in again through the AUX line.

   The following message appears:

   ```
   Press ENTER to get started.
   ```

3. Press **Enter**.

   Pressing **Enter** does not start a session.

4. Enter **s**.

   A terminal session is started.

   ```
   <Sysname>
   ```

Related commands

user-interface

user-role

Use **user-role** to assign a user role to a user line. The device assigns the user role to a user of the line when the user logs in.

Use **undo user-role** to remove a user role or restore the default.

Syntax

user-role *role-name*

undo user-role [*role-name*]

Default

A console user is assigned the network-admin user role. Other users are assigned the network-operator user role.

Views

User line view

User line class view

Predefined user roles

network-admin

Parameters

role-name: Specifies a user role name, a case-sensitive string of 1 to 63 characters. The user role can be user-defined or predefined. Available predefined user roles include network-admin, network-operator, and level-0 to level-15. The predefined security-audit and guest-manager user roles are not supported in user line view or user line class view. If you do not specify this argument, the **undo user-role** command restores the default user role.

Usage guidelines

This command is not supported in FIPS mode.

Only users assigned the network-admin, or level-15 user role can execute this command. Other users cannot execute this command, even if they are granted the right to execute this command.

This command is available in both user line view and user line class view. A non-default setting in either view takes precedence over a default setting in the other view. A non-default setting in user line view takes precedence over a non-default setting in user line class view.

A user role change does not take effect on the current session. It takes effect on subsequent login sessions.

You can assign up to 64 user roles to a user line.

For more information about user roles, see RBAC configuration in *Fundamentals Configuration Guide*.

Examples

Assign user role network-admin to AUX line 0.

```
<Sysname> system-view
[Sysname] line aux 0
[Sysname-line-aux0] user-role network-admin
```

FTP commands

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

FTP is not supported in FIPS mode.

FTP server commands

display ftp-server

Use **display ftp-server** to display FTP server configuration and status information.

Syntax

display ftp-server

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display FTP server configuration and status information.

```
<Sysname> display ftp-server
FTP server is running.
User count:                        1
Idle-timeout timer (in minutes):  30
```

Table 13 Command output

Field	Description
User count	Number of the current logged-in users.
Idle-timeout timer (in minutes)	If no packet is exchanged between the FTP server and client during this period, the FTP connection is closed.

Related commands

ftp server enable

ftp timeout

display ftp-user

Use **display ftp-user** to display detailed information about online FTP users.

Syntax

display ftp-user

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display detailed information about online FTP users.

```
<Sysname> display ftp-user
UserName     HostIP             Port     HomeDir
root         192.168.20.184     46539    flash:
```

A field value is wrapped if its length exceeds the limit. The segments are left justified.

The following are the length limits for fields:

- **UserName**—10 characters.
- **HostIP**—15 characters.
- **HomeDir**—37 characters.

```
<Sysname> display ftp-user
UserName     HostIP             Port     HomeDir
user2        2000:2000:2000:    1499     flash:/user2
             2000:2000:2000:
             2000:2000
administra   100.100.100.100    10001    flash:/123456789/123456789/123456789/
tor                                      123456789/123456789/123456789/1234567
                                         89/123456789
```

Table 14 Command output

Field	Description
UserName	Name of the user.
HostIP	IP address of the user.
Port	Port number of the user.
HomeDir	Authorized directory for the user.

free ftp user

Use **free ftp user** to manually release the FTP connections established by using a specific user account.

Syntax

free ftp user *username*

Views

User view

Predefined user roles

network-admin

Parameters

username: Specifies a username. To display online FTP users, execute the **display ftp-user** command.

Examples

Release the FTP connections established by using user account **ftpuser**.

```
<Sysname> free ftp user ftpuser
Are you sure to free FTP connection? [Y/N]:y
<Sysname>
```

free ftp user-ip

Use **free ftp user-ip** to manually release the FTP connections established from a specific IPv4 address.

Syntax

free ftp user-ip *ip-address* [**port** *port*]

Views

User view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the source IP address of an FTP connection. To view the source IP addresses of FTP connections, execute the **display ftp-user** command.

port *port*: Specifies the source port of an FTP connection. To view the source ports of FTP connections, execute the **display ftp-user** command.

Examples

Release the FTP connections established from the IP address 192.168.20.184.

```
<Sysname> free ftp user-ip 192.168.20.184
Are you sure to free FTP connection? [Y/N]:y
<Sysname>
```

free ftp user-ip ipv6

Use **free ftp user-ip ipv6 to** manually release the FTP connections established from a specific IPv6 address.

Syntax

free ftp user-ip ipv6 *ipv6-address* [**port** *port*]

Views

User view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the source IPv6 address of an FTP connection. To view the source IPv6 addresses of FTP connections, execute the **display ftp-user** command.

port *port*: Specifies the source port of an FTP connection. To view the source ports of FTP connections, execute the **display ftp-user** command.

Examples

Release the FTP connections established from IPv6 address 2000::154.

```
<Sysname> free ftp user-ip ipv6 2000::154
Are you sure to free FTP connection? [Y/N]:y
<Sysname>
```

ftp server acl

Use **ftp server acl** to use an ACL to control FTP clients' access to the FTP server.

Use **undo ftp server acl** to restore the default.

Syntax

ftp server acl { *advanced-acl-number* | *basic-acl-number* | **ipv6** { *advanced-acl-number* | *basic-acl-number* } }

undo ftp server acl [**ipv6**]

Default

No ACL is used to control FTP clients' access to the FTP server.

Views

System view

Predefined user roles

network-admin

Parameters

advanced-acl-number: Specifies an advanced IPv4 ACL number in the range of 3000 to 3999.

basic-acl-number: Specifies a basic IPv4 ACL number in the range of 2000 to 2999.

ipv6 *advanced-acl-number*: Specifies an advanced IPv6 ACL number in the range of 3000 to 3999.

ipv6 *basic-acl-number*: Specifies a basic IPv6 ACL number in the range of 2000 to 2999.

Usage guidelines

You can use this command to permit only FTP requests from specific FTP clients. This configuration takes effect only for FTP connections to be established. It does not impact existing FTP connections.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Use ACL 2001 to allow only client 1.1.1.1 to access the FTP server.

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule 0 permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2001] rule 1 deny source any
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ftp server acl 2001
```

ftp server acl-deny-log enable

Use **ftp server acl-deny-log enable** to enable logging for FTP login attempts that are denied by the FTP login control ACL.

Use **undo ftp server acl-deny-log enable** to disable logging for FTP login attempts that are denied by the FTP login control ACL.

Syntax

ftp server acl-deny-log enable

undo ftp server acl-deny-log enable

Default

Logging is disabled for FTP login attempts that are denied by the FTP login control ACL.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Only clients permitted by the FTP login control ACL can use FTP to access the device. This logging feature generates log messages for FTP login attempts that are denied by the FTP login control ACL.

For information about log message output, see the information center in *Network Management and Monitoring Configuration Guide*. For information about configuring an FTP login control ACL, see the **ftp server acl** command.

Examples

Enable logging for FTP login attempts that are denied by the FTP login control ACL.

```
<Sysname> system-view
[Sysname] FTP server acl-deny-log enable
```

Related commands

ftp server acl

ftp server dscp

Use **ftp server dscp** to set the DSCP value for IPv4 to use for FTP packets sent to an FTP client.

Use **undo ftp server dscp** to restore the default.

Syntax

ftp server dscp *dscp-value*

undo ftp server dscp

Default

IPv4 uses the DSCP value 0 for FTP packets sent to an FTP client.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value is carried in the ToS field of an IP packet to indicate the transmission priority of the packet.

Examples

Set the DSCP value for IPv4 to use for outgoing FTP packets to 30 on an FTP server.

```
<Sysname> system-view
[Sysname] ftp server dscp 30
```

ftp server enable

Use **ftp server enable** to enable the FTP server.

Use **undo ftp server enable** to disable the FTP server.

Syntax

ftp server enable

undo ftp server enable

Default

The FTP server is disabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the FTP server.

```
<Sysname> system-view
[Sysname] ftp server enable
```

ftp server ipv6 dscp

Use **ftp server ipv6 dscp** to set the DSCP value for IPv6 to use for FTP packets sent to an FTP client.

Use **undo ftp server ipv6 dscp** to restore the default.

Syntax

ftp server ipv6 dscp *dscp-value*

undo ftp server ipv6 dscp

Default

IPv6 uses the DSCP value 0 for FTP packets sent to an FTP client.

Views

System view

Predefined user roles

network-admin

Parameters

dscp-value: Specifies a DSCP value in the range of 0 to 63.

Usage guidelines

The DSCP value is carried in the Traffic class field of an IPv6 packet to indicate the transmission priority of the packet.

Examples

Set the DSCP value for IPv6 to use for outgoing FTP packets to 30 on an FTP server.

```
<Sysname> system-view
[Sysname] ftp server ipv6 dscp 30
```

ftp server ssl-server-policy

Use **ftp server ssl-server-policy** to associate an SSL server policy with the FTP server.

Use **undo ftp server ssl-server-policy** to restore the default.

Syntax

ftp server ssl-server-policy *policy-name*

undo ftp server ssl-server-policy

Default

No SSL server policy is associated with the FTP server.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies an SSL server policy by its name, a string of 1 to 31 characters.

Usage guidelines

After you associate an SSL server policy with the device, a client that supports SFTP will establish a secure connection to the device to ensure data security.

Examples

Associate SSL server policy **myssl** with the FTP server.

```
<Sysname> system-view
[Sysname] ftp server ssl-server-policy myssl
```

Related commands

ftp server enable

ssl server-policy (*Security Command Reference*)

ftp timeout

Use **ftp timeout** to set the FTP connection idle-timeout timer.

Use **undo ftp timeout** to restore the default.

Syntax

ftp timeout *minute*

undo ftp timeout

Default

The FTP connection idle-timeout timer is 30 minutes.

Views

System view

Predefined user roles

network-admin

Parameters

minute: Specifies a time interval in the range of 1 to 35791 minutes.

Usage guidelines

If no data transfer occurs on an FTP connection within the idle-timeout interval, the FTP server closes the FTP connection to release resources.

Examples

Set the FTP connection idle-timeout timer to 36 minutes.

```
<Sysname> system-view
[Sysname] ftp timeout 36
```

FTP client commands

For FTP users to execute FTP client configuration commands, you must configure authorization settings for users on the FTP server. Authorized operations include viewing the files in the working directory, reading/downloading/uploading/renaming/removing files, and creating directories.

The FTP client commands in this section are supported by the device, but whether they can be executed successfully depends on the FTP server.

The output in the examples of this section varies by FTP server type.

?

Use **?** to display all commands supported by an FTP client.

Use **?** *command-name* to display the help information for a command.

Syntax

? [*command-name*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

command-name: Specifies a command supported by the FTP client.

Usage guidelines

In FTP client view, entering **?** is the same as executing the **help** command.

Examples

Display all commands supported by the FTP client.

```
ftp> ?
Commands may be abbreviated.  Commands are:

append          delete          ls              quit            rmdir
ascii           debug           mkdir           reget           status
binary          dir             newer           rstatus         system
bye             disconnect      open            rhelp           user
cd              get             passive         rename          verbose
cdup            help            put             reset           ?
close           lcd             pwd             restart
```

Display the help information for the **dir** command.

```
ftp> ? dir
dir              list contents of remote directory
```

Related commands

help

append

Use **append** to add the content of a file on the FTP client to a file on the FTP server.

Syntax

append *localfile* [*remotefile*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

localfile: Specifies a file on the FTP client.

remotefile: Specifies a file on the FTP server.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Append the content of the local **a.txt** file to the **b.txt** file on the FTP server.

```
ftp> append a.txt b.txt
227 Entering Passive Mode (192,168,1,84,8,145)
150 Accepted data connection
226 File successfully transferred
1657 bytes sent in 0.000736 seconds (2.15 Mbyte/s)
```

ascii

Use **ascii** to set the file transfer mode to ASCII.

Syntax

ascii

Default

The file transfer mode is binary.

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

FTP transfers files in either of the following modes:

- **Binary mode**—Transfers non-text files.
- **ASCII mode**—Transfers text files.

When the device acts as the FTP server, the transfer mode is determined by the FTP client. When the device acts as the FTP client, you can set the transfer mode. The transfer mode is binary by default.

Examples

Set the file transfer mode to ASCII.

```
ftp> ascii
200 TYPE is now ASCII
```

Related commands

binary

binary

Use **binary** to set the file transfer mode to binary, which is also called the flow mode.

Syntax

binary

Default

The file transfer mode is binary.

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

FTP transfers files in either of the following modes:

- **Binary mode**—Transfers program file or pictures.

- **ASCII mode**—Transfers text files.

When the device acts as the FTP server, the transfer mode is determined by the FTP client. When the device acts as the FTP client, you can set the transfer mode. The default transfer mode is binary.

Examples

Set the file transfer mode to binary.

```
ftp> binary
200 TYPE is now 8-bit binary
```

Related commands

ascii

bye

Use **bye** to terminate the connection to the FTP server and return to user view. If no connection is established between the device and the FTP server, use this command to return to user view.

Syntax

bye

Views

FTP client view

Predefined user roles

network-admin

Examples

Terminate the connection to the FTP server and return to user view.

```
ftp> bye
221-Goodbye. You uploaded 2 and downloaded 2 kbytes.
221 Logout.
<Sysname>
```

Related commands

quit

cd

Use **cd** to change the current working directory to another directory on the FTP server.

Syntax

cd { *directory* | **..** | **/** }

Views

FTP client view

Predefined user roles

network-admin

Parameters

directory: Specifies the target directory. If the target directory does not exist, the **cd** command does not change the current working directory.

..: Specifies the upper directory. Executing the **cd ..** command is the same as executing the **cdup** command. If the current working directory is the FTP root directory, the **cd ..** command does not change the current working directory.

/: Specifies the FTP root directory.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

The directory that can be accessed must be authorized by the FTP server.

Examples

Change the working directory to the **logfile** subdirectory of the current directory.

```
ftp> cd logfile
250 OK. Current directory is /logfile
```

Change the working directory to the **folder** subdirectory of the FTP root directory.

```
ftp> cd /folder
250 OK. Current directory is /folder
```

Change the working directory to the upper directory of the current directory.

```
ftp> cd ..
250 OK. Current directory is /
```

Change the working directory to the FTP root directory.

```
ftp> cd /
250 OK. Current directory is /
```

Related commands

cdup

pwd

cdup

Use **cdup** to enter the upper directory of the FTP server.

Syntax

cdup

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

This command does not change the working directory if the current directory is the FTP root directory.

Examples

Change the working directory to the upper directory.

```
ftp> pwd
257 "/ftp/subdir" is your current location
ftp> cdup
250 OK. Current directory is /ftp
```

```
ftp> pwd
257 "/ftp" is your current location
```

Related commands

cd

pwd

close

Use **close** to terminate the connection to the FTP server without exiting FTP client view.

Syntax

close

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Terminate the connection to the FTP server without exiting the FTP client view.

```
ftp> close
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
ftp>
```

Related commands

disconnect

debug

Use **debug** to enable or disable FTP client debugging.

Syntax

debug

Default

FTP client debugging is disabled.

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

When FTP client debugging is enabled, executing this command disables FTP client debugging.

When FTP client debugging is disabled, executing this command enables FTP client debugging.

Examples

Enable and then disable FTP client debugging.

```
ftp> debug
Debugging on (debug=1).
ftp> debug
Debugging off (debug=0).
```

delete

Use **delete** to permanently delete a file from the FTP server.

Syntax

delete *remotefile*

Views

FTP client view

Predefined user roles

network-admin

Parameters

remotefile: Specifies a file on the FTP server.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

To perform this operation, you must have delete permission on the FTP server.

Examples

Delete the **b.txt** file.

```
ftp> delete b.txt
250 Deleted b.txt
```

dir

Use **dir** to display or save detailed information about files and directories on the FTP server.

Syntax

dir [*remotefile* [*localfile*]]

Views

FTP client view

Predefined user roles

network-admin

Parameters

remotefile: Specifies a file or directory on the FTP server.

localfile: Specifies the name of the local file used to save the displayed information.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

To display detailed information about the files and subdirectories in the working directory on the FTP server, use the **dir** command.

To display detailed information about a file or directory on the FTP server, use the **dir** *remotefile* command.

To save detailed information about a file or directory on the FTP server to a local file, use the **dir** *remotefile localfile* command.

In FTP client view, executing the **dir** command is the same as executing the **ls** command.

Examples

Display detailed information about the files and subdirectories in the working directory on the FTP server.

```
ftp> dir
150 Connecting to port 50201
-rwxr-xr-x    1 0          0               1481 Jul  7 15:36 a.txt
drwxr-xr-x    2 0          0               8192 Jul  2 14:33 diagfile
drwxr-xr-x    3 0          0               8192 Jul  7 15:21 ftp
drwxr-xr-x    2 0          0               8192 Jul  5 09:15 logfile
drwxr-xr-x    2 0          0               8192 Jul  2 14:33 seclog
-rwxr-xr-x    1 0          0           40808448 Jul  2 14:33 system-a1801.bin
-rwxr-xr-x    1 0          0               3050 Jul  7 12:26 startup.cfg
-rwxr-xr-x    1 0          0              54674 Jul  4 09:24 startup.mdb
-rwxr-xr-x    1 0          0               1481 Jul  7 12:34 x.cfg
226 9 matches total
```

Save detailed information about file **a.txt** to **s.txt**.

```
ftp> dir a.txt s.txt
output to local-file: s.txt ? [Y/N]y
150 Connecting to port 50203
226-Glob: a.txt
```

Display the content of the file **s.txt**.

```
ftp> bye
221-Goodbye. You uploaded 0 and downloaded 2 kbytes.
221 Logout.
<Sysname> more s.txt
-rwxr-xr-x    1 0          0               1481 Jul  7 12:34 a.txt
```

Related commands

ls

disconnect

Use **disconnect** to terminate the connection to the FTP server without exiting FTP client view.

Syntax

disconnect

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Terminate the connection to the FTP server without exiting the FTP client view.

```
ftp> disconnect
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
ftp>
```

Related commands

close

display ftp client source

Use **display ftp client source** to display the source address settings on the FTP client.

Syntax

display ftp client source

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the source address settings on the FTP client.

```
<Sysname> display ftp client source
The source IP address of the FTP client is 1.1.1.1.
```

ftp

Use **ftp** to log in to an IPv4 FTP server and enter FTP client view.

Syntax

ftp [*ftp-server* [*service-port*] [**vpn-instance** *vpn-instance-name*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* } | **-d**] *]

Views

User view

Predefined user roles

network-admin

Parameters

ftp-server: Specifies the IPv4 address or host name of an FTP server. A host name can be a case-insensitive string of 1 to 253 characters. Valid characters for a host name include letters, digits, hyphens (-), underscores (_), and dots (.).

service-port: Specifies the TCP port number of the FTP server, in the range of 0 to 65535. The default is 21.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the FTP server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the FTP server belongs to the public network, do not specify this option.

dscp *dscp-value*: Specifies the DSCP value for IPv4 to use in outgoing FTP packets to indicate the packet transmission priority. The value range is 0 to 63. The default is 0.

source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }: Specifies the source address used to establish the FTP connection.

- **interface** *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's primary IPv4 address as the source address. To establish the FTP connection successfully, make sure the interface is up and has the primary IPv4 address configured.
- **ip** *source-ip-address*: Specifies an IPv4 address. To establish the FTP connection successfully, make sure this address is the IPv4 address of an interface in up state on the device.

-d: Enables FTP client debugging.

Usage guidelines

This command is only applicable to IPv4 networks.

If no parameters are specified, this command enters the FTP client view without logging in to an FTP server.

If the server parameters are specified, you are prompted to enter the username and password for logging in to the FTP server.

Examples

Log in to FTP server 192.168.0.211. Use 192.168.0.212 as the source IPv4 address for outgoing FTP packets.

```
<Sysname>ftp 192.168.0.211 source ip 192.168.0.212
Press CTRL+C to abort.
Connected to 192.168.0.211 (192.168.0.211).
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User (192.168.0.211:(none)): abc
331 Give me your password, please
Password:
230 Logged in successfully
Remote system type is MSDOS.
ftp>
```

Log in to FTP server 192.168.0.211 and enable FTP client debugging.

```
<Sysname> ftp 192.168.0.211 –d
Press CTRL+C to abort.
Connected to 192.168.0.211 (192.168.0.211).
220 FTP service ready.
User (192.168.0.211:(none)): abc
*Apr 10 09:02:24:139 2017 Sysname FTPC/7/EVENT: PAM initialization result: 0.
*Apr 10 09:02:24:150 2017 Sysname FTPC/7/EVENT: PAM: Sent a start-accounting request.
Result: 0.
*Apr 10 09:02:24:860 2017 Sysname FTPC/7/COMMAND: USER abc
331 Password required for abc.
Password:
*Apr 10 09:02:25:575 2017 Sysname FTPC/7/COMMAND: PASS XXXX
```

```
230 User logged in.
215 UNIX Type: L8
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> *Apr 10 09:02:25:640 2017 SIMWARE FTPC/7/COMMAND: SYST
ftp>
```

ftp client ipv6 source

Use **ftp client ipv6 source** to specify the source IPv6 address for FTP packets sent to an IPv6 FTP server.

Use **undo ftp client ipv6 source** to restore the default.

Syntax

ftp client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }

undo ftp client ipv6 source

Default

No source address is specified for FTP packets sent to an IPv6 FTP server. The device selects a source IPv6 address as defined in RFC 3484.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's IPv6 address as the source address. For successful FTP packet transmission, make sure the interface is up and is configured with an IPv6 address.

ipv6 *source-ipv6-address*: Specifies an IPv6 address. For successful FTP packet transmission, make sure this address is the IPv6 address of an interface in up state on the device.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The source address specified with the **ftp ipv6** command takes precedence over the source address specified with the **ftp client ipv6 source** command.

The source address specified with the **ftp client ipv6 source** command applies to all FTP connections. The source address specified with the **ftp ipv6** command applies only to the FTP connection that is being established.

Examples

Specify the source IPv6 address of 2000::1 for FTP packets sent to an IPv6 FTP server.

```
<Sysname> system-view
[Sysname] ftp client ipv6 source ipv6 2000::1
```

Related commands

ftp ipv6

ftp client source

Use **ftp client source** to specify the source IPv4 address for FTP packets sent to an IPv4 FTP server.

Use **undo ftp client source** to restore the default.

Syntax

ftp client source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }

undo ftp client source

Default

No source IPv4 address is specified for FTP packets sent to an IPv4 FTP server. The device uses the primary IPv4 address of the output interface for the route to the server as the source address.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's primary IPv4 address as the source address. For successful FTP packet transmission, make sure the interface is up and has the primary IPv4 address configured.

ip *source-ip-address*: Specifies an IPv4 address. For successful FTP packet transmission, make sure this address is the IPv4 address of an interface in up state on the device.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The source address specified with the **ftp** command takes precedence over the source address specified with the **ftp client source** command.

The source address specified with the **ftp client source** command applies to all FTP connections. The source address specified with the **ftp** command applies only to the FTP connection that is being established.

Examples

Specify the source IPv4 address of 192.168.20.222 for FTP packets sent to an IPv4 FTP server.

```
<Sysname> system-view
[Sysname] ftp client source ip 192.168.20.222
```

Related commands

ftp

ftp ipv6

Use **ftp ipv6** to log in to an IPv6 FTP server and enter FTP client view.

Syntax

ftp ipv6 [*ftp-server* [*service-port*] [**vpn-instance** *vpn-instance-name*] [**dscp** *dscp-value* | **source** { **ipv6** *source-ipv6-address* | **interface**

interface-type interface-number } | **-d**] * [**-i** *interface-type interface-number*]]

Views

User view

Predefined user roles

network-admin

Parameters

ftp-server: Specifies the IPv6 address or host name of an FTP server. A host name can be a case-insensitive string of 1 to 253 characters. Valid characters for a host name include letters, digits, hyphens (-), underscores (_), and dots (.).

service-port: Specifies the TCP port number of the FTP server, in the range of 0 to 65535. The default is 21.

dscp *dscp-value*: Specifies the DSCP value for IPv6 to use in outgoing FTP packets to indicate the packet transmission priority. The value range is 0 to 63. The default is 0.

source { **ipv6** *source-ipv6-address* | **interface** *interface-type interface-number* }: Specifies the source address used to establish the FTP connection.

- **interface** *interface-type interface-number*: Specifies an interface by its type and number. This option can be used only when the FTP server address is a link local address and the specified output interface has a link local address. For information about link local addresses, see *Layer 3—IP Services Configuration Guide*.
- **ipv6** *source-ipv6-address*: Specifies an IPv6 address. To establish the FTP connection successfully, make sure this address is the IPv6 address of an interface in up state on the device.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the FTP server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the FTP server belongs to the public network, do not specify this option.

-i *interface-type interface-number*: Specifies an output interface by its type and number. This option can be used only when the FTP server address is a link local address and the specified output interface has a link local address.

-d: Enables FTP client debugging.

Usage guidelines

This command is only applicable to IPv6 networks.

If no parameters are specified, this command enters the FTP client view.

If the FTP server parameters are specified, you are prompted to enter the username and password for logging in to the FTP server.

Examples

Log in to FTP server 2000::154.

```
<Sysname>ftp ipv6 2000::154
Press CTRL+C to abort.
Connected to 2000::154 (2000::154).
220 FTP service ready.
User (2000::154): root
331 Password required for root.
Password:
230 User logged in
```

```
Remote system type is HPE
```

Log in to FTP server 2000::154 and enable FTP client debugging.

```
<Sysname> ftp ipv6 2000::154 –d
Press CTRL+C to abort.
Connected to 2000::154 (2000::154).
220 FTP service ready.
User (2000::154:(none)): root
*Apr 10 09:03:24:139 2017 Sysname FTPC/7/EVENT: PAM initialization result: 0.
*Apr 10 09:03:24:150 2017 Sysname FTPC/7/EVENT: PAM: Sent a start-accounting request.
Result: 0.
*Apr 10 09:03:24:860 2017 Sysname FTPC/7/COMMAND: USER root
331 Password required for root.
Password:
*Apr 10 09:03:25:575 2017 Sysname FTPC/7/COMMAND: PASS XXXX
230 User logged in.
215 UNIX Type: L8
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> *Apr 10 09:03:25:640 2017 SIMWARE FTPC/7/COMMAND: SYST
ftp>
```

get

Use **get** to download a file from the FTP server and save the file.

Syntax

get *remotefile* [*localfile*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

remotefile: Specifies the file to be downloaded.

localfile: Specifies a name for the downloaded file. If you do not specify this argument, the system uses the name of the source file.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

To save the downloaded file to the working directory accessed by the **ftp** command, perform one of the following tasks:

- Execute the command without specifying the *localfile* argument.
- Specify a file name without any path information for the *localfile* argument, for example, a.cfg.

To save the downloaded file to some other directory, you must specify a fully qualified file name for the *localfile* argument, for example, flash:/subdirectory/a.cfg.

Examples

Download the **a.txt** file and save it as **b.txt** in the working directory accessed by the **ftp** command.

```
ftp> get a.txt b.txt
local: b.txt remote: a.txt
150 Connecting to port 47457
226 File successfully transferred
1569 bytes received in 0.00527 seconds (290.6 kbyte/s)
```

Download the **a.txt** file to the **test** directory in the working directory accessed by the **ftp** command.

```
ftp> get a.txt flash:/test/b.txt
local: flash:/test/b.txt remote: a.txt
150 Connecting to port 47457
226 File successfully transferred
1569 bytes received in 0.00527 seconds (290.6 kbyte/s)
```

Download the **a.txt** file to the root directory of the flash memory on a member device. Save the file as **c.txt**.

```
ftp> get a.txt slot1#flash:/c.txt
local: slot1#flash:/c.txt remote: a.txt
150 Connecting to port 47460
226 File successfully transferred
1569 bytes received in 0.0564 seconds (27.2 kbyte/s)
```

Related commands

put

help

Use **help** to display all commands supported by the FTP client.

Use **help** *command-name* to display the help information for a command.

Syntax

help [*command-name*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

command-name: Specifies a command supported by the FTP client.

Usage guidelines

In FTP client view, executing the **help** command is the same as entering **?**.

Examples

Display all commands supported by the FTP client.

```
ftp> help

append          delete          ls              quit            rmdir
```

```
ascii           debug           mkdir           reget           status
binary          dir             newer           rstatus         system
bye             disconnect      open            rhelp           user
cd              get             passive         rename          verbose
cdup            help            put             reset           ?
close           lcd             pwd             restart
```

Display the help information for the **dir** command.

```
ftp> help dir
dir              list contents of remote directory
```

Related commands

?

lcd

Use **lcd** to display or change the local working directory of the FTP client.

Syntax

lcd [*directory* | **/**]

Views

FTP client view

Predefined user roles

network-admin

Parameters

directory: Changes the local working directory of the FTP client to the specified local directory. There must be a slash sign (/) before the name of the storage medium, for example, /flash:/logfile.

/: Changes the local working directory of the FTP client to the local root directory.

Usage guidelines

To display the local working directory of the FTP client, do not specify the *directory* or **/** argument.

Examples

Display the local working directory.

```
ftp> lcd
Local directory now /flash:
```

Change the local working directory to **flash:/logfile**.

```
ftp> lcd /flash:/logfile
Local directory now /flash:/logfile
```

ls

Use **ls** to display or save detailed information about files and directories on the FTP server.

Syntax

ls [*remotefile* [*localfile*]]

Views

FTP client view

Predefined user roles

network-admin

Parameters

remotefile: Specifies a file or directory on the FTP server.

localfile: Specifies the name of the local file used to save the displayed information.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

To display detailed information about the files and subdirectories in the working directory on the FTP server, use the **ls** command.

To display detailed information about a file or directory on the FTP server, use the **ls** *remotefile* command.

To save detailed information about a file or directory on the FTP server to a local file, use the **ls** *remotefile localfile* command.

In FTP client view, executing the **ls** command is the same as executing the **dir** command.

Examples

Display detailed information about the files and subdirectories in the working directory on the FTP server.

```
ftp> ls
150 Connecting to port 50201
-rwxr-xr-x    1 0          0               1481 Jul  7 15:36 a.txt
drwxr-xr-x    2 0          0               8192 Jul  2 14:33 diagfile
drwxr-xr-x    3 0          0               8192 Jul  7 15:21 ftp
drwxr-xr-x    2 0          0               8192 Jul  5 09:15 logfile
drwxr-xr-x    2 0          0               8192 Jul  2 14:33 seclog
-rwxr-xr-x    1 0          0           40808448 Jul  2 14:33 system-a1801.bin
-rwxr-xr-x    1 0          0               3050 Jul  7 12:26 startup.cfg
-rwxr-xr-x    1 0          0              54674 Jul  4 09:24 startup.mdb
-rwxr-xr-x    1 0          0               1481 Jul  7 12:34 x.cfg
226 9 matches total
```

Save detailed information about the file **a.txt** to **s.txt**.

```
ftp> ls a.txt s.txt
output to local-file: s.txt ? [Y/N]y
150 Connecting to port 50203
226-Glob: s.txt
```

Display the content of the file **s.txt**.

```
ftp> bye
221-Goodbye. You uploaded 0 and downloaded 2 kbytes.
221 Logout.
<Sysname> more s.txt
-rwxr-xr-x    1 0          0               1481 Jul  7 12:34 a.txt
```

Related commands

dir

mkdir

Use **mkdir** to create a subdirectory in the current directory on the FTP server.

Syntax

mkdir *directory*

Views

FTP client view

Predefined user roles

network-admin

Parameters

directory: Specifies the name for the directory to be created.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

You must have permission to perform this operation on the FTP server.

Examples

Create a subdirectory named **newdir** in the current directory of the FTP server.

```
ftp> mkdir newdir
257 "newdir" : The directory was successfully created
```

newer

Use **newer** to update a local file by using a file on the FTP server.

Syntax

newer *remotefile* [*localfile*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

remotefile: Specifies a file on the FTP server.

localfile: Specifies the local file to be updated.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

If the local file does not exist, this command downloads the file from the FTP server and saves it locally.

If the file on the FTP server is not newer than the local file, this command does not update the local file.

Examples

Update the local file with the **a.txt** file on the FTP server.

```
ftp> newer a.txt
local: a.txt remote: a.txt
```

```
150 Connecting to port 63513
226 File successfully transferred
1573 bytes received in 0.0293 seconds (52.3 kbyte/s)
```

open

Use **open** to log in to an FTP server from FTP client view.

Syntax

open *server-address* [*service-port*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

server-address: Specifies the IPv4 address, IPv6 address, or host name of the FTP server.

service-port: Specifies the TCP port number of the FTP server, in the range of 0 to 65535. The default is 21.

Usage guidelines

After you issue this command, the system will prompt you to enter the username and password.

After you log in to one FTP server, you must disconnect from the server before you can use the **open** command to log in to another server.

Examples

In FTP client view, log in to FTP server 192.168.40.7.

```
<Sysname>ftp
ftp> open 192.168.40.7
Press CTRL+C to abort.
Connected to 192.168.40.7 (192.168.40.7).
220 FTP service ready.
User (192.168.40.7:(none)): root
331 Password required for root.
Password:
230 User logged in.
Remote system type is HPE.
ftp>
```

passive

Use **passive** to change the FTP operation mode.

Syntax

passive

Default

The FTP operation mode is passive.

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

FTP can operate in either of the following modes:

- **Active mode**—The FTP server initiates the TCP connection.
- **Passive mode**—The FTP client initiates the TCP connection.

When the FTP operation mode is passive, executing this command changes the mode to active.

When the FTP operation mode is active, executing this command changes the mode to passive.

This command is typically used together with a firewall to control FTP session establishment between private network users and public network users.

Examples

Change the FTP operation mode to passive.

```
ftp> passive
Passive mode on.
ftp> passive
Passive mode off.
```

put

Use **put** to upload a file from the FTP client to the FTP server.

Syntax

put *localfile* [*remotefile*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

localfile: Specifies the local file to be uploaded.

remotefile: Specifies the name of the file for saving the uploaded file on the FTP server.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

To upload a file in the current working directory, specify a file name without the path for the *localfile* argument, for example, a.cfg.

To upload a file in some other directory, specify a fully qualified file name for the *localfile* argument, for example, flash:/subdirectory/a.cfg.

Examples

Upload the **a.txt** file from the local working directory to the FTP server. Save the file as **b.txt**.

```
ftp> put a.txt b.txt
local: a.txt remote: b.txt
150 Connecting to port 47461
```

```
226 File successfully transferred
1569 bytes sent in 0.000671 seconds (2.23 Mbyte/s)
```

Upload the **a.txt** file from the **test** directory of the local working directory to the FTP server. Save the file as **b.txt**.

```
ftp> put flash:/test/a.txt b.txt
local: flash:/test/a.txt remote: b.txt
150 Connecting to port 47461
226 File successfully transferred
1569 bytes sent in 0.000671 seconds (2.23 Mbyte/s)
```

Upload file **a.txt** from the **test** directory of the storage medium on a member device. Save the file as **b.txt** on the FTP server.

```
ftp> put slot2#flash:/test/a.txt b.txt
local: slot2#flash:/test/a.txt remote: b.txt
150 Connecting to port 47461
226 File successfully transferred
1569 bytes sent in 0.000671 seconds (2.23 Mbyte/s)
```

Related commands

get

pwd

Use **pwd** to display the currently accessed directory on the FTP server.

Syntax

pwd

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Display the currently accessed directory on the FTP server.

```
ftp> cd subdir
250 OK. Current directory is /subdir
ftp> pwd
257 "/subdir" is your current location
```

quit

Use **quit** to terminate the connection to the FTP server and return to user view.

Syntax

quit

Views

FTP client view

Predefined user roles

network-admin

Examples

Terminate the connection to the FTP server and return to user view.

```
ftp> quit
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
<Sysname>
```

Related commands

bye

reget

Use **reget** to get the missing part of a file from the FTP server.

Syntax

reget *remotefile* [*localfile*]

Views

FTP client view

Predefined user roles

network-admin

network-operator

Parameters

remotefile: Specifies a file on the FTP server.

localfile: Specifies a local file.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

If a file download is not completed due to network or storage space problems, use this command to get the part that has not been downloaded yet.

Examples

Get the part of the **s.bin** file that has not been downloaded yet.

```
ftp> reget s.bin
local: s.bin remote: s.bin
350 Restarting at 1749706
150-Connecting to port 47429
150 38143.3 kbytes to download
226 File successfully transferred
39058742 bytes received in 66.2 seconds (576.1 kbyte/s)
```

rename

Use **rename** to rename a file.

Syntax

rename [*oldfilename* [*newfilename*]]

Views

FTP client view

Predefined user roles

network-admin

Parameters

oldfilename: Specifies the original file name.

newfilename: Specifies the new file name.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Rename the **a.txt** file as **b.txt**.

- Method 1:

```
ftp> rename
(from-name) a.txt
(to-name) b.txt
350 RNFR accepted - file exists, ready for destination
250 File successfully renamed or moved
```

- Method 2:

```
ftp> rename a.txt
(to-name) b.txt
350 RNFR accepted - file exists, ready for destination
250 File successfully renamed or moved
```

- Method 3:

```
ftp> rename a.txt b.txt
350 RNFR accepted - file exists, ready for destination
250 File successfully renamed or moved
```

reset

Use **reset** to clear the reply information received from the FTP server in the buffer.

Syntax

reset

Views

FTP client view

Predefined user roles

network-admin

Examples

Clear the reply information received from the FTP server.

```
ftp> reset
```

restart

Use **restart** to specify the file retransmission offset.

Syntax

restart *marker*

Views

FTP client view

Predefined user roles

network-admin

Parameters

marker: Specifies the retransmission offset, in bytes.

Usage guidelines

Use this command to continue with a file retransmission. The file retransmission starts from the (offset+1)th byte.

You can perform this operation only after you log in to the FTP server.

Support for this command depends on the FTP server.

Examples

Set retransmission offset to 2 bytes and retransmit the **h.c** file. The file has 82 bytes in total.

```
ftp> restart 2
restarting at 2. execute get, put or append to initiate transfer
ftp> put h.c h.c
local: h.c remote: h.c
350 Restart position accepted (2).
150 Ok to send data.
226 File receive OK.
80 bytes sent in 0.000445 seconds (175.6 kbyte/s)
ftp> dir
150 Here comes the directory listing.
-rw-r--r--    1 0        0              82 Jul 18 02:58 h.c
```

rhelp

Use **rhelp** to display the FTP commands supported by the FTP server.

Use **rhelp** *protocol-command* to display the help information for an FTP command supported by the FTP server.

Syntax

rhelp [*protocol-command*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

protocol-command: Specifies an FTP command.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Display the FTP-related commands supported by the FTP server.

```
ftp> rhelp
214-The following FTP commands are recognized
 USER PASS NOOP QUIT SYST TYPE
 HELP CWD  XCWD PWD  CDUP XCUP
 XPWD LIST NLST MLSD PORT EPRT
 PASV EPSV REST RETR STOR APPE
 DELE MKD  XMKD RMD  XRMD ABOR
 SIZE RNFR RNTO
214 UNIX Type: L8
```

Table 15 Command output

Field	Description
USER	Username.
PASS	Password.
NOOP	Null operation.
SYST	System parameters.
TYPE	Request type.
CWD	Changes the current working directory.
XCWD	Extended command with the meaning of CWD.
PWD	Prints the working directory.
CDUP	Changes the directory to the upper directory.
XCUP	Extended command with the meaning of CDUP.
XPWD	Extended command with the meaning of PWD.
LIST	Lists files.
NLST	Lists brief file description.
MLSD	Lists file content.
PORT	Active mode (IPv4).
EPRT	Active mode (IPv6).
PASV	Passive mode (IPv4).
EPSV	Passive mode (IPv6).
REST	Restarts.
RETR	Downloads files.
STOR	Uploads files.
APPE	Appends uploading.

Field	Description
DELE	Deletes files.
MKD	Creates folders.
XMKD	Extended command with the meaning of MKD.
RMD	Deletes folders.
XRMD	Extended command with the meaning of RMD.
ABOR	Aborts the transmission.
SIZE	Size of the transmission file.
RNFR	Original name.
RNTO	New name.

rmdir

Use **rmdir** to permanently delete a directory from the FTP server.

Syntax

rmdir *directory*

Views

FTP client view

Predefined user roles

network-admin

Parameters

directory: Specifies a directory on the FTP server.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

To perform this operation, you must have delete permission on the FTP server.

Delete all files and subdirectories in a directory before you delete the directory. For more information about how to delete files, see the **delete** command.

The **rmdir** command does not delete the files of the specified directory from the recycle bin.

Examples

Delete empty directory **subdir1**.

```
ftp>rmdir subdir1
250 The directory was successfully removed
```

Related commands

delete

rstatus

Use **rstatus** to display FTP server status information.

Use **rstatus** *remotefile* to display detailed information about a directory or file on the FTP server.

Syntax

rstatus [*remotefile*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

remotefile: Specifies a directory or file on the FTP server.

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Support for this command depends on the FTP server.

Examples

Display FTP server status information.

```
ftp> rstatus
211-FTP server status:
     Connected to 192.168.20.177
     Logged in as root
     TYPE: ASCII
     No session bandwidth limit
     Session timeout in seconds is 300
     Control connection is plain text
     Data connections will be plain text
     At session startup, client count was 1
     vsFTPd 2.0.6 - secure, fast, stable
211 End of status
```

Table 16 Command output

Filed	Description
211-FTP server status:	Beginning of the display of FTP server status, where 211 specifies the FTP command.
Connected to 192.168.20.177	IP address of the FTP client.
Logged in as root	Login username root.
TYPE: ASCII	File transfer mode ASCII.
Session timeout in seconds is 300	FTP connection idle-timeout interval is 300 seconds.
Control connection is plain text	Control connection type is plain text.
Data connections will be plain text	Data connection type is plain text.
At session startup, client count was 1	FTP connection number is 1.
vsFTPd 2.0.6 - secure, fast, stable	FTP version is 2.0.6.
211 End of status	End of the display of FTP server status.

Display the file **a.txt**.

```
ftp> rstatus a.txt
213-Status follows:
```

```
-rw-r--r--    1 0        0              80 Jul 18 02:58 a.txt
213 End of status
```

Table 17 Command output

Field	Description
213-Status follows:	Beginning of the display of the file, where 213 specifies the FTP command.
-rw-r--r--	The first bit specifies the file type. • **-**—Common. • **B**—Block. • **c**—Character. • **d**—Directory. • **l**—Symbol connection file. • **p**—Pipe. • **s**—socket. The second bit through the tenth bit are divided into three groups. Each group contains three characters, representing the access permission of the owner, group, and other users. • **-**—No permission. • **r**—Read permission. • **w**—Write permission. • **x**—Execution permission.
1	Number of connections.
0	Name of the file owner.
0	Group number of the file owner.
80	File size, in bytes.
Jul 18 02:58	Date and time when the file was most recently modified.
a.txt	File name.
213 End of status	End of the display of the file information.

status

Use **status** to display FTP status information.

Syntax

status

Views

FTP client view

Predefined user roles

network-admin

Examples

Display FTP status information.

```
ftp> status
Connected to 192.168.1.56.
No proxy connection.
Not using any security mechanism.
Mode: stream; Type: ascii; Form: non-print; Structure: file
```

```
Verbose: on; Bell: off; Prompting: on; Globbing: off
Store unique: off; Receive unique: off
Case: off; CR stripping: on
Ntrans: off
Nmap: off
Hash mark printing: off; Use of PORT cmds: on
```

Table 18 Command output

Field	Description
Connected to 192.168.1.56.	IP address of the FTP server that is connected to the FTP client.
Verbose: on; Bell: off; Prompting: on; Globbing: off	Displays debugging information.
Store unique: off; Receive unique: off	The name of the file on the FTP server is unique and the name of the local file is unique.
Case: off; CR stripping: on	Does not support obtaining multiple files once and deletes "\r" when downloading text files.
Ntrans: off	Does not use the input-output transmission table.
Nmap: off	The file name does not use the input-to-output mapping template.
Hash mark printing: off; Use of PORT cmds: on	Does not end with a pound sign (#) and uses "PORT" data transmission.

system

Use **system** to display the system information of the FTP server.

Syntax

system

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

You can perform this operation only after you log in to the FTP server.

Examples

Display the system information of the FTP server.

```
ftp> system
215 UNIX Type: L8
```

user

Use **user** to initiate an FTP authentication on the current FTP connection.

Syntax

user *username* [*password*]

Views

FTP client view

Predefined user roles

network-admin

Parameters

username: Specifies the username.

password: Specifies the password.

Usage guidelines

If you tried to access an FTP server but failed to pass the authentication, you can use this command to try again before the connection to the FTP server expires.

After you log in to an FTP server, you can initiate an FTP authentication to change to a new account. By changing to a new account, you can get a different privilege without re-establishing the FTP connection.

Make sure the specified username and password have been configured on the FTP server. If the username or password is not configured, this command fails and the FTP connection is closed.

Examples

After logging in to the FTP server, use username **ftp** and password **123456** to log in again to the FTP server.

- Method 1:

```
ftp> user ftp 123456
331 Password required for ftp.
230 User logged in.
```

- Method 2:

```
ftp> user ftp
331 Password required for ftp.
Password:
230 User logged in.
```

verbose

Use **verbose** to enable or disable the device to display detailed information about FTP operations.

Syntax

verbose

Default

The device displays detailed information about FTP operations.

Views

FTP client view

Predefined user roles

network-admin

Usage guidelines

This command affects only the current FTP session.

Examples

Disable the device from displaying detailed information about FTP operations.

```
ftp> verbose
Verbose mode off.
```

Execute the **get** command.

```
ftp> get a.cfg 1.cfg
```

Enable the device to display detailed information about FTP operations.

```
ftp> verbose
Verbose mode on.
```

Execute the **get** command.

```
ftp> get a.cfg 2.cfg
227 Entering Passive Mode (192,168,1,58,68,14)
150-Accepted data connection
150 The computer is your friend. Trust the computer
226 File successfully transferred
3796 bytes received in 0.00762 seconds (486.5 kbyte/s)
```

TFTP commands

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

TFTP is not supported in FIPS mode.

tftp

Use **tftp** to download a file from a TFTP server or upload a file to a TFTP server in an IPv4 network.

Syntax

tftp *tftp-server* { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**vpn-instance** *vpn-instance-name*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

tftp-server: Specifies the IPv4 address or host name of a TFTP server. The host name can be a case-insensitive string of 1 to 253 characters and can contain only letters, digits, hyphens (-), underscores (_), and dots (.).

get: Downloads a file and writes the file directly to the destination folder. If the destination folder already has a file with the same name, the system deletes the existing file before starting the download operation. The existing file is permanently deleted even if the download operation fails.

put: Uploads a file.

sget: Downloads a file and saves the file to memory before writing it to the destination folder. The system starts to write the file to the destination folder only after the file is downloaded and saved to memory successfully. If the destination folder already has a file with the same name, the system overwrites the existing file. If the download or save-to-memory operation fails, the existing file in the destination folder is not overwritten.

source-filename: Specifies the source file name, a case-insensitive string of 1 to 1 to 255 characters.

destination-filename: Specifies the destination file name, a case-insensitive string of 1 to 255 characters. If this argument is not specified, the file uses the source file name.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the TFTP server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the TFTP server belongs to the public network, do not specify this option.

dscp *dscp-value*: Specifies the DSCP value for IPv4 to use for outgoing TFTP packets to indicate the packet transmission priority. The value range is 0 to 63. The default is 0.

source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }: Specifies the source address for outgoing TFTP packets. If you do not specify this option, the device uses the primary IPv4 address of the output interface for the route to the TFTP server as the source address.

- **interface** *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's primary IPv4 address as the source IPv4 address. For successful TFTP packet transmission, make sure the interface is up and has the primary IPv4 address configured.
- **ip** *source-ip-address*: Specifies an IPv4 address. For successful TFTP packet transmission, make sure this address is the IPv4 address of an interface in up state on the device.

Usage guidelines

The source address specified with the **tftp** command takes precedence over the source address specified with the **tftp client source** command.

The source address specified with the **tftp client source** command applies to all TFTP connections. The source address specified with the **tftp** command applies only to the current TFTP connection.

Examples

Download the **new.bin** file from TFTP server 192.168.1.1 and save the file as **new.bin**.

```
<Sysname> tftp 192.168.1.1 get new.bin
Press CTRL+C to abort.
   % Total    % Received % Xferd  Average Speed   Time    Time     Time   Current
                                  Dload  Upload   Total   Spent    Left   Speed
100 13.9M  100 13.9M    0     0  1206k      0  0:00:11  0:00:11  --:--:-- 1206k
Writing file...Done.
<System>
```

Table 19 Command output

Field	Description
%	Percentage of file transmission progress.
Total	Size of files to be transmitted, in bytes.
%	Percentage of received file size to total file size.
Received	Received file size, in bytes.
%	Percentage of sent file size to total file size.
Xferd	Sent file size, in bytes.
Average Dload	Average download speed, in bps.
Speed Upload	Average upload speed, in bps.
Writing file…	The system was writing the downloaded file to the storage medium. This field is displayed only when the **get** or **sget** keyword is specified. If the operation succeeded, this command displays **Done** at the end of this field. If the operation failed, this command displays **Failed**.

Related commands

tftp client source

tftp client ipv6 source

Use **tftp client ipv6 source** to specify the source IPv6 address for TFTP packets sent to an IPv6 TFTP server.

Use **undo tftp client ipv6 source** to restore the default.

Syntax

tftp client ipv6 source { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }

undo tftp client ipv6 source

Default

No source address is specified for TFTP packets sent to an IPv6 TFTP server. The device selects a source IPv6 address as defined in RFC 3484.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's IPv6 address as the source address. For successful TFTP packet transmission, make sure the interface is up and is configured with an IPv6 address.

ipv6 *source-ipv6-address*: Specifies an IPv6 address . For successful TFTP packet transmission, make sure this address is the IPv6 address of an interface in up state on the device.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The source address specified with the **tftp ipv6** command takes precedence over the source address specified with the **tftp client ipv6 source** command.

The source address specified with the **tftp client ipv6 source** command applies to all TFTP connections. The source address specified with the **tftp ipv6** command applies only to the TFTP connection that is being established.

Examples

Specify the source IPv6 address of 2000::1 for TFTP packets sent to an IPv6 TFTP server.

```
<Sysname> system-view
[Sysname] tftp client ipv6 source ipv6 2000::1
```

Related commands

tftp ipv6

tftp client source

Use **tftp client source** to specify the source IPv4 address for TFTP packets sent to an IPv4 TFTP server.

Use **undo tftp client source** to restore the default.

Syntax

tftp client source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }

undo tftp client source

Default

No source IPv4 address is specified for TFTP packets sent to an IPv4 TFTP server. The device uses the primary IPv4 address of the output interface for the route to the server as the source address.

Views

System view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's primary IPv4 address as the source address. For successful TFTP packet transmission, make sure the interface is up and has the primary IPv4 address configured.

ip *source-ip-address*: Specifies an IPv4 address. For successful TFTP packet transmission, make sure this address is the IPv4 address of an interface in up state on the device.

Usage guidelines

If you execute this command multiple times, the most recent configuration takes effect.

The source address specified with the **tftp** command takes precedence over the source address specified with the **tftp client source** command.

The source address specified with the **tftp client source** command applies to all TFTP connections. The source address specified with the **tftp** command applies only to the TFTP connection that is being established.

Examples

Specify the source IP address of 192.168.20.222 for TFTP packets sent to an IPv4 TFTP server.

```
<Sysname> system-view
[Sysname] tftp client source ip 192.168.20.222
```

Related commands

tftp

tftp ipv6

Use **tftp ipv6** to download a file from a TFTP server or upload a file to a TFTP server in an IPv6 network.

Syntax

tftp ipv6 *tftp-server* [**-i** *interface-type interface-number*] { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**vpn-instance** *vpn-instance-name*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }] *

Views

User view

Predefined user roles

network-admin

Parameters

tftp-server: Specifies the IPv6 address or host name of a TFTP server. The host name can be a case-insensitive string of 1 to 253 characters and can contain only letters, digits, hyphens (-), underscores (_), and dots (.).

-i *interface-type interface-number*: Specifies an output interface by its type and number. This option can be used only when the TFTP server address is a link local address and the specified output interface has a link local address. For information about link local addresses, see *Layer 3—IP Services Configuration Guide*.

get: Downloads a file and writes the file directly to the destination folder. If the destination folder already has a file with the same name, the system deletes the existing file before starting the download operation. The existing file is permanently deleted even if the download operation fails.

put: Uploads a file.

sget: Downloads a file and saves the file to memory before writing it to the destination folder. The system starts to write the file to the destination folder only after the file is downloaded and saved to memory successfully. If the destination folder already has a file using the same name, the system overwrites the existing file. If the download or save-to-memory operation fails, the existing file in the destination folder is not overwritten.

source-filename: Specifies the source file name, a case-insensitive string of 1 to 255 characters.

destination-filename: Specifies the destination file name, a case-insensitive string of 1 to 255 characters. If this argument is not specified, the file uses the source file name.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the TFTP server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the TFTP server belongs to the public network, do not specify this option.

dscp *dscp-value*: Specifies the DSCP value for IPv6 to use in outgoing TFTP packets to indicate the packet transmission priority. The value range is 0 to 63. The default is 0.

source { **interface** *interface-type interface-number* | **ipv6** *source-ipv6-address* }: Specifies the source address for outgoing TFTP packets. If you do not specify this option, the device selects a source IPv6 address as defined in RFC 3484.

- **interface** *interface-type interface-number*: Specifies an interface by its type and number. The device will use the interface's IPv6 address as the source IPv6 address. For successful TFTP packet transmission, make sure the interface is up and is configured with an IPv6 address.
- **ipv6** *source-ipv6-address*: Specifies an IPv6 address. For successful TFTP packet transmission, make sure this address is the IPv6 address of an interface in up state on the device.

Usage guidelines

The source address specified with the **tftp ipv6** command takes precedence over the source address specified with the **tftp client ipv6 source** command.

The source address specified with the **tftp client ipv6 source** command applies to all TFTP connections. The source address specified with the **tftp ipv6** command applies only to the current TFTP connection.

Examples

Download the **new.bin** file from TFTP server 2001::1 and save the file as **new.bin**.

```
<Sysname> tftp ipv6 2001::1 get new.bin new.bin
Press CTRL+C to abort.
   % Total    % Received % Xferd  Average Speed   Time    Time     Time   Current
                                  Dload  Upload   Total   Spent    Left   Speed
100 13.9M  100 13.9M    0     0  1206k      0  0:00:11  0:00:11  --:--:-- 1206k
Writing file...Done.
```

For more information about the command output, see Table 19.

tftp-server acl

Use **tftp-server acl** to use an ACL to control the device's access to TFTP servers in an IPv4 network.

Use **undo tftp-server acl** to restore the default.

Syntax

tftp-server acl *acl-number*

undo tftp-server acl

Default

No ACL is used to control the device's access to TFTP servers.

Views

System view

Predefined user roles

network-admin

Parameters

acl-number: Specifies the number of a basic ACL, in the range of 2000 to 2999.

Usage guidelines

You can use an ACL to deny or permit the device's access to specific TFTP servers.

Examples

Allow the device to access only TFTP server 1.1.1.1.

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] tftp-server acl 2000
```

tftp-server ipv6 acl

Use **tftp-server ipv6 acl** to use an ACL to control the device's access to TFTP servers in an IPv6 network.

Use **undo tftp-server ipv6 acl** to restore the default.

Syntax

tftp-server ipv6 acl *ipv6-acl-number*

undo tftp-server ipv6 acl

Default

No ACL is used to control the device's access to TFTP servers.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6-acl-number: Specifies the number of a basic ACL, in the range of 2000 to 2999.

Usage guidelines

You can use an ACL to deny or permit the device's access to specific TFTP servers.

Examples

Allow the device to access only TFTP server 2001::1.

```
<Sysname> System-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl-ipv6-basic-2001] rule permit source 2001::1/128
[Sysname-acl-ipv6-basic-2001] quit
[Sysname] tftp-server ipv6 acl 2001
```

File system management commands

IMPORTANT:

- Before managing storage media, file systems, directories, and files, make sure you know the possible impact.
- A file or directory whose name starts with a dot character (.) is a hidden file or directory. To prevent the system from hiding a file or directory, make sure the file or directory name does not start with a dot character.
- Some system files and directories are hidden. For correct system operation and full functionality, do not modify or delete hidden files or directories.

File system names, directory names, and file names must be compliant with the naming conventions. For more information about the naming conventions and the methods for specifying the names, see file system management in *Fundamentals Configuration Guide*.

Before you use the **copy**, **delete**, **fixdisk**, **format**, **gunzip**, **gzip**, **mkdir**, **move**, **rename**, **rmdir**, or **undelete** command on a file system, make sure the file system is not write protected.

You cannot access a storage medium that is being partitioned, or a file system that is being formatted or repaired. To access the file system, wait for the ongoing operation to be completed and then use one of the following methods:

- Use the absolute path to specify a file or directory. For example, use the **dir flash:/** command to display the files and directories in the **flash:** file system.
- Use the **cd** command to change the working directory to the root directory of the file system before accessing a file or directory in the file system. For example, to display the files and directories in the root directory of the **flash:** file system, perform the following tasks:
  a. Use the **cd flash:/** command to change the working directory to the root directory of the file system.
  b. Execute the **dir** command.

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

cd

Use **cd** to change the working directory.

Syntax

cd { *directory* | **..** }

Views

User view

Predefined user roles

network-admin

Parameters

directory: Specifies the destination directory.

..: Specifies the parent directory. If the working directory is the root directory, an error message appears when you execute the **cd ..** command. No online help information is available for this keyword.

Examples

Access the **test** directory after logging in to the device.

```
<Sysname> cd test
```

Change to the parent directory.

```
<Sysname> cd ..
```

copy

Use **copy** to copy a file.

Syntax

In non-FIPS mode:

copy *source-file* { *dest-file* | *dest-directory* } [**vpn-instance** *vpn-instance-name*] [**source interface** *interface-type interface-number*]

In FIPS mode:

copy *source-file* { *dest-file* | *dest-directory* }

Views

User view

Predefined user roles

network-admin

Parameters

source-file: Specifies the name or URL of the file to be copied in non-FIPS mode, and specifies the name of the file to be copied in FIPS mode. If the file resides on an FTP, TFTP, or HTTP server rather than on the device, specify the URL of the file. Whether a URL is case sensitive depends on the server.

dest-file: Specifies the name or URL for the destination file in non-FIPS mode, and specifies the name for the destination file in FIPS mode. To copy the source file to an FTP, TFTP, or HTTP server, specify a URL. Whether a URL is case sensitive depends on the server.

dest-directory: Specifies the destination directory or URL in non-FIPS mode, and specifies the destination directory in FIPS mode. To copy the source file to an FTP, TFTP, or HTTP server, specify a URL. The device copies the source file to the destination location and saves the file with its original file name. Whether a URL is case sensitive depends on the server.

vpn-instance *vpn-instance-name*: Specifies the MPLS L3VPN instance to which the destination FTP, TFTP, or HTTP server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the server belongs to the public network, do not specify this option.

source interface *interface-type interface-number*: Specifies the source interface used to connect to the server. After you specify the source interface, the device uses the primary IP address of the source interface as the source IP address for outgoing packets. If you do not specify this option, the device uses the outgoing interface as the source interface.

Usage guidelines

In FIPS mode, the **copy** command can only copy a local file and save it locally.

In non-FIPS mode, you can use the **copy** command to perform the following tasks:

- Copy a local file and save it locally.
- Copy a local file and save it to an FTP, TFTP, or HTTP server.
- Copy a file from an FTP, TFTP, or HTTP server and save it locally.

To specify a file or directory, use the following guidelines:

Location	Name format	Remarks
On the device	Use the file name guidelines in *Fundamentals Configuration Guide*.	N/A
On an FTP server	Enter the URL in the format of **ftp://***FTP username*[**:***password*]*@server address*[**:***port number*]**/***file path*[**/***file name*].	The username and password must be the same as the username and password configured on the FTP server. If the server authenticates users only by the username, you are not required to enter the password. For example, to use the username a and password 1 and specify the startup.cfg file in the authorized working directory on the FTP server 1.1.1.1, enter ftp://a:1@1.1.1.1/startup.cfg.
On a TFTP server	Enter the URL in the format of **tftp://***server address*[**:***port number*]**/***file path*[**/***file name*].	For example, to specify the startup.cfg file in the working directory on TFTP server 1.1.1.1, enter the URL tftp://1.1.1.1/startup.cfg.
On an HTTP server	Enter the URL in the format of **http://**[*HTTP username*[**:***password*]@]*server address*[**:***port number*]**/***filepath*[**/***file name*].	The username and password in the URL must be the same as the username and password configured on the server. If only the username is required for authentication, you do not need to enter the password. If authentication is not required, you do not need to enter the username or password. For example, the **startup.cfg** file is saved in the authorized directory on the HTTP server at 1.1.1.1. The HTTP account username and password are **a** and **1**, respectively. To copy the file, enter the URL http://a:1@1.1.1.1/startup.cfg. If authentication is not required, enter the URL http://1.1.1.1/startup.cfg.

To specify an IPv6 address, enclose the IPv6 address in square brackets ([ ]), for example, ftp://test:test@[2001::1]:21/test.cfg.

Examples

Copy the **test.cfg** file in the current directory and save it to the current directory as **testbackup.cfg**.

```
<Sysname> copy test.cfg testbackup.cfg
Copy flash:/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file flash:/test.cfg to flash:/testbackup.cfg...Done.
```

Copy the **1.cfg** file from the **flash:** file system's **test** directory to the USB disk. Save the copy to the **testbackup** directory on the first partition as **1backup.cfg**.

```
<Sysname> copy flash:/test/1.cfg usba0:/testbackup/1backup.cfg
Copy flash:/test/1.cfg to usba0:/testbackup/1backup.cfg? [Y/N]:y
Copying file flash:/test/1.cfg to usba0:/testbackup/1backup.cfg...Done.
```

Copy the **test.cfg** file in the current directory and save it to the root directory of a file system in a specific slot as **testbackup.cfg**.

```
<Sysname> copy test.cfg slot2#flash:/
Copy flash:/test.cfg to slot2#flash:/test.cfg? [Y/N]:y
Copying file flash:/test.cfg to slot2#flash:/test.cfg...Done.
```

Copy **test.cfg** from the working directory on FTP server 1.1.1.1. Save the copy to the local current directory as **testbackup.cfg.** The FTP username is **user**. The password is **private**.

```
<Sysname> copy ftp://user:private@1.1.1.1/test.cfg testbackup.cfg
```

```
Copy ftp://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file ftp://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the current directory. Save the copy to the working directory on FTP server 1.1.1.1 as **testbackup.cfg**. The FTP username is **user**. The password is **private**.

```
<Sysname> copy test.cfg ftp://user:private@1.1.1.1/testbackup.cfg
Copy flash:/test.cfg to ftp://user:private@1.1.1.1/testbackup.cfg? [Y/N]:y
Copying file flash:/test.cfg to ftp://user:private@1.1.1.1/testbackup.cfg... Done.
```

Copy **test.cfg** from the working directory on TFTP server 1.1.1.1. Save the copy to the local current directory as **testbackup.cfg**.

```
<Sysname> copy tftp://1.1.1.1/test.cfg testbackup.cfg
Copy tftp://1.1.1.1/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file tftp://1.1.1.1/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the current directory. Save the copy to the working directory on TFTP server 1.1.1.1 as **testbackup.cfg**.

```
<Sysname> copy test.cfg tftp://1.1.1.1/testbackup.cfg
Copy flash:/test.cfg to tftp://1.1.1.1/testbackup.cfg? [Y/N]:y
Copying file flash:/test.cfg to tftp://1.1.1.1/testbackup.cfg... Done.
```

Copy **test.cfg** from the working directory on FTP server 1.1.1.1. Save the copy to the local current directory as **testbackup.cfg**. The FTP username is **user**. The password is **private**. The FTP server belongs to VPN instance vpn1.

```
<Sysname> copy ftp://user:private@1.1.1.1/test.cfg testbackup.cfg vpn-instance vpn1
Copy ftp://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file ftp://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the working directory on TFTP server 1.1.1.1. Save the copy to the local current directory as **testbackup.cfg**. The TFTP server belongs to VPN instance vpn1.

```
<Sysname> copy tftp://1.1.1.1/test.cfg testbackup.cfg vpn-instance vpn1
Copy tftp://1.1.1.1/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file tftp://1.1.1.1/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the working directory on FTP server 2001::1. Save the copy to the local current directory as **testbackup.cfg**. The FTP username is **user**. The password is **private**.

```
<Sysname> copy ftp://user:private@[2001::1]/test.cfg testbackup.cfg
Copy ftp://user:private@[2001::1]/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file ftp://user:private@[2001::1]/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the working directory on TFTP server 2001::1. Save the copy to the local current directory as **testbackup.cfg**.

```
<Sysname> copy tftp://[2001::1]/test.cfg testbackup.cfg
Copy tftp://[2001::1]/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file tftp://[2001::1]/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the authorized directory on HTTP server 1.1.1.1. Save the copy to the local current directory as **testbackup.cfg**. The HTTP login username is **user**. The password is **private**.

```
<Sysname> copy http://user:private@1.1.1.1/test.cfg testbackup.cfg
Copy http://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file http://user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg... Done.
```

Copy **test.cfg** from the current directory. Save the copy to the authorized directory on HTTP server 1.1.1.1 as **testbackup.cfg**. The HTTP login username is **user**. The password is **private**.

```
<Sysname> copy test.cfg http://user:private@1.1.1.1/testbackup.cfg
Copy flash:/test.cfg to http://user:private@1.1.1.1/testbackup.cfg? [Y/N]:y
Copying file flash:/test.cfg to http://user:private@1.1.1.1/testbackup.cfg... Done.
```

Copy **test.cfg** from the authorized directory on HTTP server 2001::1. Save the copy to the local current directory as **testbackup.cfg**. The HTTP login username is **user**. The password is **private**.

```
<Sysname> copy http://user:private@[2001::1]/test.cfg testbackup.cfg
Copy http://user:private@[2001::1]/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file http://user:private@[2001::1]/test.cfg to flash:/testbackup.cfg... Done.
```

delete

Use **delete** to delete a file.

Syntax

delete [**/unreserved**] *file*

Views

User view

Predefined user roles

network-admin

Parameters

/unreserved: Permanently deletes the specified file. If you do not specify this keyword, the command moves the file to the recycle bin.

file: Specifies the name of the file to be deleted. Asterisks (*) are acceptable as wildcards. For example, to remove files with the **.txt** extension in the current directory, enter **delete *.txt**.

Usage guidelines

The **delete /unreserved** *file* command deletes a file permanently. The file cannot be restored.

The **delete** *file* command (without **/unreserved**) moves a file to the recycle bin.

A file moved to the recycle bin can be restored by using the **undelete** command.

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

If you delete two files that have the same name from different directories, both files are retained in the recycle bin. If you successively delete two files that have the same name from the same directory, only the most recently deleted file is retained in the recycle bin.

Examples

Remove the **1.cfg** file from the current directory.

```
<Sysname> delete 1.cfg
Delete flash:/1.cfg? [Y/N]:y
Deleting file flash:/1.cfg...Done.
```

Permanently delete the **1.cfg** file from the current directory.

```
<Sysname> delete /unreserved 1.cfg
The file cannot be restored. Delete flash:/1.cfg? [Y/N]:y
Deleting the file permanently will take a long time. Please wait...
Deleting file flash:/1.cfg...Done.
```

Related commands

reset recycle-bin

undelete

dir

Use **dir** to display files or directories.

Syntax

dir [**/all**] [*file* | *directory* | **/all-filesystems**]

Views

User view

Predefined user roles

network-admin

Parameters

/all: Displays all files and directories in the current directory, visible or hidden. If you do not specify this option, only visible files and directories are displayed.

file: Displays a specific file. This argument can use the asterisk (*) as a wildcard. For example, to display files with the **.txt** extension in the current directory, enter **dir *.txt**.

directory: Displays a specific directory.

/all-filesystems: Displays files and directories in the root directories of all file systems on the device.

Usage guidelines

If no option is specified, the command displays all visible files and directories in the current directory.

The directory name of the recycle bin is **.trash**. To display files in the recycle bin, use either of the following methods:

- Execute the **dir /all .trash** command.
- Execute the **cd .trash** command and then the **dir** command.

If multiple users perform file operations (for example, creating or deleting files or directories) at the same time, the output for this command might be incorrect.

Examples

Display information about all files and directories in the current directory.

```
<Sysname> dir /all
Directory of flash:/
...
```

Display files and directories in the root directories of all file systems on the device.

```
<Sysname> dir /all-filesystems
Directory of flash:/
...

Directory of usba0:/
...
```

Table 20 Command output

Field	Description
Directory of	Current directory.

Field	Description
0 -rwh 3144 Apr 26 2014 13:45:28 xx.xx	File or directory information: • **0**—File or directory number, which is automatically allocated by the system. • **-rwh**—Attributes of the file or directory. The first character is the directory indicator (**d** for directory and **–** for file). The second character indicates whether the file or directory is readable (**r** for readable). The third character indicates whether the file or directory is writable (**w** for writable). The fourth character indicates whether the file or directory is hidden (**h** for hidden, **-** for visible). Modifying, renaming, or deleting hidden files might affect functions. • **3144**—File size in bytes. For a directory, a hyphen (-) is displayed. • **Apr 26 2014 13:45:28**—Last date and time when the file or directory was modified. • **xx.xx**—File or directory name.

execute

Use **execute** to execute a batch file.

Syntax

execute *filename*

Views

System view

Predefined user roles

network-admin

Parameters

filename: Specifies the name of a batch file.

Usage guidelines

A batch file contains a set of commands. Executing a batch file executes the commands in the file one by one.

To execute a batch file on the device, create a batch file on a PC and load the batch file to the device.

As a best practice, try every command on the device to make sure the command line can be executed correctly before adding the command to a batch file. If a command is invalid or a condition for executing the command is not met, the command fails and the system continues to execute the next command.

When executing an interactive command in a batch file, the system uses the default inputs.

Examples

Execute batch file **test.bat**.

```
<Sysname> fdisk usba: 3
[Sysname] execute test.bat
```

fdisk

Use **fdisk** to partition a storage medium.

Syntax

fdisk *medium* [*partition-number*]

Views

User view

Predefined user roles

network-admin

Parameters

medium: Specifies the name of the storage medium to be partitioned.

partition-number: Specifies the number of partitions, in the range of 1 to 4. If you specify this argument, the storage medium is divided evenly into the specified number of partitions. To customize the sizes of partitions, do not provide this argument.

Usage guidelines

The flash memory cannot be partitioned. A partition cannot be partitioned.

Before partitioning a storage medium, perform the following tasks:

- Back up the files in the storage medium. The partition operation clears all data on the medium.
- Make sure no other users are accessing the medium.
- Make sure the storage medium to be partitioned is not write protected. If the storage medium is write protected, the operation will fail, and you must remount or reinstall the storage medium to restore access to the storage medium.

After partitioning a storage medium, you must format the partitions to create the file systems before you can access the file systems.

The actual partition size and the specified partition size might have a difference of less than 5% of the storage medium's total size.

To change the sizes of partitions on a storage medium, partition the storage medium again and specify the required sizes for the partitions.

Before removing a partitioned storage medium, you must unmount all file systems on the storage medium.

Examples

Divide the USB disk on the device evenly into three partitions.

```
<Sysname> fdisk usba: 3
Capacity of usba: : 256M bytes
usba: will be divided into the following partitions:
DeviceName      Capacity
usba0:            85MB
usba1:            85MB
usba2:            86MB
All data on usba: will be lost, continue? [Y/N]:y
Partitioning usba:...Done.
```

Divide the USB disk on the device into one partition.

```
<Sysname> fdisk usba:
The capacity of usba: : 256M bytes
Partition 1 (32MB~224MB, 256MB. Press CTRL+C to quit or Enter to use all available space):
```

// Press **Enter** or enter **256.**

```
usba: will be divided into the following partition(s):
DeviceName    Capacity
usba0:          256MB
All data on usba: will be lost, continue? [Y/N]:y
```

```
Partitioning usba:...Done.
```

Divide the USB disk on the device into three partitions and specify the size for each partition.

```
<Sysname> fdisk usba:
The capacity of usba: : 256M bytes
Partition 1 (32MB~224MB, 256MB, Press CTRL+C to quit or Enter to use all available
space):128
```

// Enter **128** to set the size of the first partition to 128 MB.

```
Partition 2 (32MB~96MB, 128MB, Press CTRL+C to quit or Enter to use all available space):31
```

// Enter **31** to set the size of the second partition to 31 MB.

```
The partition size must be greater than or equal to 32MB.
Partition 2 (32MB~96MB, 128MB, Press CTRL+C to quit or Enter to use all available
space):1000
```

// Enter **1000** to set the size of the second partition to 1000 MB.

```
The partition size must be less than or equal to 128MB.
Partition 2 (32MB~96MB, 128MB, Press CTRL+C to quit or Enter to use all available space):127
```

// Enter **127** to set the size of the second partition to 127 MB.

```
The remaining space is less than 32MB. Please enter the size of partition 2 again.
Partition 2 (32MB~96MB, 128MB, Press CTRL+C to quit or Enter to use all available space):56
```

// Enter **56** to set the size of the second partition to 56 MB.

```
Partition 3 (32MB~40MB, 72MB, Press CTRL+C to quit or Enter to use all available space):
```

// Press **Enter** to assign the remaining space to the third partition.

```
usba: will be divided into the following partition(s):
DeviceName     Capacity
usba0:            128MB
usba1:            56MB
usba2:            72MB
All data on usba: will be lost, continue? [Y/N]:y
Partitioning usba:...Done.
```

file prompt

Use **file prompt** to set the operation mode for files and directories.

Use **undo file prompt** to restore the default.

Syntax

file prompt { **alert** | **quiet** }

undo file prompt

Default

The operation mode is **alert**. The system prompts for confirmation when you perform a destructive file or directory operation.

Views

System view

Predefined user roles

network-admin

Parameters

alert: Prompts for confirmation when a destructive file or directory operation is being performed.

quiet: Gives no confirmation prompt for file or directory operations except the recycle bin emptying operation.

Usage guidelines

In quiet mode, the system does not prompt for confirmation when a user performs a file or directory operation except the recycle bin emptying operation. The **alert** mode provides an opportunity to cancel a disruptive operation.

Examples

Set the file and directory operation mode to **alert**.

```
<Sysname> system-view
[Sysname] file prompt alert
```

fixdisk

Use **fixdisk** to check a file system for damage and repair any damage.

Syntax

fixdisk *filesystem*

Views

User view

Predefined user roles

network-admin

Parameters

filesystem: Specifies the name of a file system.

Usage guidelines

Use this command to fix a file system when space in the file system cannot be used or released.

You can repair a file system only when no other users are accessing the file system.

Examples

Repair file system **flash:**.

```
<Sysname> fixdisk flash:
Restoring flash: may take some time...
Restoring flash:...Done.
```

format

Use **format** to format a file system.

Syntax

format *filesystem*

Views

User view

Predefined user roles

network-admin

Parameters

filesystem: Specifies the name of a file system.

Usage guidelines

The device requires that the file systems on hot swappable storage media be VFAT file systems. To use a file system of a different type on the device, you must use this command to format the file system.

Formatting a file system permanently deletes all files in the file system. If a startup configuration file exists in the file system, back up the file if necessary.

You can format a file system only when no other users are accessing the file system.

A file system to be formatted cannot contain security log files. Only a user with the security-audit user role can delete security log files. For more information about the security-audit user role, see RBAC in *Fundamentals Configuration Guide*.

Examples

Format file system **flash:**.

```
<Sysname> format flash:
All data on flash: will be lost, continue? [Y/N]:y
Formatting flash:... Done.
```

Format the file system on the third partition of the USB disk.

```
<Sysname> format usba2:
All data on usba2: will be lost, continue? [Y/N]:y
Formatting usba2:... Done.
```

gunzip

Use **gunzip** to decompress a file.

Syntax

gunzip *file*

Views

User view

Predefined user roles

network-admin

Parameters

file: Specifies the name of the file to be decompressed. This argument must use the **.gz** extension.

Usage guidelines

This command deletes the specified file after decompressing it.

Examples

Decompress file **system.bin.gz**:

1. Before decompressing the file, you can display files whose names start with the **system.** string.

```
<Sysname> dir system.*
Directory of flash:
   1 -rw-          20 Jun 14 2012 10:18:53   system.bin.gz
```

```
3710740 KB total (472844 KB free)
```

2. Decompress the file **system.bin.gz**.

```
<Sysname> gunzip system.bin.gz
Decompressing file flash:/system.bin.gz..... Done.
```

3. Verify the decompress operation.

```
<Sysname> dir system.*
Directory of flash:
   1 -rw-           0 May 30 2012 11:42:25   system.bin


3710740 KB total (472840 KB free)
```

gzip

Use **gzip** to compress a file.

Syntax

gzip *file*

Views

User view

Predefined user roles

network-admin

Parameters

file: Specifies the name of the file to be compressed.

Usage guidelines

This command saves the compressed file to the *file***.gz** file and deletes the source file.

Examples

Compress file **system.bin**:

1. Before compressing the file, you can display files whose names start with the **system.** string.

```
<Sysname> dir system.*
Directory of flash:
   1 -rw-           0 May 30 2012 11:42:24   system.bin


3710740 KB total (472840 KB free)
```

2. Compress the file **system.bin**.

```
<Sysname> gzip system.bin
Compressing file flash:/system.bin..... Done.
```

3. Verify the compress operation.

```
<Sysname> dir system.*
Directory of flash:
   1 -rw-          20 Jun 14 2012 10:18:53   system.bin.gz


3710740 KB total (472844 KB free)
```

md5sum

Use **md5sum** to use the MD5 algorithm to calculate the digest of a file.

Syntax

md5sum *file*

Views

User view

Predefined user roles

network-admin

network-operator

Parameters

file: Specifies the name of a file.

Usage guidelines

You can use file digests to verify file integrity.

Examples

Use the MD5 algorithm to calculate the digest of file **system.bin**.

```
<Sysname> md5sum system.bin
MD5 digest:
4f22b6190d151a167105df61c35f0917
```

mkdir

Use **mkdir** to create a directory.

Syntax

mkdir *directory*

Views

User view

Predefined user roles

network-admin

Parameters

directory: Specifies a directory.

Usage guidelines

The name of the directory to be created must be unique in the parent directory.

You can create a directory only in an existing directory. For example, to create the **flash:/test/mytest** directory, make sure the **test** directory already exists.

Examples

Create the **test** directory in the current directory.

```
<Sysname> mkdir test
Creating directory flash:/test... Done.
```

Create the **test/subtest** directory in the current directory.

```
<Sysname> mkdir test/subtest
```

```
Creating directory flash:/test/subtest... Done.
```

more

Use **more** to display the contents of a text file.

Syntax

more *file*

Views

User view

Predefined user roles

network-admin

Parameters

file: Specifies the name of a file.

Examples

Display the contents of the **test.txt** file.

```
<Sysname> more test.txt
Have a nice day.
```

Display the contents of the **testcfg.cfg** file.

```
<Sysname> more testcfg.cfg

#
 version 7.1.070, Release 1201
#
 sysname Sysname
#
vlan 2
#
return
<Sysname>
```

mount

Use **mount** to mount a file system.

Syntax

mount *filesystem*

Views

User view

Predefined user roles

network-admin

Parameters

filesystem: Specifies the name of a file system.

Usage guidelines

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

To avoid file system corruption, do not perform the following tasks while the system is mounting a file system:

- Reboot, power cycle, or power off the device.
- Install or remove storage media.
- Perform a switchover.

To remove a hot-swappable storage medium from the device, you must first unmount all file systems on the storage medium. Removing a mounted hot-swappable storage medium might damage files on the storage medium or even the storage medium.

Examples

Mount a file system on the USB disk.

```
<Sysname> mount usba0:
```

Related commands

umount

move

Use **move** to move a file.

Syntax

move *source-file* { *dest-file* | *dest-directory* }

Views

User view

Predefined user roles

network-admin

Parameters

source-file: Specifies the name of the source file.

dest-file: Specifies the name of the destination file.

dest-directory: Specifies the name of the destination directory.

Usage guidelines

If you specify a destination directory, the system moves the source file to the specified directory without changing the file name.

Examples

Move the **flash:/test/sample.txt** file to **flash:/**, and save it as **1.txt**.

```
<Sysname> move test/sample.txt 1.txt
Move flash:/test/sample.txt to flash:/1.txt? [Y/N]:y
Moving file flash:/test/sample.txt to flash:/1.txt ...Done.
```

Move the **b.cfg** file to the **test2** directory.

```
<Sysname> move b.cfg test2
Move flash:/b.cfg to flash:/test2/b.cfg? [Y/N]:y
Moving file flash:/b.cfg to flash:/test2/b.cfg... Done.
```

pwd

Use **pwd** to display the working directory.

Syntax

pwd

Views

User view

Predefined user roles

network-admin

Examples

Display the working directory.

```
<Sysname> pwd
flash:
```

rename

Use **rename** to rename a file or directory.

Syntax

rename { *source-file* | *source-directory* } { *dest-file* | *dest-directory* }

Views

User view

Predefined user roles

network-admin

Parameters

source-file: Specifies the name of the source file.

source-directory: Specifies the name of the source directory.

dest-file: Specifies the name of the destination file.

dest-directory: Specifies the name of the destination directory.

Usage guidelines

This command is not executed if the destination file or directory name is already used by an existing file or directory in the working directory.

Examples

Rename the **copy.cfg** file as **test.cfg**.

```
<Sysname> rename copy.cfg test.cfg
Rename flash:/copy.cfg as flash:/test.cfg? [Y/N]:y
Renaming flash:/copy.cfg as flash:/test.cfg... Done.
```

reset recycle-bin

Use **reset recycle-bin** to delete files from the recycle bin.

Syntax

reset recycle-bin [**/force**]

Views

User view

Predefined user roles

network-admin

Parameters

/force: Deletes all files in the recycle bin without prompting for confirmation. If you do not specify this option, the command prompts you to confirm the deletion operation for each file.

Usage guidelines

The **delete** *file* command only moves a file to the recycle bin. To permanently delete the file, use the **reset recycle-bin** command to delete the file from the recycle bin.

Examples

Empty the recycle bin. (In this example there are two files in the recycle bin.)

```
<Sysname> reset recycle-bin
Clear flash:/a.cfg? [Y/N]:y
Clearing file flash:/a.cfg... Done.
Clear flash:/b.cfg? [Y/N]:y
Clearing file flash:/b.cfg... Done.
```

Delete the **b.cfg** file from the recycle bin. (In this example there are two files in the recycle bin.)

```
<Sysname> reset recycle-bin
Clear flash:/a.cfg? [Y/N]:n
Clear flash:/b.cfg? [Y/N]:y
Clearing file flash:/b.cfg... Done.
```

Related commands

delete

rmdir

Use **rmdir** to delete a directory.

Syntax

rmdir *directory*

Views

User view

Predefined user roles

network-admin

Parameters

directory: Specifies a directory.

Usage guidelines

To delete a directory, you must delete all files and subdirectories in the directory permanently or move them to the recycle bin. If you move them to the recycle bin, executing the **rmdir** command permanently deletes them.

Examples

Delete the **subtest** directory.

```
<Sysname>rmdir subtest/
Remove directory flash:/test/subtest and the files in the recycle-bin under this directory
will be deleted permanently. Continue? [Y/N]:y
Removing directory flash:/test/subtest... Done.
```

sha256sum

Use **sha256sum** to use the SHA-256 algorithm to calculate the digest of a file.

Syntax

sha256sum *file*

Views

User view

Predefined user roles

network-admin

Parameters

file: Specifies the name of a file.

Usage guidelines

You can use file digests to verify file integrity.

Examples

Use the SHA-256 algorithm to calculate the digest of file **system.bin**.

```
<Sysname> sha256sum system.bin
SHA256 digest:
0851e0139f2770e87d01ee8c2995ca9e59a8f5f4062e99af14b141b1a36ca152
```

tar create

Use **tar create** to archive files and directories.

Syntax

tar create [**gz**] **archive-file** *dest-file* [**verbose**] **source** { *source-file* | *source-directory* }&<1-5>

Views

User view

Predefined user roles

network-admin

Parameters

gz: Uses gzip to compress the files and directories before archiving them. If you do not specify this keyword, the command archives the files and directories without compressing them.

archive-file *dest-file*: Specifies the archive file name. If you specified the **gz** keyword, the extension of the archive file name must be **.tar.gz**. If you did not specify the **gz** keyword, the extension of the archive file name must be **.tar**.

verbose: Displays the names of the successfully archived files and directories. If you do not specify this keyword, the command does not display the names of the successfully archived files and directories.

source { *source-file* | *source-directory* }&<1-5>: Specifies the files and directories to be archived. The argument can be a space-separated list of up to five items. Each item can be a file or directory name.

Examples

Archive the **1.cfg** and **2.cfg** files and the **test** directory to **a.tar**.

```
<Sysname> tar create archive-file a.tar source 1.cfg 2.cfg test
Creating archive flash:/a.tar Done.
```

Compress and archive the **1.cfg** and **2.cfg** files and the **test** directory to **b.tar.gz**.

```
<Sysname> tar create gz archive-file b.tar.gz source 1.cfg 2.cfg test
Creating archive flash:/b.tar.gz Done.
```

Compress and archive files and directories, and display the successfully archived files and directories.

```
<Sysname> tar create gz archive-file c.tar.gz verbose source 1.cfg 2.cfg test
1.cfg
2.cfg
test/
test/a.log
test/subtest/
test/subtest/aa.log
```

Related commands

tar extract

tar list

tar extract

Use **tar extract** to extract files and directories.

Syntax

tar extract archive-file *file* [**verbose**] [**screen** | **to** *directory*]

Views

User view

Predefined user roles

network-admin

Parameters

archive-file *file*: Specifies the archive file name. The extension can be **.tar** or **.tar.gz**.

verbose: Displays the names of the successfully extracted files and directories.

screen: Displays the content of the extracted files and directories on the screen. The extracted files are not saved.

to *directory*: Saves the extracted files and directories to a different directory. The *directory* argument specifies the directory.

Usage guidelines

IMPORTANT:

Before specifying the **screen** keyword for this command, use the **tar list** command to identify the types of the archived files. As a best practice, specify the keyword only if all archived files are text files. Displaying the content of an archived non-text file that contains terminal control characters might result in garbled characters and even cause the terminal unable to operate correctly. To use the terminal again, you must close the current connection and log in to the device again.

If you do not specify the **screen** keyword or the **to** *directory* option, the command saves the extracted files and directories to the working directory.

The command saves the extracted files and directories by using their original names. If a file or directory that has the same name as an extracted file or directory already exists in the destination directory, the file or directory is overwritten.

Examples

Extract files and directories from archive file **a.tar**.

```
<Sysname> tar extract archive-file a.tar
Extracting archive flash:/a.tar Done.
```

Extract files and directories from archive file **a.tar**, and display the names of the successfully extracted files and directories.

```
<Sysname> tar extract archive-file b.tar.gz verbose
1.cfg
2.cfg
test/
test/a.log
test/subtest/
test/subtest/aa.log
```

Extract files and directories from archive file **a.tar**, and display the content of the files on the screen.

```
<Sysname> tar extract archive-file c.tar.gz screen
#
 version 7.1.070, Release 1201
#
 sysname Sysname
#
...
```

Related commands

tar create

tar list

tar list

Use **tar list** to display the names of archived files and directories.

Syntax

tar list archive-file *file*

Views

User view

Predefined user roles

network-admin

Parameters

archive-file *file*: Specifies the archive file name. The extension can be **.tar** or **.tar.gz**.

Examples

Display the names of archived files and directories.

```
<Sysname> tar list archive-file a.tar
1.cfg
2.cfg
test/
test/a.log
test/subtest/
test/subtest/aa.log
```

Related commands

tar create

tar extract

umount

Use **umount** to unmount a file system.

Syntax

umount *filesystem*

Views

User view

Predefined user roles

network-admin

Parameters

filesystem: Specifies the name of a file system.

Usage guidelines

File systems on a storage medium are automatically mounted when the storage medium is connected to the device. To remove a hot-swappable storage medium from the device, you must first unmount all file systems on the storage medium. Removing a mounted hot-swappable storage medium might damage files on the storage medium or even the storage medium.

You can unmount a file system only when no other users are accessing the file system.

To avoid file system corruption, do not perform the following tasks while the system is unmounting a file system:

- Reboot, power cycle, or power off the device.
- Install, remove, or access storage media.
- Perform a switchover.

Examples

Unmount a file system on a USB disk.

```
<Sysname> umount usba0:
```

Related commands

mount

undelete

Use **undelete** to restore a file from the recycle bin.

Syntax

undelete *file*

Views

User view

Predefined user roles

network-admin

Parameters

file: Specifies the name of the file to be restored.

Usage guidelines

If a file with the same name already exists in the directory, the system prompts whether or not you want to overwrite the existing file. If you enter **Y**, the existing file is overwritten. If you enter **N**, the command is not executed.

Examples

Restore the **copy.cfg** file, which was moved from the root directory of the **flash:** file system to the recycle bin.

```
<Sysname>undelete copy.cfg
Undelete flash:/copy.cfg? [Y/N]:y
Undeleting file flash:/copy.cfg... Done.
```

Restore the **startup.cfg** file, which was moved from the **flash:/seclog** directory to the recycle bin.

- Method 1:

```
<Sysname>undelete seclog/startup.cfg
Undelete flash:/seclog/startup.cfg? [Y/N]:y
Undeleting file flash:/seclog/startup.cfg... Done.
<Sysname>
```

- Method 2:

```
<Sysname> cd seclog
<Sysname> undelete startup.cfg
Undelete flash:/seclog/startup.cfg? [Y/N]:y
Undeleting file flash:/seclog/startup.cfg... Done.
```

Configuration file management commands

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

archive configuration

Use **archive configuration** to manually archive the running configuration to the configuration archive directory.

Syntax

archive configuration

Views

User view

Predefined user roles

network-admin

Usage guidelines

This command saves the running configuration to the specified configuration archive directory with file names generated from the specified name prefix.

Before executing this command, you must use one of the following methods to specify a directory and a name prefix for the configuration archives:

- For local archiving, use the **archive configuration location** command to specify a local configuration archive directory and a name prefix.
- For remote archiving, use the **archive configuration server** command to specify a configuration archive directory and a name prefix on a remote SCP server. In addition, you must use the **archive configuration server user** and **archive configuration server password** commands to configure a username and password for accessing the server.

If you use the **archive configuration location** command to specify a local configuration archive directory, manual configuration archiving saves the running configuration only on the master device.

Examples

Archive the running configuration.

```
<Sysname> archive configuration
Save the running configuration to an archive file. Continue? [Y/N]: Y
The running configuration was saved to myarchive_1.cfg.
```

Related commands

archive configuration interval

archive configuration location

archive configuration max

archive configuration server

archive configuration server password

archive configuration server user

display archive configuration

archive configuration interval

Use **archive configuration interval** to enable automatic running-configuration archiving and set the archiving interval.

Use **undo archive configuration interval** to disable automatic running-configuration archiving.

Syntax

archive configuration interval *interval*

undo archive configuration interval

Default

The automatic running-configuration archiving feature is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval for automatically saving the running configuration. The value range is 10 to 525600, in minutes.

Usage guidelines

Automatic configuration archiving enables the system to periodically save the running configuration to the archive directory. After the system finishes an automatic archive, it resets the archiving interval timer.

Before enabling automatic configuration archiving, you must use one of the following methods to specify a directory and a name prefix for the configuration archives:

- For local archiving, use the **archive configuration location** command to specify a local configuration archive directory and a name prefix.
- For remote archiving, use the **archive configuration server** command to specify a configuration archive directory and a name prefix on a remote SCP server. In addition, you must use the **archive configuration server user** and **archive configuration server password** commands to configure a username and password for accessing the server.

If you use the **archive configuration location** command to specify a local configuration archive directory, automatic configuration archiving saves the running configuration only on the master device.

Examples

Set the system to archive the running configuration every 60 minutes.

```
<Sysname> system-view
[Sysname] archive configuration interval 60
Archive file will be saved every 60 minutes.
```

Related commands

archive configuration

archive configuration location

archive configuration max

archive configuration server

archive configuration server password

archive configuration server user

display archive configuration

archive configuration location

Use **archive configuration location** to specify a local directory and file name prefix for archiving the running configuration.

Use **undo archive configuration location** to restore the default.

Syntax

archive configuration location *directory* **filename-prefix** *filename-prefix*

undo archive configuration location

Default

No local directory or file name prefix is specified on the device for archiving the running configuration.

Views

System view

Predefined user roles

network-admin

Parameters

directory: Specifies the archive directory, a string of 1 to 63 characters. The value for this argument must take the format of *storage-medium-name:/folder-name*. The directory must already exist on the master.

filename-prefix: Specifies a file name prefix for configuration archives, a case-insensitive string of 1 to 30 characters. Valid characters are letters, digits, underscores (_), and hyphens (-).

Usage guidelines

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

The local configuration archives on the device are named in the format of *prefix_serial number***.cfg**, for example, **archive_1.cfg** and **archive_2.cfg**. The serial number is automatically assigned from 1 to 1000, increasing by 1. After the serial number reaches 1000, it restarts from 1.

If you change the file directory or file name prefix on the device, the following events occur:

- The old configuration archives change to common configuration files.
- The configuration archive counter is reset. The serial number for new configuration archives starts at 1.
- The **display archive configuration** command no longer displays the old configuration archives.

The configuration archive counter does not restart when you delete configuration archives from the archive directory. However, if the device reboots after all configuration archives have been deleted,

the configuration archive counter restarts. The serial number for new configuration archives starts at 1.

The **undo archive configuration location** command removes the local configuration archive directory and file name prefix settings. The command also performs the following operations:

- Disables the configuration archive feature (both manual and automatic methods).
- Restores the default settings of the **archive configuration interval** and **archive configuration max** commands.
- Clears the configuration archive information displayed by using the **display archive configuration** command.

Examples

Set the configuration archive directory as **flash:/archive** and the archive file name prefix as **my_archive**.

```
<Sysname> mkdir flash:/archive
Creating directory flash:/archive... Done.
<Sysname> system-view
[Sysname] archive configuration location flash:/archive filename-prefix my_archive
```

Related commands

archive configuration

archive configuration interval

archive configuration max

display archive configuration

archive configuration max

Use **archive configuration max** to set the maximum number of configuration archives that can be saved on the device.

Use **undo archive configuration max** to restore the default.

Syntax

archive configuration max *file-number*

undo archive configuration max

Default

The maximum number is 5.

Views

System view

Predefined user roles

network-admin

Parameters

file-number: Specifies the maximum number of configuration archives that can be saved on the device. The value range is 1 to 10. Adjust the setting depending on the amount of storage space available.

Usage guidelines

Before you execute this command, use the **archive configuration location** command to specify a configuration archive directory and archive file name prefix on the device.

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

Changing the limit setting to a lower value does not cause immediate deletion of excess archives. Instead, the configuration archive feature deletes the oldest *n* files when a new archive is manually or automatically saved, where *n* = current archive count – new archive limit + 1. For example, seven configuration archives have been saved before the archive limit is set to four. When saving a new configuration archive, the system first deletes the oldest four (7 – 4 + 1) archives.

If you execute the **undo archive configuration location** command, the default archive limit is restored.

Examples

Set the maximum number of configuration archives to 10.

```
<Sysname> system-view
[Sysname] archive configuration max 10
```

Related commands

archive configuration

archive configuration location

archive configuration interval

display archive configuration

archive configuration server

Use **archive configuration server** to configure the parameters for archiving the running configuration to a remote SCP server.

Use **undo archive configuration server** to restore the default.

Syntax

archive configuration server scp { *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**vpn-instance** *vpn-instance-name*] [**directory** *directory*] **filename-prefix** *filename-prefix*

undo archive configuration server

Default

No parameters are set for archiving the running configuration to a remote SCP server.

Views

System view

Predefined user roles

network-admin

Parameters

scp: Specifies a remote SCP server.

ipv4-address: Specifies the SCP server by its IPv4 address.

ipv6 *ipv6-address*: Specifies the SCP server by its IPv6 address.

port *port-number*: Specifies the TCP port number of the SCP server. The value range for the *port-number* argument is 1 to 65535, and the default port number is 22.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the SCP server is on the public network, do not specify this option.

directory *directory*: Specifies the archive directory, a case-insensitive string. If you do not specify this option, the archive directory is the root directory of the SCP server.

filename-prefix *filename-prefix*: Specifies a file name prefix for configuration archives, a case-insensitive string of 1 to 30 characters. Valid characters are letters, digits, underscores (_), and hyphens (-).

Usage guidelines

IMPORTANT:

In FIPS mode, the device does not support archiving the running configuration to a remote SCP server.

Before archiving the running configuration to a remote SCP server, you must perform the following tasks:

- Use this command to specify a configuration archive directory and a name prefix on the remote SCP server.
- Use the **archive configuration server user** and **archive configuration server password** commands to configure a username and password for accessing the server.

To manually archive the running configuration, use the **archive configuration** command. To periodically archive the running configuration, use the **archive configuration interval** command.

On the specified remote SCP server, configuration archives are named in the format of *filename-prefix_YYYYMMDD_HHMMSS***.cfg**, for example, **archive_20170526_203430.cfg**.

Local archiving (the **archive configuration location** command) and remote archiving (the **archive configuration server** command) are mutually exclusive. You cannot use the two features at the same time.

The maximum number of configuration archives on a remote SCP server depends on the SCP server setting and is not restricted by the **archive configuration max** command.

The **undo archive configuration server** command removes the configuration archive directory and file name prefix settings, but it does not delete the configuration archives saved on the server. The command also performs the following operations:

- Disables the configuration archive feature (both manual and automatic methods).
- Restores the default setting for the **archive configuration interval** command.
- Clears the configuration archive information displayed by using the **display archive configuration** command.

Examples

Set the configuration archive directory as **archive/** on the SCP server at 192.168.1.1 and set the archive file name prefix as **my_archive**.

```
<Sysname> system-view
[Sysname] archive configuration server scp 192.168.1.1 port 22 directory /archive/
filename-prefix my_archive
```

Related commands

archive configuration

archive configuration interval

archive configuration location

archive configuration server password

archive configuration server user

display archive configuration

archive configuration server password

Use **archive configuration server password** to configure the password for accessing the SCP server that saves configuration archives.

Use **undo archive configuration server password** to restore the default.

Syntax

archive configuration server password { **cipher** | **simple** } *string*

undo archive configuration server password

Default

No password is configured for accessing the SCP server that saves configuration archives.

Views

System view

Predefined user roles

network-admin

Parameters

cipher: Specifies a password in encrypted form.

simple: Specifies a password in plaintext form. For security purposes, the password specified in plaintext form will be stored in encrypted form.

string: Specifies the password. Its plaintext form is a case-sensitive string of 1 to 63 characters. Its encrypted form is a case-sensitive string of 33 to 117 characters.

Examples

Set the password to **admin** in plaintext form for accessing the SCP server that saves configuration archives.

```
<Sysname> system-view
[Sysname] archive configuration server password simple admin
```

Related commands

archive configuration server

archive configuration server user

display archive configuration

archive configuration server user

Use **archive configuration server user** to configure the username for accessing the SCP server that saves configuration archives.

Use **undo archive configuration server user** to restore the default.

Syntax

archive configuration server user *user-name*

undo archive configuration server user

Default

No username is configured for accessing the SCP server that saves configuration archives.

Views

System view

Predefined user roles

network-admin

Parameters

user-name: Specifies the username, a case-sensitive string of 1 to 63 characters.

Examples

Set the username to **admin** for accessing the SCP server that saves configuration archives.

```
<Sysname> system-view
[Sysname] archive configuration server user admin
```

Related commands

archive configuration server

archive configuration server password

display archive configuration

backup startup-configuration

Use **backup startup-configuration** to back up the main next-startup configuration file to a TFTP server.

Syntax

backup startup-configuration to { *ipv4-server* | **ipv6** *ipv6-server* } [*dest-filename*] [**vpn-instance** *vpn-instance-name*]

Views

User view

Predefined user roles

network-admin

Parameters

ipv4-server: Specifies a TFTP server by its IPv4 address or host name. The host name is a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.).

ipv6 *ipv6-server*: Specifies a TFTP server by its IPv6 address or host name. The host name is a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.).

dest-filename: Specifies the name of the target file used for saving the file on the server. The file must be a .cfg file. The file name is a case-insensitive string of up to 255 characters. If you do not specify a target file name, the source file name is used.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the TFTP server is on the public network, do not specify this option.

Usage guidelines

This command is not supported in FIPS mode.

Examples

Back up the main next-startup configuration file to the IPv4 TFTP server at 2.2.2.2 in the public network, and set the target file name to **192-168-1-26.cfg**.

```
<Sysname> backup startup-configuration to 2.2.2.2 192-168-1-26.cfg
Backing up the main startup configuration file to 2.2.2.2...
Done.
```

Back up the main next-startup configuration file to the IPv4 TFTP server at 2.2.2.2 in MPLS L3VPN instance **VPN1**, and set the target file name to **192-168-1-26.cfg**.

```
<Sysname> backup startup-configuration to 2.2.2.2 192-168-1-26.cfg vpn-instance VPN1
Backing up the main startup configuration file to 2.2.2.2 in VPN VPN1...
Done.
```

Back up the main next-startup configuration file to the IPv6 TFTP server at 2001::2 in the public network, and set the target file name to **192-168-1-26.cfg**.

```
<Sysname> backup startup-configuration to ipv6 2001::2 192-168-1-26.cfg
Backing up the main startup configuration file to 2001::2...
Done.
```

Related commands

`restore startup-configuration`

configuration commit

Use **`configuration commit`** to commit the settings configured after the configuration commit delay timer was set.

Syntax

`configuration commit`

Views

System view

Predefined user roles

network-admin

Usage guidelines

You must execute the **`configuration commit delay`** command to set the configuration delay timer before executing this command.

The settings you made during the commit delay interval are automatically removed if you have not manually committed them before the configuration commit delay timer expires.

As a best practice, configure the information center to output logs to the console. Use the logs to determine whether you want to commit the settings. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Set the configuration commit delay timer to 10 minutes.

```
<Sysname> system-view
[Sysname] configuration commit delay 10
```

Commit the settings configured after the configuration commit delay timer was set and before the delay timer expires.

```
[Sysname] configuration commit
```

Related commands

configuration commit delay

configuration commit delay

Use **configuration commit delay** to enable the configuration commit delay feature and start the configuration commit delay timer.

Syntax

configuration commit delay *delay-time*

Views

System view

Predefined user roles

network-admin

Parameters

delay-time: Sets the configuration commit delay interval. The value range is 1 to 65535 minutes.

Usage guidelines

The system creates a rollback point to record the configuration status when you execute this command to start the configuration commit delay timer. The settings you made during the commit delay interval takes effect immediately. However, these settings will be removed automatically if you have not manually committed them before the configuration commit delay timer expires. Then, the system returns to the configuration status when the commit delay timer started.

This feature prevents a misconfiguration from causing the inability to access the device and is especially useful when you configure the device remotely.

When you use this feature, follow these restrictions and guidelines:

- In a multi-user context, make sure no one else is configuring the device.
- To avoid unexpected errors, do not perform any operations during the configuration rollback.
- You can reconfigure the configuration commit delay timer before it expires to shorten or extend the commit delay interval. However, the rollback point will not change.
- The configuration commit delay feature is a one-time setting. The feature is disabled with the rollback point removed when the commit delay timer expires or after a manual commit operation is performed. To use this feature again, you must re-execute this command.

Examples

Set the configuration commit delay timer to 10 minutes.

```
<Sysname> system-view
[Sysname] configuration commit delay 10
```

Change the configuration commit delay timer to 60 minutes before the old delay timer expires.

```
[Sysname] configuration commit delay 60
The commit delay already set 10 minutes, overwrite it? [Y/N]:y
```

Related commands

configuration commit

configuration encrypt

Use **configuration encrypt** to enable configuration encryption.

Use **undo configuration encrypt** to disable configuration encryption.

Syntax

configuration encrypt { **private-key** | **public-key** }

undo configuration encrypt

Default

Configuration encryption is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

private-key: Encrypts configuration with a private key. All devices running Comware 7 software use the same private key.

public-key: Encrypts configuration with a public key. All devices running Comware 7 software use the same public key.

Usage guidelines

Configuration encryption enables the device to automatically encrypt a configuration file when saving the running configuration to the file.

Any devices running Comware 7 software can decrypt the encrypted configuration file. To prevent an encrypted file from being decoded by unauthorized users, make sure the file is accessible only to authorized users.

Examples

Enable the public-key method for configuration encryption.

```
<Sysname> system-view
[Sysname] configuration encrypt public-key
```

configuration replace file

Use **configuration replace file** to perform configuration rollback.

Syntax

configuration replace file *filename*

Views

System view

Predefined user roles

network-admin

Parameters

filename: Specifies the path of the replacement configuration file, a string of up to 255 characters. The file must be a .cfg file. The file and file path must be valid and on the local system.

Usage guidelines

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

To ensure a successful rollback, follow these guidelines:

- Make sure the replacement configuration file is created by using the configuration archive feature or the **save** command on the device.
- If the configuration file is not created on the device, make sure the command lines in the configuration file are fully compatible with the device.
- If the replacement configuration file is encrypted, make sure the device can decrypt it.

Examples

Replace the running configuration with the configuration in the **my_archive_1.cfg** configuration file.

```
<Sysname> system-view
[Sysname] configuration replace file my_archive_1.cfg
Current configuration will be lost, save current configuration? [Y/N]:n
Now replacing the current configuration. Please wait...
Succeeded in replacing current configuration with the file my_archive_1.cfg.
```

display archive configuration

Use **display archive configuration** to display configuration archive information.

Syntax

display archive configuration

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about the configuration archives saved on the device.

```
<Sysname> display archive configuration
Location: flash:/archive
Filename prefix: my_archive
Archive interval in minutes: 120
Maximum number of archive files: 10
Archive history:
  No.  TimeStamp               FileName
  1    Aug 05 2007 20:24:54    my_archive_1.cfg
  2    Aug 05 2007 20:34:54    my_archive_2.cfg
# 3    Aug 05 2007 20:44:54    my_archive_3.cfg
The pound sign (#) indicates the most recent archive file.
Next archive file to be saved: my_archive_4.cfg
```

Display information about the configuration archives saved on a remote SCP server.

```
<Sysname> display archive configuration
```

```
Username: test
Location: scp://192.168.21.21:22/archive
Filename prefix: my_archive
Archive interval in minutes: 120
Archive history:
 No.   TimeStamp                  FileName
 1    Wed Dec 15 14:20:18 2010   my_archive_20170509_142018.cfg
!2    Wed Dec 15 14:33:10 2010   my_archive_20170509_143018.cfg
#!3    Wed Dec 15 14:49:37 2010   my_archive_20170509_144018.cfg
The exclamation mark (!) indicates that the remote archiving attempt failed.
The pound sign (#) indicates the most recent archive file.
```

Table 21 Command output

Field	Description
Username	Username for accessing the SCP server that saves configuration archives.
Location	Absolute path of the directory for saving running-configuration archives.
Filename prefix	File name prefix for configuration archives.
Archive interval in minutes	Interval (in minutes) for the system to automatically archive the running configuration. If automatic configuration saving is disabled, this field is not available.
Maximum number of archive files	Maximum number of configuration archives that can be saved on the device.
Archive history	History configuration archive information.
No.	Number of a configuration archive.
TimeStamp	Time when the configuration archive was created.

Related commands

archive configuration

archive configuration interval

archive configuration location

archive configuration max

archive configuration server

archive configuration server user

display current-configuration

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

Syntax

display current-configuration [[**configuration** [*module-name*] | **exclude-provision** | **interface** [*interface-type* [*interface-number*]]] [**all**] | **slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

configuration [*module-name*]: Displays the feature configuration. The *module-name* argument specifies a feature module. If you do not specify a feature module, the command displays all feature settings you have made.

exclude-provision: Excludes preprovisioned settings from the running configuration.

interface [*interface-type* [*interface-number*]]: Displays interface configuration, where the *interface-type* argument represents the interface type and the *interface-number* argument represents the interface number. If you do not specify the *interface-type interface-number* arguments, the command displays the running configuration for all interfaces. If you specify only the *interface-type* argument, the command displays the running configuration for all interfaces of this type.

all: Displays all settings in the running configuration, including the default settings. If you do not specify this keyword, the command displays only non-default settings in the running configuration.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify an IRF member device, this command displays the running configuration for all IRF member devices.

Usage guidelines

Use this command to verify the configuration you have made.

If the system has automatically changed the setting you have made for a parameter, this command displays the effective setting instead of the configured one. An automatic change typically occurs because of system restrictions. This command does not display parameters that are using the default settings if you do not specify the **all** keyword.

Examples

Display local user configuration.

```
<Sysname> display current-configuration configuration local-user
#
local-user ftp
 password hash
$h$6$Twd73mLrN8O2vvD5$Cz1vgdpR4KoTiRQNE9pg33gU14Br2p1VguczLSVyJLO2huV5Syx/LfDIf8ROLtV
ErJ/C31oq2rFtmNuyZf4STw==
 service-type ftp
 authorization-attribute user-role network-operator
#
local-user root
 password hash
$h$6$Twd73mLrN8O2vvD5$Cz1vgdpR4KoTiRQNE9pg33gU14Br2p1VguczLSVyJLO2huV5Syx/LfDIf8ROLtV
ErJ/C31oq2rFtmNuyZf4STw==
 service-type ssh telnet terminal
 authorization-attribute user-role network-admin
#
return
```

Display VLAN interface configuration.

```
<Sysname> display current-configuration interface Vlan-interface
#
interface Vlan-interface1
 ip address 192.168.1.84 255.255.255
#
Return
```

display current-configuration diff

Use **display current-configuration diff** to display the differences that the running configuration has as compared with the next-startup configuration.

Syntax

display current-configuration diff

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

This command searches for the next-startup configuration in the following order:

1. The .cfg main next-startup configuration file.
2. The .cfg backup next-startup configuration file if the .cfg main next-startup configuration file is unavailable.

If both configuration files are unavailable, the system displays a message indicating that no next-startup configuration files exist.

Examples

Display the differences that the running configuration has as compared with the next-startup configuration.

```
<Sysname> display current-configuration diff
--- Startup configuration
+++ Current configuration
@@ -5,7 +5,7 @@
 #
  sysname Sysname
 #
-alias dhc display history-command
+alias dh display hotkey
 #
  system-working-mode standard
<Sysname>
```

Table 22 Command output

Field	Description
- - - *A* +++ *B*	• *A* represents the source configuration for comparison, which can be **Startup configuration**, **Current configuration**, or the name of the source configuration file with its directory information. • *B* represents the target configuration for comparison, which can be **Current configuration**, **Startup configuration**, or the name of the target configuration file with its directory information. In this example, the startup configuration and the current configuration are the source and target, respectively.
@@ *-linenumber1*,*number1* *+linenumber2*,*number2* @@	Location information for identifying the command line differences: • *-linenumber1*,*number1*—Source configuration section that contains differences. The *linenumber1* argument represents the start line of the section. The *number1* argument represents the number of lines between the start line and the end line of the section. • *+linenumber2*,*number2*—Target configuration section that contains differences. The *linenumber2* argument represents the start line of the section. The *number2* argument represents the number of lines between the start line and the end line of the section.
cmd1 *- cmd2* *+ cmd3* *cmd4*	Displays command differences. • *cmd1* and *cmd4*—Command lines are contained in both source and target configurations if they are not prefixed with a minus (-) or plus (+) sign. They provide a context for locating command line differences. • *- cmd2*—Command lines are prefixed with a minus sign if they are contained in the source configuration but not in the target configuration. • *+ cmd3*—Command lines are prefixed with a plus sign if they are contained in the target configuration but not in the source configuration. In this example, the sample output shows that the **`alias dhc display history-command`** command is contained only in the source configuration, and the **`alias dh display hotkey`** command is contained only in the target configuration.

Related commands

`display current-configuration`

`display diff`

`display saved-configuration`

display default-configuration

Use **`display default-configuration`** to display the factory defaults.

Syntax

`display default-configuration`

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Factory defaults are custom basic settings that came with the device. Factory defaults vary by device models and might differ from the initial default settings for the commands.

The device starts up with the factory defaults if no next-startup configuration files are available.

Examples

Display the factory defaults.

```
<Sysname> display default-configuration
```

display diff

Use **display diff** to display differences between configurations.

Syntax

display diff configfile *file-name-s* { **configfile** *file-name-d* | **current-configuration** | **startup-configuration** }

display diff current-configuration { **configfile** *file-name-d* | **startup-configuration** }

display diff startup-configuration { **configfile** *file-name-d* | **current-configuration** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

configfile *file-name-s*: Specifies the source configuration file for comparison.

configfile *file-name-d*: Specifies the target configuration file for comparison.

current-configuration: Specifies the running configuration. In the **display diff current-configuration** command, this keyword specifies the source configuration for comparison. In the **display diff configfile** *file-name-s* and **display diff startup-configuration** commands, this keyword specifies the target configuration.

startup-configuration: Specifies the next-startup configuration. In the **display diff startup-configuration** command, this keyword specifies the source configuration for comparison. In the **display diff configfile** *file-name-s* and **display diff current-configuration** commands, this keyword specifies the target configuration.

Usage guidelines

If you specify the **startup-configuration** keyword, the system searches for the next-startup configuration in the following order:

1. The .cfg main next-startup configuration file.
2. The .cfg backup next-startup configuration file if the .cfg main next-startup configuration file is unavailable.

If both configuration files are unavailable, the system displays a message indicating that no next-startup configuration files exist.

Examples

Display the differences between **startup.cfg** and **test.cfg**.

```
<Sysname> display diff configfile startup.cfg configfile test.cfg
--- flash:/startup.cfg
+++ flash:/test.cfg
@@ -5,7 +5,7 @@
 #
  sysname Sysname
 #
-alias dhc display history-command
+alias dh display hotkey
 #
  system-working-mode standard
<Sysname>
```

The output shows that the **alias dhc display history-command** command is contained only in **startup.cfg**, and the **alias dh display hotkey** command is contained only in **test.cfg**.

Display the differences between the running configuration and the next-startup configuration.

```
<Sysname> display diff current-configuration startup-configuration
--- Current configuration
+++ Startup configuration
@@ -5,7 +5,7 @@
 #
  sysname Sysname
 #
-alias dhc display history-command
+alias dh display hotkey
 #
  system-working-mode standard
<Sysname>
```

The output shows that the **alias dhc display history-command** command is contained only in the running configuration, and the **alias dh display hotkey** command is contained only in the next-startup configuration.

For the command output description, see Table 22.

Related commands

display current-configuration

display current-configuration diff

display saved-configuration

display saved-configuration

Use **display saved-configuration** to display the contents of the configuration file for the next system startup.

Syntax

display saved-configuration

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Use this command to verify that important settings have been saved to the configuration file for the next system startup.

This command selects the configuration file to display in the following order:

1. If the main startup configuration file is available, this command displays the contents of the main startup configuration file.
2. If only the backup startup configuration file is available, this command displays the contents of the backup file.
3. If both the main and backup startup configuration files are not available, this command does not display anything.

Examples

Display the contents of the configuration file for the next system startup.

```
<Sysname> display saved-configuration
#
 version 7.1.070, Release 1201
#
 sysname Sysname
#
 ftp server enable
#
 telnet server enable
#
 domain default enable system
#
vlan 1
#
domain system
#
  ---- More ----
```

Related commands

reset saved-configuration

save

display startup

Use **display startup** to display the names of the current startup configuration file and the next-startup configuration files.

Syntax

display startup

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

All IRF members use the same current startup configuration file as the master.

After a master/subordinate switchover, it is normal that the current startup configuration files on all IRF members are displayed as NULL. This is because the new master continues to run with the running configuration rather than rebooting with a startup configuration file.

Examples

Display names of the startup configuration files.

```
<Sysname> display startup
MainBoard:
 Current startup saved-configuration file: flash:/startup.cfg(*)
 Next main startup saved-configuration file: flash:/startup.cfg
 Next backup startup saved-configuration file: NULL
```

Table 23 Command output

Field	Description
MainBoard	Displays the startup configuration files on the master device.
Current startup saved-configuration file	Configuration file that the device has started up with. If the field is suffixed with an asterisk (*), the startup configuration file is a binary configuration file.
Next main startup saved-configuration file	Primary configuration file to be used at the next startup.
Next backup startup saved-configuration file	Backup configuration file to be used at the next startup.

Related commands

startup saved-configuration

display this

Use **display this** to display the running configuration in the current view.

Syntax

display this [**all**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Displays all settings in the running configuration in the current view, including the default settings. If you do not specify this keyword, the command displays only non-default settings in the running configuration.

Usage guidelines

Use this command to verify the configuration you have made in a certain view.

This command does not display parameters that are using the default settings if you do not specify the **all** keyword.

Some parameters can be successfully set even if their dependent features are not enabled. For these parameters, this command displays their settings after the dependent features are enabled.

This command can be executed in any user line view to display the running configuration of all user lines.

Examples

Display the running configuration on VLAN-interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] display this
#
interface Vlan-interface1
#
return
```

reset saved-configuration

Use **reset saved-configuration** to delete a next-startup configuration file.

Syntax

reset saved-configuration [**backup** | **main**]

Views

User view

Predefined user roles

network-admin

Parameters

backup: Specifies the backup next-startup configuration file.

main: Specifies the main next-startup configuration file.

Usage guidelines

CAUTION:

By default, this command permanently deletes the specified next-startup configuration file from all IRF member devices. To delete the configuration file only from the master device, disable automatic system-wide next-startup configuration file operations. For more information about disabling these operations, see *Fundamentals Configuration Guide*.

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

To delete a file that is set as both main and backup next-startup configuration files, you must execute both the **reset saved-configuration backup** command and the **reset**

saved-configuration main command. Using only one of the commands sets the target file attribute to NULL instead of deleting the file.

If you do not specify a configuration file attribute, the **reset saved-configuration** command deletes the main next-startup configuration file.

Examples

Delete the main next-startup configuration file.

```
<Sysname> reset saved-configuration
The saved configuration file will be erased. Are you sure? [Y/N]:y
Configuration file in flash: is being cleared.
Please wait ...........
Configuration file is cleared.
```

Related commands

display saved-configuration

restore startup-configuration

Use **restore startup-configuration** to download a configuration file from a TFTP server and specify it as the main next-startup configuration file.

Syntax

restore startup-configuration from { *ipv4-server* | **ipv6** *ipv6-server* } *src-filename* [**vpn-instance** *vpn-instance-name*]

Views

User view

Predefined user roles

network-admin

Parameters

ipv4-server: Specifies a TFTP server by its IPv4 address or host name. The host name is a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.).

ipv6 *ipv6-server*: Specifies a TFTP server by its IPv6 address or host name. The host name is a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), and dots (.).

src-filename: Specifies the name of the configuration file to be downloaded. The file must be a .cfg file. The file name is a case-insensitive string of up to 255 characters.

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the TFTP server is on the public network, do not specify this option.

Usage guidelines

This command is not supported in FIPS mode.

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

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

This command downloads the configuration file to the root directory of the default storage medium on each member device and specifies the file as the main next-startup configuration file. If the default storage medium has been partitioned, the configuration file is saved on the first partition. Make sure all IRF members use the same type of default storage media. If a subordinate device uses a different type of default storage medium than the master, the command cannot propagate the configuration file to the subordinate device. For example, the subordinate device uses a USB disk, but the master uses a flash memory. In this situation, you must manually restore the main next-startup configuration file on the subordinate device.

Examples

Download **test.cfg** from the IPv4 TFTP server at 2.2.2.2 in the public network, and specify the file as the main next-startup configuration file.

```
<Sysname> restore startup-configuration from 2.2.2.2 test.cfg
Restoring the next startup-configuration file from 2.2.2.2. Please wait...finished.
```

Download **test.cfg** from the IPv4 TFTP server at 2.2.2.2 in MPLS L3VPN instance **VPN1**, and specify the file as the main next-startup configuration file.

```
<Sysname> restore startup-configuration from 2.2.2.2 test.cfg vpn-instance VPN1
Restoring the next startup-configuration file from 2.2.2.2. Please wait...finished.
```

Download **test.cfg** from the IPv6 TFTP server at 2001::2 in the public network, and specify the file as the main next-startup configuration file.

```
<Sysname> restore startup-configuration from ipv6 2001::2 test.cfg
Restoring the next startup-configuration file from 2001::2. Please wait...finished.
```

Related commands

backup startup-configuration

save

Use **save** *file-url* [**all** | **slot** *slot-number*] to save the running configuration to a configuration file, without specifying the file as a next-startup configuration file.

Use **save** [**safely**] [**backup** | **main**] [**force**] [**changed**] to save the running configuration as a next-startup configuration file in the root directory of the storage medium.

Syntax

save *file-url* [**all** | **slot** *slot-number*]

save [**safely**] [**backup** | **main**] [**force**] [**changed**]

Views

Any view

Predefined user roles

network-admin

Parameters

file-url: Specifies a file path, a string of up to 255 characters. The file must be a .cfg file. If you specify the **all** keyword or the **slot** *slot-number* option, the file path cannot include a member ID. If the file path includes a folder name, the folder must already exist on the specified IRF member devices.

all: Saves the running configuration to all member devices. If you do not specify this keyword or the **slot** *slot-number* option, the command saves the running configuration only to the master.

slot *slot-number*: Specifies a subordinate device by its member ID. If you do not specify a subordinate device or the **all** keyword, this command saves the running configuration only to the master.

safely: Saves the configuration file in safe mode. If you do not specify this keyword, the device saves the configuration file in fast mode.

backup: Saves the running configuration to a configuration file, and specifies the file as the backup next-startup configuration file. If you do not specify this keyword or the **main** keyword, the command specifies the saved file as the main next-startup configuration file.

main: Saves the running configuration to a configuration file, and specifies the file as the main next-startup configuration file. If you do not specify this keyword or the **backup** keyword, the command specifies the saved file as the main next-startup configuration file.

force: Saves the running configuration to the existing next-startup configuration file without prompting for confirmation. If you do not specify this keyword, the system prompts you to confirm the operation. If you do not confirm the operation within 30 seconds, the system automatically aborts the operation. If you enter **Y** within the time limit, you can continue the save process and change the target file name during the process.

changed: Overwrites the target configuration file with the running configuration if an inconsistency is detected between the settings in the configuration file and the running configuration. The **save** command does not take effect if no inconsistency is detected. If you do not specify this keyword, the **save** command always overwrites the target configuration file with the running configuration.

Usage guidelines

If you do not specify a file name or the **force** keyword when entering the **save** command, the system prompts for a file name when the command is executing. The device saves the running configuration to the specified file and specifies the file as a next-startup configuration file.

- If the specified file does not exist, the device creates the file before saving the running configuration.
- If the specified file already exists in the root directory of the storage medium, the device compares the running configuration with the existing file and displays the difference summary. You can choose to cancel the save operation and use the **display diff** command to view detailed configuration differences or continue the save operation to overwrite the existing file.

If you specify a file name when entering the **save** command, the device saves the running configuration only to the specified file.

- If the specified file does not exist, the device creates the file before saving the running configuration.
- If the specified file already exists in the root directory of the storage medium, the device does not compare the running configuration with the contents in the existing file. Instead, the device prompts you to confirm whether to overwrite the existing file. If you choose to not overwrite the file, the system cancels the save operation. You can view the differences between the running configuration and the target file by using the **display diff** command.

This command saves the running configuration to an .mdb binary file as well as a .cfg text file. The two files use the same file name. An .mdb file takes less time to load than a .cfg file.

When you use the **save** [**safely**] [**backup** | **main**] [**force**] [**changed**] command, follow these guidelines:

- In safe mode, the system saves configuration in a temporary file and starts overwriting the target next-startup configuration file after the save operation is complete. If a reboot, power failure, or out of memory or storage space event occurs during the save operation, the next-startup configuration file is retained.
- In fast mode, the device directly overwrites the target next-startup configuration file. If a reboot, power failure, or out of memory or storage space event occurs during this process, all settings in the next-startup configuration file are lost.

Safe mode is slower than fast mode, but more secure. As a best practice, specify the **safely** keyword for reliable configuration saving.

By default, the **save** [**safely**] [**backup** | **main**] [**force**] [**changed**] command saves the configuration to all IRF member devices. To save the configuration only to the master device, disable automatic system-wide next-startup configuration file operations. For more information about disabling these operations, see *Fundamentals Configuration Guide*.

Examples

Save the running configuration to **backup.cfg**, without specifying the file as a next-startup configuration file.

```
<Sysname> save backup.cfg
The current configuration will be saved to flash:/backup.cfg. Continue? [Y/N]:y
Now saving current configuration to the device.
Saving configuration flash:/backup.cfg. Please wait...
Configuration is saved to device successfully.
```

Save the running configuration to the main next-startup configuration file without any confirmation required.

```
<Sysname> save force
Validating file. Please wait....
Saved the current configuration to mainboard device successfully.
```

Save the running configuration to file **test.cfg** in the root directory of the default storage medium, and specify the file as the main next-startup configuration file.

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/backup.cfg]
(To leave the existing filename unchanged, press the enter key):test.cfg
Validating file. Please wait.............
Saved the current configuration to mainboard device successfully.
```

Save the running configuration to file **backup.cfg** in the root directory of the default storage medium, and specify the file as the main next-startup configuration file. In this example, the specified file already exists in the root directory of the default storage medium.

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/backup.cfg]
(To leave the existing filename unchanged, press the enter key):backup.cfg
Validating file. Please wait.............
The backup.cfg file already exists.
Compared with the backup.cfg file, the current configuration adds 5 commands and deletes
2 commands.
If you want to see the configuration differences, please cancel this operation, and then
use the display diff command to show the details.
If you continue the save operation, the file will be overwritten.
Are you sure you want to continue the save operation? [Y/N]:y
Saving the current configuration to the file. Please wait...
Saved the current configuration to mainboard device successfully.
```

Related commands

display current-configuration

display diff

display saved-configuration

standby auto-update config

Use **standby auto-update config** to enable automatic system-wide next-startup configuration file operations.

Use **undo standby auto-update config** to disable automatic system-wide next-startup configuration file operations.

Syntax

standby auto-update config

undo standby auto-update config

Default

Next-startup configuration file operations are automatically synchronized across the entire system.

Views

System view

Predefined user roles

network-admin

Usage guidelines

By default, automatic system-wide next-startup configuration file operations are enabled. The system performs the following operations on all IRF subordinate devices in addition to the master device:

- Saves the running configuration to the next-startup configuration file on each member device when you execute the **save** [**safely**] [**backup** | **main**] [**force**] [**changed**] command.
- Deletes the next-startup configuration file on each member device when you execute the# **reset saved-configuration** command.

If you disable automatic system-wide next-startup configuration file operations, the system saves the running configuration or deletes the next-startup configuration file only on the master device.

Automatic system-wide operations ensure start-up configuration file consistency between the master and subordinate devices. However, a system-wide operation takes more time than an operation performed only on the master device. In addition, the amount of time required to complete a system-wide configuration operation increases as the amount of configuration data grows.

If you are disabling automatic system-wide operations for faster configuration saving, be aware that the next-startup configuration files will be inconsistent between the master device and the subordinate devices.

Examples

Enable automatic system-wide next-startup configuration file operations.

```
<Sysname> system-view
[Sysname] standby auto-update config
```

Related commands

reset saved-configuration

save

startup saved-configuration

Use **startup saved-configuration** to specify a file as a next-startup configuration file.

Use **undo startup saved-configuration** to configure the system to start up with the factory defaults at the next startup.

Syntax

startup saved-configuration *cfgfile* [**backup** | **main**]

undo startup saved-configuration

Default

No next-startup configuration files are specified.

Views

User view

Predefined user roles

network-admin

Parameters

cfgfile: Specifies the path of a configuration file, a string of up to 191 characters. The file must be a .cfg file. The file path can include only the file name, or the storage medium information and file name. If the file is not on the default storage medium, you must specify the file name with storage medium information.

backup: Specifies the configuration file as the backup next-startup configuration file.

main: Specifies the configuration file as the main next-startup configuration file. This is the primary configuration file that the device attempts to load at startup. If the loading attempt fails, the device tries the backup next-startup configuration file.

Usage guidelines

CAUTION:

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

The **startup saved-configuration** command applies to all IRF members. To successfully execute this command, make sure the specified file has been saved in the root directory of the storage medium on each member.

If you do not specify the **backup** or **main** keyword, the **startup saved-configuration** command specifies the main next-startup configuration file.

As a best practice, specify different files as the main and backup next-startup configuration files.

The **undo startup saved-configuration** command changes the file attribute of the main and backup next-startup configuration files to NULL. However, the command does not delete the two configuration files.

You can also specify a configuration file as a next startup file when you use the **save** command to save the running configuration.

Examples

Specify the main next-startup configuration file.

```
<Sysname> startup saved-configuration testcfg.cfg
Please wait ....... Done.
```

Related commands

display startup

Software upgrade commands

As a best practice, store the startup images in a fixed storage medium. If you store the startup images in a hot swappable storage medium, do not remove the hot swappable storage medium during the startup process.

boot-loader file

Use **boot-loader file** to specify startup image files.

Syntax

boot-loader file boot *filename* **system** *filename* [**feature** *filename*&<1-30>] [**patch** *filename*&<1-16>] { **all** | **slot** *slot-number* } { **backup** | **main** }

boot-loader file *ipe-filename* [**patch** *filename*&<1-16>] { **all** | **slot** *slot-number* } { **backup** | **main** }

Views

User view

Predefined user roles

network-admin

Parameters

boot: Specifies a boot image file.

system: Specifies a system image file.

feature: Specifies a space-separated list of up to 30 feature image files.

patch: Specifies a space-separated list of up to 16 patch image files. You can specify only non-incremental patch image files.

filename: Specifies a .bin file in the *filesystemname***:***filename***.bin** format. The file must be stored in the root directory of a file system on the device. Excluding the file system location section (if any), the value string can have a maximum of 63 characters. For more information about specifying a file, see *Fundamentals Configuration Guide*.

ipe-filename: Specifies an .ipe image package file in the *filesystemname***:***filename***.ipe** format. The file must be stored in the root directory of a file system on the device. Excluding the file system location section (if any), the value string can have a maximum of 63 characters. For more information about specifying a file, see *Fundamentals Configuration Guide*.

all: Specifies all IRF member devices.

slot *slot-number*: Specifies the IRF member ID of a member device.

backup: Specifies the files as backup startup image files. Backup images are used only when main images are not available.

main: Specifies the files as main startup image files. The device always first attempts to start up with main startup files.

Usage guidelines

The **boot-loader file** command overwrites the entire startup image list. To add new startup feature images, specify all feature image files in the old startup image list, including feature image files. The new startup image list will contain only the feature image files that are specified in the command.

To load the specified startup software images, you must reboot the system.

If the upgrade images are not found in the file system on the slot specified to upgrade, the system automatically copies the images to that file system. The destination directory is the root directory of the file system. If the destination root directory already contains a startup image with the same name as an upgrade image, you must choose whether to overwrite the image.

Examples

Specify **flash:/all.ipe** as the main startup image file for slot 1.

```
<Sysname> boot-loader file flash:/all.ipe slot 1 main
Verifying the file flash:/all.ipe on slot 1.............Done.
HPE FF 5945 4-slot Switch images in IPE:
  boot.bin
  system.bin
This command will set the main startup software images. Continue? [Y/N]:Y
Add images to slot 1.
File flash:/boot.bin already exists on slot 1.
File flash:/system.bin already exists on slot 1.
Overwrite the existing files? [Y/N]:Y
Decompressing file boot.bin to flash:/boot.bin.......................Done.
Decompressing file system.bin to flash:/system.bin..............................Done.
Verifying the file flash:/boot.bin on slot 1...Done.
Verifying the file flash:/system.bin on slot 1.............Done.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 1.
```

Specify **flash:/all.ipe** as the main startup image file for all IRF member devices.

```
<Sysname> boot-loader file slot1#flash:/all.ipe all main
Verifying the file flash:/all.ipe on slot 1.....................................Done.
HPE FF 5945 4-slot Switch images in IPE:
  boot.bin
  system.bin
This command will set the main startup software images. Continue? [Y/N]:y
Add images to slot 1.
File flash:/boot.bin already exists on slot 1.
File flash:/system.bin already exists on slot 1.
Overwrite the existing files? [Y/N]:y
Decompressing file boot.bin to flash:/boot.bin.......................Done.
Decompressing file system.bin to flash:/system.bin.......................Done.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 1.
File flash:/boot.bin already exists on slot 2.
Do you want to overwrite the file?
 Y: Overwrite the file.
 N: Not overwrite the file.
 A: From now on, overwrite or not overwrite without prompt.
Please make a choice. [Y/N/A]:a
What type of overwrite operation do you want to perform?
 Y: Overwrite without prompt.
 N: Not overwrite or display prompt.
 Q: Return to the previous step.
```

```
Please make a choice. [Y/N/Q]:y
An existing file will be overwritten without prompt if it has the same name as any upgrade
file.
Loading.....................Done.
Loading.....................Done.
Loading.....................Done.
Loading.....................Done.
Loading.....................Done.
Loading.....................Done.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 2.
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 3.
Decompression completed.
Do you want to delete flash:/all.ipe now? [Y/N]:n
```

Related commands

display boot-loader

boot-loader update

Use **boot-loader update** to synchronize startup images.

Syntax

boot-loader update { **all** | **slot** *slot-number* }

Views

User view

Predefined user roles

network-admin

Parameters

all: Synchronizes startup images from the master to all subordinate devices.

slot *slot-number*: Specifies the IRF member ID of a subordinate device.

Usage guidelines

You can use this command to synchronize startup images after adding new member devices.

The startup images synchronized to the subordinate device are set as main startup images, regardless of whether the source startup images are main or backup.

- If the master device has started up with main startup images, its main startup images are synchronized to the subordinate device, regardless of whether any main startup image has been respecified on the master device.
- If the master device has started up with backup startup images, its backup startup images are synchronized to the subordinate device, regardless of whether any backup startup image has been respecified on the master device.

If a patch installation or ISSU has been performed on the master, use the **install commit** command to update the set of main startup images on the master before software synchronization. This command ensures startup image consistency between the master and the subordinate device.

Startup image synchronization fails if any software image being synchronized is not available or is corrupted.

Examples

Synchronize startup images to a slot.

```
<Sysname> boot-loader update slot 2
This command will update the specified standby MPU. Continue? [Y/N]:y
Updating. Please wait...
Verifying the file flash:/boot.bin on slot 1...Done.
Verifying the file flash:/system.bin on slot 1....Done.
Copying main startup software images to slot 2. Please wait...
Done.
Setting copied images as main startup software images for slot 2...
The images that have passed all examinations will be used as the main startup software
images at the next reboot on slot 2.
Done.
Successfully updated the startup software images of slot 2.
```

Related commands

display boot-loader

install commit

display boot-loader

Use **display boot-loader** to display current software images and startup software images.

Syntax

display boot-loader [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies the member ID of an IRF member device. If you do not specify a member device, this command displays the software images on each IRF member device.

Examples

Display the current software images and startup software images.

```
<Sysname> display boot-loader
Software images on slot 1:
Current software images:
  flash:/boot.bin
  flash:/system.bin
Main startup software images:
  flash:/boot.bin
  flash:/system.bin
Backup startup software images:
  flash:/boot.bin
  flash:/system.bin
```

Table 24 Command output

Field	Description
Current software images	Comware images that have been loaded.
Main startup software images	Primary Comware images for the next startup.
Backup startup software images	Backup Comware images for the next startup.

Related commands

boot-loader file

ISSU commands

display install active

Use **display install active** to display active software images.

Syntax

display install active [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all IRF members.

verbose: Displays detailed information. If you do not specify this keyword, the command displays only image names.

Examples

Display active software images.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot.bin
  flash:/system.bin
  flash:/feature1.bin
```

Display detailed information about active software images.

```
<Sysname> display install active verbose
Active packages on slot 1:
flash:/boot.bin
 [Package]
 Vendor: HPE
 Product: 5945
 Service name: boot
 Platform version: 7.1.070
 Product version: Test 0001015
 Supported board: mpu
 [Component]
 Component: boot
 Description: boot package

flash:/system.bin
 [Package]
 Vendor: HPE
 Product: 5945
```

```
 Service name: system
 Platform version: 7.1.070
 Product version: Test 0001015
 Supported board: mpu
 [Component]
 Component: system
 Description: system package

flash:/feature1.bin
 [Package]
 Vendor: HPE
 Product: 5945
 Service name: test
 Platform version: 7.1.070
 Product version: Test 0001015
 Supported board: mpu
 [Component]
 Component: test
 Description: test package
```

Table 25 Command output

Field	Description
[Package]	Detailed information about the software image.
Service name	Image type: • **boot**—Boot image. • **system**—System image. • **boot patch**—Patch image for the boot image. • **system patch**—Patch image for the system image. • Any other value indicates a feature image.
Supported board	Hardware types supported by the software image: **mpu**—Member device.
[Component]	Information about components included in the image file.

Related commands

`install active`

display install backup

Use **`display install backup`** to display backup startup software images.

Syntax

`display install backup` [**`slot`** *`slot-number`*] [**`verbose`**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all IRF members.

verbose: Displays detailed information. If you do not specify this keyword, the command displays only image names.

Usage guidelines

Backup startup images are used only when the main boot or system image is missing or corrupt. For more information, see *Fundamentals Configuration Guide*.

To modify the backup startup image list, use the **boot-loader file** command.

Examples

Display the backup startup software images.

```
<Sysname> display install backup
Backup startup software images on slot 1:
  flash:/boot.bin
  flash:/system.bin
```

Display detailed information about backup startup software images.

```
<Sysname> display install backup verbose
Backup startup software images on slot 1:
 flash:/boot.bin
 [Package]
 Vendor: HPE
 Product: 5945
 Service name: boot
 Platform version: 7.1.070
 Product version: Test 0001015
 Supported board: mpu
 [Component]
 Component: boot
 Description: boot package

 flash:/system.bin
 [Package]
 Vendor: HPE
 Product: 5945
 Service name: system
 Platform version: 7.1.070
 Product version: Test 0001015
 Supported board: mpu
 [Component]
 Component: system
 Description: system package
```

For information about the command output, see Table 25.

Related commands

boot-loader file

display install committed

Use **display install committed** to display main startup software images.

Syntax

display install committed [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

verbose: Displays detailed information. If you do not specify this keyword, the command displays only image names.

Usage guidelines

Some **install** commands modify the current software image list but do not modify the main startup image list. For the software image changes to take effect after a reboot, you must execute the **install commit** command to update the main startup image list with the image changes. You can use the **display install committed** command to verify the operation results.

Both the **install commit** and **boot-loader file** commands modify the main startup software image list.

Examples

Display the main startup software images.

```
<Sysname> display install committed
Committed packages on slot 1:
 flash:/boot.bin
 flash:/system.bin
 flash:/feature1.bin
```

Display detailed information about main startup software images.

```
<Sysname> display install committed verbose
Committed packages on slot 1:
 flash:/boot.bin
 [Package]
 Vendor: HPE
 Product: 5945
 Service name: boot
 Platform version: 7.1.070
 Product version: Test 0001015
 Supported board: mpu
 [Component]
 Component: boot
 Description: boot package
```

```
 flash:/system.bin
 [Package]
 Vendor: HPE
 Product: 5945
 Service name: system
 Platform version: 7.1.070
 Product version: Test 0001015
 Supported board: mpu
 [Component]
 Component: system
 Description: system package

flash:/feature1.bin
 [Package]
 Vendor: HPE
 Product: 5945
 Service name: feature1
 Platform version: 7.1.070
 Product version: Test 0001015
 Supported board: mpu
 [Component]
 Component: feature1
 Description: feature1 package
```

For information about the command output, see Table 25.

Related commands

boot-loader file

display install backup

install commit

display install inactive

Use **display install inactive** to display inactive software images in the root directories of file systems.

Syntax

display install inactive [**slot** *slot-number*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

verbose: Displays detailed information. If you do not specify this keyword, the command displays only image names.

Examples

Display brief information about inactive software images in the root directories of the file systems.

```
<Sysname> display install inactive
Inactive packages on slot 1:
 flash:/feature1.bin
```

Display detailed information about inactive software images in the root directories of the file systems.

```
<Sysname> display install inactive verbose
Inactive packages on slot 1:
flash:/feature1.bin
 [Package]
 Vendor: HPE
 Product: 5945
 Service name: feature1
 Platform version: 7.1.070
 Product version: Test 0001015
 Supported board: mpu
 [Component]
 Component: feature1
 Description: feature1 package
```

For information about the command output, see Table 25.

Related commands

install deactivate

display install ipe-info

Use **display install ipe-info** to display the software images included in an .ipe file.

Syntax

display install ipe-info *ipe-filename*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipe-filename: Specifies an .ipe file in the *filesystemname*/*filename*.**ipe** format. The file must be stored in the root directory of a file system on the device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

Examples

Display information about .ipe file **flash:/test.ipe**.

```
<Sysname> display install ipe-info flash:/test.ipe
Verifying the file flash:/test.ipe on slot 1.............Done.
```

```
HPE FF 5945 4-slot Switch images in IPE:
  boot.bin
  system.bin
```

Related commands

display install package

display install job

Use **display install job** to display ongoing ISSU activate, deactivate, and rollback operations.

Syntax

display install job

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display ongoing ISSU activate, deactivate, and rollback operations.

```
<Sysname> display install job
 JobID:5
  Action:install activate flash:/feature1.bin on slot 1
```

The output shows that the device is executing the **install activate flash:/feature1.bin slot 1** command.

display install log

Use **display install log** to display ISSU log information.

Syntax

display install log [*log-id*] [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

log-id: Specifies a log entry by its ID. If you do not specify this argument, the command displays all ISSU log entries.

verbose: Displays detailed ISSU log information. If you do not specify this keyword, the command displays brief ISSU log information.

Usage guidelines

The device creates one log entry for each ISSU operation to track the ISSU process and operation result.

The ISSU log can contain a maximum of 50 entries. The latest entry overwrites the oldest entry if the log is full.

A device reboot clears all ISSU log entries.

Examples

Display all ISSU log entries.

```
<Sysname> display install log
Install job 1 started by user root at 04/28/2001 08:39:29.
Job 1 completed successfully at 04/28/2001 08:39:30.
Install job 1 started by user root at 04/28/2001 08:39:29.
    Install activate flash:/feature1.bin on slot 1
Job 1 completed successfully at 04/28/2001 08:39:30.
Install job 1 started by user root at 04/28/2001 08:39:29.
Job 1 completed successfully at 04/28/2001 08:39:30.
------------------------------------------------------------
Install job 2 started by user root at 04/28/2001 08:40:29.
Job 2 completed successfully at 04/28/2001 08:40:30.
Install job 2 started by user root at 04/28/2001 08:40:29.
    Install activate flash:/route.bin on slot 1
Job 2 completed successfully at 04/28/2001 08:40:30.
Install job 2 started by user root at 04/28/2001 08:40:29.
Job 2 completed successfully at 04/28/2001 08:40:30.
```

Displays detailed information about ISSU log entry 1.

```
<Sysname> display install log 1 verbose
Install job 1 started by user root at 04/28/2001 08:39:29.
Job 1 completed successfully at 04/28/2001 08:39:30.
Install job 1 started by user root at 04/28/2001 08:39:29.
    Install activate flash:/feature1.bin on slot 1
Job 1 completed successfully at 04/28/2001 08:39:30.
Install job 1 started by user root at 04/28/2001 08:39:29.
Job 1 completed successfully at 04/28/2001 08:39:30.
Detail of activating packages on slot 1.
    Get upgrade policy successfully.
Detail of activating packages on slot 1.
    Uncompress package to system successfully.
    Remove files from system successfully.
```

Table 26 Command output

Field	Description
Detail of xxx	Detailed information about an ISSU operation.
Get upgrade policy successfully.	Obtained the upgrade policy.
Uncompress package to system successfully.	Decompressed the package successfully.
Remove files from system successfully.	Deleted files from the system successfully.

Related commands

reset install log-history oldest

display install package

Use **display install package** to display software image file information.

Syntax

display install package { *filename* | **all** } [**verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

filename: Specifies a .bin file in the *filesystemname*/*filename*.**bin** format. The file must be stored in the root directory of a file system on the device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

all: Specifies all software image files in the root directories of the master's file systems.

verbose: Displays detailed information. If you do not specify this keyword, the command displays only basic software image information.

Examples

Display information about **system.bin**.

```
<Sysname> display install package flash:/system.bin
  flash:/system.bin
  [Package]
  Vendor: HPE
  Product: 5945
  Service name: system
  Platform version: 7.1.070
  Product version: Test 0001015
  Supported board: mpu
```

Display detailed information about **system.bin**.

```
<Sysname> display install package flash:/system.bin verbose
  flash:/system.bin
  [Package]
  Vendor: HPE
  Product: 5945
  Service name: system
  Platform version: 7.1.070
  Product version: Test 0001015
  Supported board: mpu
  [Component]
  Component: system
  Description: system package
```

For information about the command output, see Table 25.

display install rollback

Use **display install rollback** to display rollback point information.

Syntax

display install rollback [*point-id*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

point-id: Specifies a rollback point ID. If you do not specify a rollback point ID, the command displays all rollback points.

Usage guidelines

Use this command to identify available rollback points during an ISSU that uses **install** commands. The system does not record rollback points during an ISSU that uses **issu** commands.

Examples

Display all rollback points.

```
<Sysname> display install rollback
Install rollback information 1 on slot 1:
  Updating from flash:/route-1.bin
         to flash:/route-2.bin.

Install rollback information 2 on slot 1:
   Deactivating flash:/route-2.bin
```

The output shows that the device has two rollback points.

- At rollback point 1, **flash:/route-1.bin** was upgraded to **flash:/route-2.bin**.
- At rollback point 2, **flash:/route-2.bin** was deactivated.

Related commands

install rollback

reset install rollback oldest

display install which

Use **display install which** to display all software image files that include a specific component or file.

Syntax

display install which { **component** *name* | **file** *filename* } [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

component *name*: Specifies a component name.

file *filename*: Specifies a file in the *filename.extension* format, a case-insensitive string of up to 63 characters. It cannot contain path information.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all IRF members.

Usage guidelines

A component is a collection of features. The features of a component are installed or uninstalled at the same time.

When the system displays a component or file error, use this command to identify the image files that include the component or file. Then, you can use the **install verify** command to identify image file problems.

This command searches only the root directories of the file systems at the specified location.

Examples

Display the software image file that includes **pkg_ctr**.

```
<Sysname> display install which file pkg_ctr
Verifying the file flash:/system-t0001015.bin on slot 1.......................Done.
Found pkg_ctr in flash:/system-t0001015.bin on slot 1.
  flash:/system-t0001015.bin
  [Package]
  Vendor: HPE
  Product: 5945
  Service name: system
  Platform version: 7.1.070
  Product version: Test 0001015
  Supported board: mpu

Verifying the file flash:/boot-d2601007.bin on slot 1.....Done.
```

Table 27 Command output

Field	Description
Verifying the file	The system was verifying the validity of the file.
[Package]	Detailed information about the software image.
Service name	Image type: • **boot**—Boot image. • **system**—System image. • **patch**—Patch image. • Any other value indicates a feature image.
Supported board	Hardware types supported by the software image: **mpu**—Member device.

display issu rollback-timer

Use **display issu rollback-timer** to display automatic rollback timer information.

Syntax

display issu rollback-timer

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Change to the automatic rollback interval does not take effect on the ongoing ISSU process. The current remaining rollback time might be greater than the specified automatic rollback interval.

Examples

Display automatic rollback timer information after the **issu run switchover** command is executed.

```
<Sysname> display issu rollback-timer
Rollback timer: Working
Rollback interval: 45 minutes
Rollback time remaining : 40 minutes
```

Display automatic rollback timer information after the **issu accept** command is executed.

```
<Sysname> display issu rollback-timer
Rollback timer: Not working
Rollback interval: 30 minutes
```

Display automatic rollback timer information when no ISSU process is taking place.

```
<Sysname> display issu rollback-timer
Rollback timer: Not working
Rollback interval: 45 minutes
```

Related commands

issu rollback-timer

display issu state

Use **display issu state** to display ISSU status information.

Syntax

display issu state

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

During an ISSU that uses **issu** commands, you can use this command to verify the ISSU status and determine what to do next.

This command does not apply to an ISSU that uses **install** commands, because the ISSU state machine is not involved.

Examples

Display ISSU status information when no upgrade is taking place.

```
<Sysname> display issu state
ISSU state: Init
Compatibility: Unknown
Work state: Normal
Upgrade method: Card by card
Upgraded slot: None
Current upgrading slot: None
Current version list:
  boot: 7.1.070, Test 0001015
  system: 7.1.070, Test 0001015
  feature1: 7.1.070, Test 0001015
Current software images:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
  flash:/feature1-t0001015.bin
```

Display ISSU status information while the **issu load** command is being executed.

```
<Sysname> display issu state
ISSU state: Loading
Compatibility: Incompatible
Work state: Normal
Upgrade method: Card by card
Upgraded slot: None
Current upgrading slot:
  slot 1
Previous version list:
  boot: 7.1.070, Test 0001015
  system: 7.1.070, Test 0001015
  feature1: 7.1.070, Test 0001015
Previous software images:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
  flash:/feature1-t0001015.bin
Upgrade version list:
  boot: 7.1.070, Test 0001016
  system: 7.1.070, Test 0001016
  feature1: 7.1.070, Test 0001016
Upgrade software images:
  flash:/boot-t0001016.bin
  flash:/system-t0001016.bin
  flash:/feature1-t0001016.bin
```

Table 28 Command output

Field	Description
ISSU state	ISSU status: • **Init**—The ISSU process has not started or has finished. • **Loading**—The system is executing the **issu load** command. • **Loaded**—The **issu load** command is completed. • **Switching**—The system is executing the **issu run switchover** command. • **Switchover**—The **issu run switchover** command is completed. • **Accepted**—The **issu accept** command is completed. • **Committing**—The system is executing the **issu commit** command. • **Rollbacking**—A rollback is in progress. • **Unknown**—An upgrade is in progress. This value is displayed if you execute the command on an original subordinate member.
Compatibility	Version compatibility: • **Compatible**—Upgrade to a compatible version. • **Incompatible**—Upgrade to an incompatible version. • **Unknown**—No upgrade is in progress.
Work state	Operating status of the device: • **Normal**—The device is operating correctly. • **Independent active**—When you perform an ISSU to an incompatible version, a subordinate member that is upgraded first enters this state. In this state, member devices are not running the same software versions.
Upgrade method	Upgrade mode. The value of this field is fixed at **Card by card**. In this mode, member devices are upgraded one by one.
Upgraded slot	Upgraded members. During a rollback, this field displays **Unknown**.
Current upgrading slot	Members that are being upgraded. During a rollback, this field displays **Unknown**.
Current version list	Versions of currently running images. This field is displayed if no upgrade is taking place.
Current software images	File names of currently running images. This field is displayed if no upgrade is taking place.
Previous version list	Versions of the images that were running on the device before the ISSU. If you execute the command on an original subordinate member while the member is being upgraded to an incompatible version, this field displays **Unknown**.
Previous software images	File names of the images that were running on the device before the ISSU. If you execute the command on an original subordinate member while the member is being upgraded to an incompatible version, this field displays **Unknown**.
Upgrade version list	Versions of the upgrade images. If you execute the command on an original subordinate member while the member is being upgraded to an incompatible version, this field displays **Unknown**.
Upgrade software images	File names of the upgrade images. If you execute the command on an original subordinate member while the member is being upgraded to an incompatible version, this field displays **Unknown**.

Related commands

issu accept

issu commit

issu load

issu rollback

issu run switchover

display version comp-matrix

Use **display version comp-matrix** to display the recommended ISSU methods.

Syntax

display version comp-matrix file { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> | **patch** *filename*&<1-30> } *

display version comp-matrix file ipe *ipe-filename* [**patch** *filename*&<1-30>]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

boot: Specifies a boot image file.

system: Specifies a system image file.

feature: Specifies a space-separated list of up to 30 feature image files.

patch: Specifies a space-separated list of up to 30 patch image files.

filename: Specifies a .bin file in the *filesystemname*:*filename***.bin** format. The file must be stored in the root directory of a file system on the device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

ipe-filename: Specifies an .ipe file in the *filesystemname*:*filename***.ipe** format. The file must be stored in the root directory of a file system on the device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

Usage guidelines

If one or more images are incompatible, the incompatible upgrade method applies. The entire system needs to be rebooted during an incompatible upgrade.

Examples

Display the recommended ISSU methods. In this example, the specified images are compatible with the running images.

```
<Sysname> display version comp-matrix file boot flash:/boot-t0001015.bin system
flash:/system-t0001015.bin feature flash:/feature1-t0001015.bin patch
flash:/system-patch1-t0001015.bin
Verifying the file flash:/feature1-t0001015.bin on slot 1.....Done.
Verifying the file flash:/boot-t0001015.bin on slot 1.....Done.
```

```
Verifying the file flash:/system-t0001015.bin on slot 1.....Done.
Verifying the file flash:/system-patch1-t0001015.bin on slot 1.....Done.

  Slot     Upgrade Way
  1        File Upgrade
```

Table 29 Command output

Field	Description
Verifying the file	The system was verifying the validity of the file.
Influenced service according to following table	Services that will be affected by the upgrade. This field is displayed only for compatible versions.
Incompatible upgrade	You are upgrading the software to an incompatible version.
Upgrade Way	ISSU method: • **Service Upgrade**. • **File Upgrade**. • **Reboot**. This field is displayed only for compatible versions. For more information about ISSU methods, see *Fundamentals Configuration Guide*.

Related commands

issu load

install abort

Use **install abort** to abort an ongoing activate or deactivate operation.

Syntax

install abort [*job-id*]

Views

User view

Predefined user roles

network-admin

Parameters

job-id: Specifies the job ID of an ISSU operation. If you do not specify this argument, the command aborts all ongoing software image activate and deactivate operations.

Usage guidelines

The system creates a software image management job each time you use the **install activate**, **install add**, **install commit**, **install deactivate**, **install remove**, or **install rollback to** command. Each job represents one command and is assigned a unique job ID. To obtain the ID of a job, use the **display install job** command.

When you abort an ongoing activate or deactivate operation, the system rolls back to the status it was in before the operation was started.

Examples

Abort all ongoing software image activate and deactivate operations.

```
<Sysname> install abort
```

Related commands

display install job

install activate

Use **install activate** to activate software images, or identify the ISSU method and the possible impact on the device.

Syntax

install activate { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> } * **slot** *slot-number* [**test**]

install activate patch *filename* { **all** | **slot** *slot-number* }

Views

User view

Predefined user roles

network-admin

Parameters

boot: Specifies a boot image file.

system: Specifies a system image file.

feature: Specifies a space-separated list of up to 30 feature image files

patch: Specifies a patch image file. You can specify only one patch image file for the command at a time. However, you can execute the command multiple times to activate multiple patch image files. You can specify both incremental and non-incremental patch image files. The device can use a maximum of 30 incremental patch image files. Because the boot, system, and feature images each can have one non-incremental patch image file, the device can use a maximum of 16 non-incremental patch image files. For more information about incremental and non-incremental patch images, see software upgrade in *Fundamentals Configuration Guide*.

filename: Specifies a .bin file in the *filesystemname*/*filename***.bin** format. The file must be stored in the root directory of a file system on the device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

all: Specifies all member devices.

slot *slot-number*: Specifies an IRF member device by its member ID.

test: Only identifies the ISSU method to be used for the upgrade. If you do not specify this keyword, the command activates the specified software images.

Usage guidelines

This command requires that all image files on the startup software image list be the same version after the upgrade is finished. It can be executed successfully only if the boot, system, and feature image files on the list are the same version after the upgrade. Before being executed successfully, this command uninstalls all existing patch image files on the list automatically.

If this command fails, perform the following tasks:

1. If some features are not needed anymore, disable the features and use the **install deactivate** command to uninstall the feature images.
2. Obtain the image files that are required to make sure all image files on the startup software image list are the same version after the upgrade.

3. Specify the image files for this command to activate the images.

Images run in memory immediately after they are activated. However, only patch images activated by using the **install activate patch** *filename* **all** command still run in memory after a reboot. For other images to take effect after a reboot, you must commit the software change by using the **install commit** command.

If the specified files are not stored on the member device to be upgraded, the command copies the images to the member device automatically.

At reboot, a subordinate device automatically synchronizes the master device's configuration and status data. You must wait for the synchronization to complete before using the **install activate** command on the subordinate device. To identify whether the synchronization is complete, use the **display system stable state** command. The synchronization is complete if the **System State** field displays **Stable**.

Examples

Identify the ISSU method for feature upgrade with **feature1.bin** on subordinate member 2 and the upgrade impact.

```
<Sysname> install activate feature flash:/feature1.bin slot 2 test
Copying file flash:/feature1.bin to slot2#flash:/feature1.bin......Done.
Verifying the file flash:/feature1.bin on slot 2.....Done.
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version             New Version
  Test 0001015                Test 0001016

  Slot                        Upgrade Way
  2                           Reboot

Influenced service according to following table:
flash:/feature1.bin
     Feature1
```

The output shows that a reboot upgrade is recommended.

Activate the system image in **system.bin** and the feature images in **feature1.bin** on member device 2.

```
<Sysname> install activate system flash:/system.bin feature flash:/feature1.bin slot 2
Copying file flash:/system.bin to slot2#flash:/system.bin......Done.
Verifying the file flash:/system.bin on slot 2.....Done.
Copying file flash:/feature1.bin to slot2#flash:/feature1.bin......Done.
Verifying the file flash:/feature1.bin on slot 2.....Done.
Upgrade summary according to following table:

flash:/system.bin
  Running Version             New Version
  Test 0001015                Test 0001016

flash:/feature1.bin
  Running Version             New Version
  None                        Test 0001016
```

```
  Slot                        Upgrade Way
  2                           Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

Table 30 Command output

Field	Description
Verifying the file	The system was verifying the validity of the file.
Upgrade summary according to following table	Upgrade summary.
Running Version	Version number of the running software.
New Version	Version number of the new software.
Upgrade Way	ISSU methods: • **Service Upgrade**. • **File Upgrade**. • **Reboot**. This field is displayed only for an upgrade to a compatible version. For more information about ISSU methods, see *Fundamentals Configuration Guide*.
Influenced service according to following table	Services influenced by the upgrade.

Related commands

`display install active`

`install commit`

`install deactivate`

install add

Use **`install add`** to decompress an .ipe file.

Syntax

`install add` *`ipe-filename filesystem`*

Views

User view

Predefined user roles

network-admin

Parameters

`ipe-filename`: Specifies an .ipe file in the *filesystemname***/***filename***.ipe** format. The file must be stored in the root directory of a file system on the device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

`filesystem`: Specifies the destination file system for the software images, in the *filesystemname* format.

Usage guidelines

To use the **install activate** command to activate software images, you must use .bin image files. If the upgrade file is an .ipe file, use this command to decompress the .ipe file before you start the upgrade.

To identify software images that are included in an .ipe file, use the **display install ipe-info** command.

Examples

Decompress **all.ipe** to the flash memory.

```
<Sysname> install add flash:/all.ipe flash:
Verifying the file flash:/all.ipe on slot 1...Done.
Decompressing file boot.bin to flash:/boot.bin.....................Done.
Decompressing file system.bin to
flash:/system.bin.............................Done.
```

install commit

Use **install commit** to commit software changes.

Syntax

install commit

Views

User view

Predefined user roles

network-admin

Usage guidelines

This command adds the patch image file to the startup software image list that the device used at startup.

- If the device used the main startup software image list at startup, this command adds the patch image file to the main startup software image list.
- If the device used the backup startup software image list at startup, this command adds the patch image file to the backup startup software image list.

You must execute this command after using the following commands:

- The **install activate** command in an incremental upgrade.
- The **install deactivate** command.
- The **install rollback** command.

In a reboot upgrade, the **install activate** command modifies both the current and startup software image lists. You do not need to commit software changes.

Both the **install commit** and **boot-loader file** commands modify the main startup software image list. However, the **boot-loader file** command can also modify the backup startup image list and add inactive images as main startup images.

For more information about main and backup startup software images, see *Fundamentals Configuration Guide*.

Examples

Commit software changes.

```
<Sysname> install commit
```

```
This operation will take several minutes, please wait.........................Done.
The current software images have been saved as the startup software images.
Current software images on slot 1:
  flash:/boot.bin
  flash:/system.bin
Current software images on slot 2:
  flash:/boot.bin
  flash:/system.bin
```

Related commands

`install activate`

`install deactivate`

`install rollback`

install deactivate

Use **`install deactivate`** to deactivate feature images and patch images.

Syntax

`install deactivate feature` *`filename`*`&<1-30>` **`slot`** *`slot-number`*

`install deactivate patch` *`filename`* { **`all`** | **`slot`** *`slot-number`* }

Views

User view

Predefined user roles

network-admin

Parameters

`feature`: Specifies a space-separated list of up to 30 feature image files.

`patch`: Specifies a patch image file. You can specify only one patch image file for the command at a time. However, you can execute the command multiple times to deactivate multiple patch image files.

`filename`: Specifies a .bin file in the *filesystemname***/***filename***.bin** format. The value string can have a maximum of 63 characters. The file system name cannot contain file system location information. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

`all`: Specifies all member devices on which the specified patch image file has been activated.

`slot` *`slot-number`*: Specifies an IRF member device by its member ID.

Usage guidelines

At reboot, a subordinate device automatically synchronizes the master device's configuration and status data. You must wait for the synchronization to complete before using the **`install deactivate`** command on the subordinate device. To identify whether the synchronization is complete, use the **`display system stable state`** command. The synchronization is complete if the **System State** field displays **Stable**.

You can deactivate only active feature and patch images.

Images stop running in memory immediately after they are deactivated. However, only patch images deactivated by using the **`install deactivate patch`** *`filename`* **`all`** command do not run

after a reboot. To prevent other deactivated images from running after a reboot, you must commit the software change by using the **install commit** command.

Examples

Deactivate the patch images in the **route-patch.bin** file for a slot.

```
<Sysname> install deactivate patch flash:/route-patch.bin slot 1
This operation might take several minutes, please wait...Done.
```

Related commands

display install active

display install inactive

install remove

Use **install remove** to delete an inactive software image file.

Syntax

install remove [**slot** *slot-number*] { *filename* | **inactive** }

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command deletes inactive software images from all IRF members.

filename: Specifies a .bin file in the *filesystemname***/***filename***.bin** format. The value string can have a maximum of 63 characters. The file must be stored in the root directory of a file system on the device. The file system name cannot contain file system location information. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

inactive: Deletes all inactive software image files in the root directories of the specified file systems.

Usage guidelines

This command permanently deletes the image files from the device. You cannot use the **install rollback to** command to revert the operation, or use the **install abort** command to abort the operation.

Examples

Delete inactive software image file **flash:/feature1.bin**.

```
<Sysname> install remove flash:/feature1.bin
```

install rollback to

Use **install rollback to** to roll back the software to an earlier rollback point.

Syntax

install rollback to { *point-id* | **original** }

Views

User view

Predefined user roles

network-admin

Parameters

point-id: Specifies a rollback point ID. This option is supported only when there are two or more rollback points. To identify available rollback points, use the **display install rollback** command.

original: Rolls back to the status before any activate or deactivate operations were performed.

Usage guidelines

During an incremental upgrade, the system creates a rollback point for each activate or deactivate operation of a boot, system, or feature image. The device supports a maximum of 50 rollback points. The earliest rollback point is deleted if this limit has been reached when a rollback point is created.

During a reboot upgrade, the system does not create rollback points. After the upgrade, you can roll back the software only to the status before any activate or deactivate operations were performed.

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

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

Patch images do not support rollback.

Examples

Roll back the software to rollback point 1.

```
<Sysname>install rollback to 1
This operation might take several minutes, please wait...Done.
```

Roll back the software to the original software versions and observe the change made by the rollback.

```
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
  flash:/feature1-t0001015.bin
<Sysname> display install rollback
Install rollback information 1 on slot 1:
  Updating from no package
         to flash:/feature1-t0001015.bin.
```

The output shows that currently three image files are active but only two of them are confirmed. Image file flash:/feature1-t0001015.bin is not confirmed yet.

```
<Sysname> install rollback to original
This operation might take several minutes, please wait...Done.
<Sysname> display install active
Active packages on slot 1:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
<Sysname> display install committed
Committed packages on slot 1:
  flash:/boot-t0001015.bin
  flash:/system-t0001015.bin
```

The output shows the SSH feature has been rolled back to the original software version. The image file flash:/feature1-t0001015.bin has been removed.

Related commands

display install rollback

install verify

Use **install verify** to verify the software change commit status, image integrity, and image consistency.

Syntax

install verify

Views

User view

Predefined user roles

network-admin

Usage guidelines

To ensure a successful ISSU and make sure that the system can start up and operate correctly after an ISSU, execute this command to verify the following items:

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

If a software image fails the verification, perform the following tasks to resolve the problem:

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

Examples

Verify the software change confirmation status and software image integrity and consistency.

```
<Sysname> install verify
Active packages on slot 1 are the reference packages.
Packages will be compared with the reference packages.
This operation will take several minutes, please wait...
  Verifying packages on slot 1:
  Start to check active package completeness.
Verifying the file flash:/boot-t0001015.bin on slot 1.....................Done.
    flash:/boot-t0001015.bin verification successful.
Verifying the file flash:/system-t0001015.bin on slot 1.....................Done.
    flash:/system-t0001015.bin verification successful.
  Start to check active package consistency.
    Active packages are consistent with committed packages on their own board.
    Active packages are consistent with the reference packages.
  Verifying packages on slot 2:
  Start to check active package completeness.
Verifying the file flash:/boot-t0001015.bin on slot 2.....................Done.
    flash:/boot-t0001015.bin verification successful.
Verifying the file flash:/system-t0001015.bin on slot 2.....................Done.
    flash:/system-t0001015.bin verification successful.
  Start to check active package consistency.
```

```
    Active packages are consistent with committed packages on their own board.
    Active packages are consistent with the reference packages.
Verification is done.
```

issu accept

Use **issu accept** to accept the upgrade to a compatible version and delete the automatic rollback timer.

Syntax

issu accept

Views

User view

Predefined user roles

network-admin

Usage guidelines

The system cannot perform automatic rollback for the ISSU process after you execute this command. However, you can use the **issu rollback** command to perform a manual rollback.

The **issu accept** command does not apply to an ISSU to an incompatible version.

Examples

Accept the upgrade to a compatible version.

```
<Sysname> issu accept
```

Related commands

issu load

issu run switchover

issu commit

Use **issu commit** to upgrade the original master and the subordinate members that have not been upgraded and complete the ISSU upgrade.

Syntax

issu commit slot *slot-number*

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies the member ID of the original master or a subordinate member that has not been upgraded.

Usage guidelines

At reboot, a subordinate device automatically synchronizes the master device's configuration and status data. You must wait for the synchronization to complete before using the **issu commit** command on the subordinate device. To identify whether the synchronization is complete, use the

display system stable state command. The synchronization is complete if the **System State** field displays **Stable**.

Use this command to upgrade the original master and the subordinate members that have not been upgraded, one by one. You must wait for one upgraded member to start up again and join the IRF fabric before upgrading another member. After all members are upgraded, the ISSU status changes to Init, and the ISSU process ends and cannot be rolled back.

Examples

After member 2 is upgraded and becomes the new master, upgrade the original master (member 3) and the other subordinate members that have not been upgraded (member 4 and member 1).

```
<Sysname> issu commit slot 3
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version             New Version
  Test 0001015                Test 0001016

  Slot                        Upgrade Way
  3                           Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
<Sysname> issu commit slot 4
Verifying the file flash:/feature1.bin on slot 4.............Done.
Copying file flash:/feature1.bin to slot4#flash:/feature1.bin...Done.
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version             New Version
  Test 0001015                Test 0001016

  Slot                        Upgrade Way
  4                           Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
<Sysname> issu commit slot 1
Verifying the file flash:/feature1.bin on slot 1.............Done.
Copying file flash:/feature1.bin to slot1#flash:/feature1.bin...Done.
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version             New Version
  Test 0001015                Test 0001016

  Slot                        Upgrade Way
  1                           Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

For information about the command output, see Table 29.

Related commands

issu accept

issu load

issu run switchover

issu load

Use **issu load** to upgrade the software images of subordinate members and configure the new images as main startup software images for those members.

Syntax

issu load file { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> | **patch** *filename*&<1-30> } * **slot** *slot-number*&<1-9> [**reboot**]

issu load file ipe *ipe-filename* [**patch** *filename*&<1-30>] **slot** *slot-number*&<1-9> [**reboot**]

Views

User view

Predefined user roles

network-admin

Parameters

boot: Specifies a boot image file.

system: Specifies a system image file.

feature: Specifies a space-separated list of up to 30 feature image files.

patch: Specifies a space-separated list of up to 30 patch image files. You can specify both incremental and non-incremental patch image files. The device can have a maximum of 30 incremental patch image files. Because the boot image, system image, and feature images each can have only one non-incremental patch image file, the device can have a maximum of 16 non-incremental patch image files. For more information about incremental and non-incremental patch images, see software upgrade in *Fundamentals Configuration Guide*.

filename: Specifies a .bin file in the *filesystemname*:*filename***.bin** format. The file must be stored in the root directory of a file system on the master device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

ipe-filename: Specifies an .ipe file in the *filesystemname*:*filename***.ipe** format. The file must be stored in the root directory of a file system on the master device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

slot *slot-number*: Specifies the member ID of a subordinate member. You can specify a space-separated list of up to nine member IDs. On a single-chassis IRF fabric, enter the member ID of the member device to upgrade the entire fabric. On a multichassis IRF fabric, you can specify only one member ID for a compatible upgrade and can specify multiple member IDs for an incompatible upgrade. As a best practice, specify half of the subordinate members if the member devices form a ring. Make sure the specified subordinate members are directly connected by physical links.

reboot: Uses the reboot method for the upgrade. For an incremental upgrade, specify this keyword if you want to use the reboot upgrade method. If you do not specify this keyword, the recommended upgrade method is used.

Usage guidelines

This command requires that all image files on the startup software image list be the same version after the upgrade is finished. It can be executed successfully only if the boot, system, and feature image files on the list are the same version after the upgrade. Before being executed successfully, this command uninstalls all existing patch image files on the list automatically.

If this command fails, perform the following tasks:

1. If some features are not needed anymore, disable the features and use the **`install deactivate`** command to uninstall the feature images.
2. Obtain the image files that are required to make sure all image files on the startup software image list are the same version after the upgrade.
3. Specify the image files for this command to activate the images.

This command performs the following operations:

- Checks the version compatibility.
- Identifies the upgrade method.
- Loads the new images to upgrade the member devices.
- Sets the new images as the main startup software images so the upgrade can survive a reboot.

At reboot, a subordinate device automatically synchronizes the master device's configuration and status data. You must wait for the synchronization to complete before using the **`issu load`** command on the subordinate device. To identify whether the synchronization is complete, use the **`display system stable state`** command. The synchronization is complete if the **System State** field displays **Stable**.

Examples

Upgrade member device 2 (a subordinate member) with feature image file **flash:/feature1.bin**, and install a patch image file for the feature image. (In this example, the image is compatible with the running images.)

```
<Sysname> issu load file feature flash:/feature1.bin patch flash:/feature1-patch1.bin
slot 2
This operation will delete the rollback point information for the previous upgrade and
maybe get unsaved configuration lost. Continue? [Y/N]:Y
Verifying the file flash:/feature1.bin on slot 1...Done.
Verifying the file flash:/feature1-patch1.bin on slot 1...Done.
Copying file flash:/feature1.bin to slot2#flash:/feature1.bin......Done.
Copying file flash:/feature1-patch1.bin to slot2#flash:/feature1-patch1.bin......Done.
Verifying the file flash:/feature1.bin on slot 2...Done.
Verifying the file flash:/feature1-patch1.bin on slot 2...Done.
Identifying the upgrade methods….Done.
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version             New Version
  Test 0001015                Test 0001016

flash:/feature1-patch1.bin
  Running Version             New Version
  None                        Test 0001016

  Slot                        Upgrade Way
  2                           Service Upgrade
```

```
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

Use the reboot method to upgrade and patch member device 2 (a subordinate member) when the incremental upgrade method is recommended.

```
<Sysname> issu load file feature flash:/feature1.bin patch flash:/feature1-patch1.bin
slot 2 reboot
This operation will delete the rollback point information for the previous upgrade and
maybe get unsaved configuration lost. Continue? [Y/N]:Y
Verifying the file flash:/feature1.bin on slot 1...Done.
Verifying the file flash:/feature1-patch1.bin on slot 1...Done.
Copying file flash:/feature1.bin to slot2#flash:/feature1.bin......Done.
Copying file flash:/feature1-patch1.bin to slot2#flash:/feature1-patch1.bin......Done.
Verifying the file flash:/feature1.bin on slot 2...Done.
Verifying the file flash:/feature1-patch1.bin on slot 2...Done.
Identifying the upgrade methods….Done.
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version             New Version
  Test 0001015                Test 0001016

flash:/feature1-patch1.bin
  Running Version             New Version
  None                        Test 0001016

  Slot                        Upgrade Way
  2                           Reboot
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

Upgrade member devices 3 and 4 (subordinate members) with feature image file **flash:/feature1.bin**, and install a patch image file for the feature image. (In this example, the image is incompatible with the running images.)

```
<Sysname> issu load file feature flash:/feature1.bin patch flash:/feature1-patch1.bin
slot 3 4
This operation will delete the rollback point information for the previous upgrade and
maybe get unsaved configuration lost. Continue? [Y/N]:Y
Verifying the file flash:/feature1.bin on slot 1...Done.
Verifying the file flash:/feature1-patch1.bin on slot 1...Done.
Copying file flash:/feature1.bin to slot3#flash:/feature1.bin......Done.
Copying file flash:/feature1-patch1.bin to slot3#flash:/feature1-patch1.bin......Done.
Verifying the file flash:/feature1.bin on slot 3...Done.
Verifying the file flash:/feature1-patch1.bin on slot 3...Done.
Copying file flash:/feature1.bin to slot4#flash:/feature1.bin......Done.
Copying file flash:/feature1-patch1.bin to slot4#flash:/feature1-patch1.bin......Done.
Verifying the file flash:/feature1.bin on slot 4...Done.
Verifying the file flash:/feature1-patch1.bin on slot 4...Done.
Identifying the upgrade methods….Done.
Upgrade summary according to following table:
```

```
flash:/feature1.bin
  Running Version             New Version
  Test 0001015                Test 0001016

flash:/feature1-patch1.bin
  Running Version             New Version
  None                        Test 0001016

  Slot                        Upgrade Way
  3                           Reboot
  4                           Reboot
Upgrading software images to incompatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

Table 31 Command output

Field	Description
Verifying the file	The system was verifying the validity of the file.
Copying file	The system was copying the upgrade file to a subordinate member. This field is displayed if you specified a subordinate member for the command.
Upgrade Way	ISSU method: • **Service Upgrade**. • **File Upgrade**. • **Reboot**. This field is displayed only for an upgrade to a compatible version. For more information about ISSU methods, see *Fundamentals Configuration Guide*.

issu one-step

Use **issu one-step** to perform an ISSU in one step.

Syntax

issu one-step file { **boot** *filename* | **system** *filename* | **feature** *filename*&<1-30> | **patch** *filename*&<1-30> } * [**slot** *slot-number*&<1-9>] [**reboot**]

issu one-step file ipe *ipe-filename* [**patch** *filename*&<1-30>] **slot** *slot-number*&<1-9> [**reboot**]

Views

User view

Predefined user roles

network-admin

Parameters

boot: Specifies a boot image file.

system: Specifies a system image file.

feature: Specifies a space-separated list of up to 30 feature image files.

patch: Specifies a space-separated list of up to 30 patch image files. You can specify both incremental and non-incremental patch image files. The device can have a maximum of 30 incremental patch image files. Because the boot image, system image, and feature images each can have only one non-incremental patch image file, the device can have a maximum of 16 non-incremental patch image files. For more information about incremental and non-incremental patch images, see software upgrade in *Fundamentals Configuration Guide*.

filename: Specifies a .bin file in the *filesystemname***:***filename***.bin** format. The file must be stored in the root directory of a file system on the master device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

ipe-filename: Specifies an .ipe file in the *filesystemname***:***filename***.ipe** format. The file must be stored in the root directory of a file system on the master device. The value string excluding the file system location section (if any) can have a maximum of 63 characters. For more information about specifying a file, see file system management in *Fundamentals Configuration Guide.*

slot *slot-number*: Specifies the member ID of a subordinate member.

- On a single-chassis IRF fabric, enter the member ID of the member device.
- On a multichassis IRF fabric, you can specify only one member ID for a compatible upgrade. The member device will become the master device after the ISSU. For an incompatible upgrade, you can specify a space-separated list of up to nine member IDs. As a best practice, specify half of the subordinate members if the member devices form a ring. Make sure the specified subordinate members are directly connected by physical links. The device automatically selects one of the specified subordinate members as the master device after the ISSU. If you do not specify this option, the device automatically selects one subordinate member as the master device after the ISSU.

reboot: Uses the reboot method for the upgrade. For an incremental upgrade, specify this keyword if you want to use the reboot upgrade method. If you do not specify this keyword, the recommended upgrade method is used.

Usage guidelines

This command starts and finishes an ISSU. During the operation, you cannot perform a rollback or any other tasks.

Both the current software version and the new software version must support one-step ISSU.

This command requires that all image files on the startup software image list be the same version after the upgrade is finished. It can be executed successfully only if the boot, system, and feature image files on the list are the same version after the upgrade. Before being executed successfully, this command uninstalls all existing patch image files on the list automatically.

If this command fails, perform the following tasks:

1. If some features are not needed anymore, disable the features and use the **install deactivate** command to uninstall the feature images.
2. Obtain the image files that are required to make sure all image files on the startup software image list are the same version after the upgrade.
3. Specify the image files for this command to activate the images.

At reboot, a subordinate device automatically synchronizes the master device's configuration and status data. Before using this command, identify whether the synchronization is complete on all subordinate devices by using the **display system stable state** command. The synchronization is complete if the **System State** field displays **Stable**.

Examples

Perform an ISSU in one step by using **flash:/boot.bin**, **flash:/system.bin**, and **flash:/feature1.bin**.

```
<Sysname> issu one-step file boot flash:/boot.bin system flash:/system.bin feature
flash:/feature1.bin
```

```
This operation will delete the rollback point information for the previous upgrade and
maybe get unsaved configuration lost. Continue? [Y/N]:Y
This operation might take several minutes, please wait...Done.
```

Use the reboot method to perform an ISSU in one step.

```
<Sysname> issu one-step file boot flash:/boot.bin system flash:/system.bin feature
flash:/feature1.bin flash:/feature1.bin reboot
This operation will delete the rollback point information for the previous upgrade and
maybe get unsaved configuration lost. Continue? [Y/N]:Y
This operation might take several minutes, please wait...Done.
```

issu quit

Use **issu quit** to terminate the ongoing ISSU process forcibly.

Syntax

issu quit

Views

System view

Predefined user roles

network-admin

Usage guidelines

Use this command to terminate the ISSU process if one of the following exceptions occurs and you cannot perform an upgrade or rollback:

- The ISSU status is not **Init** but the upgrade has stopped.
- The ISSU status is **Init** but the upgrade has not completed.

After using this command to terminate the ISSU process, identify whether the requirements for an ISSU are met. If yes, use **boot-loader** or **install** commands as needed to restore the device to the state prior to the terminated ISSU and then try an ISSU again. If the ISSU fails again, contact the technical support.

Examples

Terminate the ongoing ISSU process forcibly.

```
<Sysname> system-view
[Sysname] issu quit
This command stops the ongoing ISSU process. Execute this command only under the guidance
of the technical support. Continue? [Y/N]:y

Succeeded.
```

Related commands

install activate

issu load

issu rollback

Use **issu rollback** to cancel the ISSU and roll back to the original software versions.

Syntax

issu rollback

Views

User view

Predefined user roles

network-admin

Usage guidelines

The device supports automatic rollback and manual rollback. This command performs a manual rollback.

You can perform a manual rollback while an ISSU is in one of the following states:

- Loaded.
- Switching (during an upgrade to a compatible version).
- Switchover (during an upgrade to a compatible version).
- Accepted.

In Switching state, a rollback during a reboot upgrade and an automatic rollback during an incompatible upgrade can result in the following situations:

- The upgraded subordinate members reboot.
- The master might also reboot because of a master/subordinate switchover, resulting in service outage.
- After the rollback, the member devices run the software that they run before the upgrade, but their master/subordinate roles might not be the same as before.

As a best practice, make sure the automatic rollback timer is long enough, and do not perform a rollback while an ISSU is in Switching state.

Examples

Roll back to the original software versions.

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

Related commands

issu accept

issu commit

issu load

issu run switchover

issu rollback-timer

Use **issu rollback-timer** to set the automatic rollback timer.

Use **undo issu rollback-timer** to restore the default.

Syntax

issu rollback-timer *minutes*

undo issu rollback-timer

Default

The automatic rollback timer is set to 45 minutes.

Views

System view

Predefined user roles

network-admin

Parameters

minutes: Specifies the automatic rollback interval, in the range of 0 to 120 minutes. Setting it to 0 disables automatic rollback.

Usage guidelines

The automatic software version rollback feature is available only during an ISSU to a compatible version when the IRF fabric has multiple members.

The system starts the automatic rollback timer when you execute the **issu run switchover** command in a scenario where automatic rollback is supported. If you do not execute the **issu accept** or **issu commit** command before the timer expires, the system automatically rolls back to the software version used before the ISSU.

Change to the automatic rollback interval does not take effect on the ongoing ISSU process.

Examples

Set the automatic rollback timer to 50 minutes.

```
<Sysname> system-view
[Sysname] issu rollback-timer 50
```

Related commands

issu rollback

issu run switchover

Use **issu run switchover** to perform an ISSU switchover.

Syntax

issu run switchover

Views

User view

Predefined user roles

network-admin

Usage guidelines

Use this command on a multichassis IRF fabric.

- For a compatible upgrade, this command performs operations depending on the ISSU method.
  - **Incremental upgrade**—Performs a process-level master/subordinate switchover for the processes to be upgraded.
  - **Reboot upgrade**—Reboots the current master with the old software version, causing the upgraded subordinate member to be elected as the new master.
- For an incompatible upgrade, the **issu load** command splits the IRF fabric into two fabrics, with the upgraded members forming a new fabric. The **issu run switchover** command reboots the members in the old IRF fabric with the upgrade images to upgrade the members. After startup, the members join the new IRF fabric as subordinate members.

At reboot, a subordinate device automatically synchronizes the master device's configuration and status data. You must wait for the synchronization to complete before using the **issu run switchover** command on the subordinate device. To identify whether the synchronization is complete, use the **display system stable state** command. The synchronization is complete if the **System State** field displays **Stable**.

When you execute the **issu run switchover** command during an ISSU to a compatible version, the system starts the automatic rollback timer. If you do not execute the **issu accept** or **issu commit** command before the timer expires, the system automatically rolls back to the original software versions.

Examples

On a multichassis IRF fabric, perform a master/subordinate switchover during an ISSU to a compatible version.

```
<Sysname> issu run switchover
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version             New Version
  Test 0001015                Test 0001016

  Slot                        Switchover Way
  1                           Active standby process switchover
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

On a multichassis IRF fabric, perform a master/subordinate switchover, and upgrade members that have not been upgraded (member 1 and member 2) during an ISSU to an incompatible version.

```
<Sysname> issu run switchover
Upgrade summary according to following table:

flash:/feature1.bin
  Running Version             New Version
  Test 0001015                Test 0001016

  Slot                        Upgrade Way
  1                           Reboot
  2                           Reboot
Upgrading software images to incompatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait...Done.
```

Table 32 Command output

Field	Description
Switchover Way	Switchover method: • **Active standby process switchover**—Switch from the active process to the standby process. • **Master subordinate switchover**—Switch from the master to a subordinate member.

For more information about the command output, see Table 29.

Related commands

issu load

reset install log-history oldest

Use **reset install log-history oldest** to clear ISSU log entries.

Syntax

reset install log-history oldest *log-number*

Views

User view

Predefined user roles

network-admin

Parameters

log-number: Specifies the number of ISSU log entries to be deleted.

Usage guidelines

This command clears the specified number of log entries, beginning with the oldest log entry.

Examples

Clear the two oldest ISSU log entries.

```
<Sysname> reset install log-history oldest 2
```

Related commands

display install log

reset install rollback oldest

Use **reset install rollback oldest** to clear ISSU rollback points.

Syntax

reset install rollback oldest *point-id*

Views

User view

Predefined user roles

network-admin

Parameters

point-id: Specifies a rollback point by its ID.

Usage guidelines

This command clears the specified rollback point and all rollback points older than the specified rollback point.

Examples

Clear rollback point 2 and all rollback points older than rollback point 2.

```
<Sysname> reset install rollback oldest 2
```

Related commands

display install rollback

Preprovisioning commands

display provision failed-config

Use **display provision failed-config** to display preprovisioned-commands application failure records.

Syntax

display provision failed-config

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

A preprovisioned command cannot be applied if it conflicts with the running configuration.

Use this command to verify the application result of preprovisioned commands except for the following commands:

- **duplex**
- **speed**
- **sflow**

To verify the application result of the listed commands, use the **display current-configuration** command. The **display provision failed-config** command might display incorrect application results for the listed commands.

Examples

Display preprovisioned-commands application failure records.

```
<Sysname> display provision failed-config
Configuration applied at: Sat Jun 14 06:06:00 2014

Slot information: slot 1
Commands that failed to be applied:
#
interface Twenty-FiveGigE1/0/1
 speed 25000
#
```

Related commands

provision

reset provision failed-config

provision

Use **provision** to enable preprovisioning.

Use **undo provision** to disable preprovisioning.

Syntax

provision [**subslot** *subslot-number*] **model** *model*

undo provision [**subslot** *subslot-number*] **model**

Default

Preprovisioning is disabled.

Views

Slot view

Predefined user roles

network-admin

Parameters

subslot *subslot-number*: Specifies a subslot by its subslot number. If you do not specify a subslot, preprovisioning is enabled on the slot. To specify a subslot, you must first enable provisioning on the slot and make sure the provisioned slot has subslots.

model *model*: Specifies the IRF member device or subcard model to be preprovisioned. To obtain available models, enter a question mark (?) for the *model* argument.

Usage guidelines

This command allows you to enable preprovisioning on offline modules, including IRF member devices and subcards.

The device automatically creates interfaces when preprovisioning is enabled for a module. The **display interface** command will not display these interfaces until the module comes online. However, you can preprovision the interfaces.

When you disable preprovisioning on a slot, the device removes all preconfigured settings for the slot, including the preconfigured settings for the subslots.

When you disable preprovisioning on a subslot, the device removes preconfigured settings for the subslot.

Only the HPE FlexFabric 5945 2-slot Switch and HPE FlexFabric 5945 4-slot Switch support specifying a subslot for the command.

Examples

Enable preprovisioning for the HPE FF 5945 4-slot Switch on a slot.

```
<Sysname> system-view
[Sysname] slot 2
[Sysname-slot-2] provision model FF 5945 4-slot
```

Related commands

display provision failed-config

reset provision failed-config

slot

reset provision failed-config

Use **reset provision failed-config** to clear preprovisioned-commands application failure records.

Syntax

reset provision failed-config

Views

User view

Predefined user roles

network-admin

Usage guidelines

Preprovisioned modules that repeatedly come online and go offline (or join and leave the IRF fabric) might leave in memory a large number of commands that were not applied. To release the occupied memory space, execute the **reset provision failed-config** command.

Examples

Clear preprovisioned-commands application failure records.

```
<Sysname> reset provision failed-config
```

Related commands

display provision failed-config

provision

slot

Use **slot** to select a slot to provision and enter slot view.

Syntax

slot *slot-number*

Views

System view

Predefined user roles

network-admin

Parameters

slot-number: Specifies an IRF member device by its member ID.

Examples

Enter the view of a slot.

```
<Sysname> system-view
[Sysname] slot 2
[Sysname-slot-2]
```

Related commands

provision

Device management commands

clock datetime

Use **clock datetime** to set the system time.

Syntax

clock datetime *time date*

Default

The system time is UTC time 00:00:00 01/01/2011.

Views

User view

Predefined user roles

network-admin

Parameters

time: Specifies a time in the *hh:mm:ss* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. The value range for *ss* is 0 to 59. The leading zero in a segment can be omitted. If the seconds segment is 0 (*hh*:*mm*:00), you can omit it. If both the minutes and seconds segments are 0 (*hh*:00:00), you can omit both of the segments. For example, to specify 08:00:00, you can enter 8.

date: Specifies a date in the *MM/DD/YYYY* or *YYYY/MM/DD* format. The value range for *YYYY* is 2000 to 2035. The value range for *MM* is 1 to 12. The value range for *DD* varies by month.

Usage guidelines

Correct system time is essential to network management and communication. You must configure the system time correctly before you run the device on the network.

For the device to use the local system time, execute the **clock protocol none** command and this command in turn. The specified system time takes effect immediately. Then, the device uses the clock signals generated by its built-in crystal oscillator to maintain the system time.

A device power cycling operation restores the local system time to the default. After the device is power cycled, you must execute this command again to set the local system time.

Examples

Set the system time to 08:08:08 01/01/2015.

```
<Sysname> clock datetime 8:8:8 1/1/2015
```

Set the system time to 08:10:00 01/01/2015.

```
<Sysname> clock datetime 8:10 2015/1/1
```

Related commands

clock protocol

clock summer-time

clock timezone

display clock

clock protocol

Use **clock protocol** to specify the system time source.

Use **undo clock protocol** to restore the default.

Syntax

clock protocol { **none** | **ntp** | **ptp** }

undo clock protocol

Default

The device obtains the UTC time from an NTP time source.

Views

System view

Predefined user roles

network-admin

Parameters

none: Uses the system time set by using the **clock datetime** command.

ptp: Uses PTP to obtain the UTC time. You must configure PTP correctly. For more information about PTP and PTP configuration, see *Network Management and Monitoring Configuration Guide*.

ntp: Uses NTP to obtain the UTC time. You must configure NTP correctly. For more information about NTP and NTP configuration, see *Network Management and Monitoring Configuration Guide*.

Usage guidelines

Correct system time is essential to network management and communication. You must configure the system time correctly before you run the device on the network.

The device can use the locally set system time, or obtain the UTC time from a time source on the network and calculate the system time.

If you configure the **clock protocol none** command, the device uses the locally set system time. The device then uses the clock signals generated by its built-in crystal oscillator to maintain the system time.

If you configure the **clock protocol** { **ntp** | **ptp** } command, the device obtains the UTC time through NTP or PTP and calculates the system time. The device then periodically synchronizes the UTC time and recalculates the system time.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Configure the device to use the local UTC time.

```
<Sysname> system-view
[Sysname] clock protocol none
```

clock summer-time

Use **clock summer-time** to set the daylight saving time.

Use **undo clock summer-time** to restore the default.

Syntax

clock summer-time *name start-time start-date end-time end-date add-time*

undo clock summer-time

Default

The daylight saving time is not set.

Views

System view

Predefined user roles

network-admin

Parameters

name: Specifies a name for the daylight saving time schedule, a case-sensitive string of 1 to 32 characters.

start-time: Specifies the start time in the *hh:mm:ss* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. The value range for *ss* is 0 to 59. The leading zero in a segment can be omitted. If the seconds segment is 0 (*hh*:*mm*:00), you can omit it. If both the minutes and seconds segments are 0 (*hh*:00:00), you can omit both of the segments. For example, to specify 08:00:00, you can enter 8.

start-date: Specifies the start date in one of the following formats:

- *MM/DD*. The value range for *MM* is 1 to 12. The value range for *DD* varies by month.
- *month week day*, where:
  - *month*—Takes **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November** or **December**.
  - *week*—Represents week of the month. It takes **first**, **second**, **third**, **fourth**, **fifth**, or **last**.
  - *day*—Takes **Sunday**, **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, or **Saturday**.

end-time: Specifies the end time in the *hh:mm:ss* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. The value range for *ss* is 0 to 59. The leading zero in a segment can be omitted. If the seconds segment is 0 (*hh*:*mm*:00), you can omit it. If both the minutes and seconds segments are 0 (*hh*:00:00), you can omit both of the segments. For example, to specify 08:00:00, you can enter 8.

end-date: Specifies the end date in one of the following formats:

- *MM/DD*. The value range for *MM* is 1 to 12. The value range for *DD* varies by month.
- *month week day*, where:
  - *month*—Takes **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November** or **December**.
  - *week*—Represents week of the month. It takes **first**, **second**, **third**, **fourth**, **fifth**, or **last**.
  - *day*—Takes **Sunday**, **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, or **Saturday**.

add-time: Specifies the time to be added to the standard time, in the *hh:mm:ss* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. The value range for *ss* is 0 to 59. The leading zero in a segment can be omitted. If the seconds segment is 0 (*hh*:*mm*:00), you can omit it. If both the minutes and seconds segments are 0 (*hh*:00:00), you can omit both of the segments. For example, to specify 08:00:00, you can enter 8.

Usage guidelines

Correct system time is essential to network management and communication. You must configure the system time correctly before you run the device on the network.

After you set the daylight saving time, the device recalculates the system time. To view the system time, use the **display clock** command.

Make sure all devices on the network are using the same daylight saving time as the local time.

Examples

Set the system time ahead 1 hour for the period between 06:00:00 on 08/01 and 06:00:00 on 09/01.

```
<Sysname> system-view
[Sysname] clock summer-time PDT 6 08/01 6 09/01 1
```

Related commands

clock datetime

clock timezone

display clock

clock timezone

Use **clock timezone** to set the time zone.

Use **undo clock timezone** to restore the default.

Syntax

clock timezone *zone-name* { **add** | **minus** } *zone-offset*

undo clock timezone

Default

The UTC time zone is used.

Views

System view

Predefined user roles

network-admin

Parameters

zone-name: Specifies a time zone by its name, a case-sensitive string of 1 to 32 characters.

add: Adds an offset to the UTC time.

minus: Decreases the UTC time by an offset.

zone-offset: Specifies an offset to the UTC time, in the *hh:mm:ss* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. The value range for *ss* is 0 to 59. The leading zero in a segment can be omitted. If the seconds segment is 0 (*hh*:*mm*:00), you can omit it. If both the minutes and seconds segments are 0 (*hh*:00:00), you can omit both of the segments. For example, to specify 08:00:00, you can enter 8.

Usage guidelines

Correct system time is essential to network management and communication. You must configure the system time correctly before you run the device on the network.

After you set the time zone, the device recalculates the system time. To view the system time, use the **display clock** command.

Make sure all devices on the network are using the same time zone as the local time.

Examples

Set the name of the time zone to **Z5**, and add 5 hours to the UTC time.

```
<Sysname> system-view
[Sysname] clock timezone Z5 add 5
```

Related commands

clock datetime

clock summer-time

display clock

command

Use **command** to assign a command to a job.

Use **undo command** to revoke a command.

Syntax

command *id command*

undo command *id*

Default

No command is assigned to a job.

Views

Job view

Predefined user roles

network-admin

Parameters

id: Specifies an ID for the command, in the range of 0 to 4294967295. A command ID uniquely identifies a command in a job. Commands in a job are executed in ascending order of their command IDs.

command: Specifies the command to be assigned to the job.

Usage guidelines

To assign a command (command A) to a job, you must first assign the job the command or commands for entering the view of command A.

If you specify the ID of an existing command for another command, the existing command is replaced.

Make sure all commands in a schedule are compliant to the command syntax. The system does not examine the syntax when you assign a command to a job.

If a command requires a yes or no answer, the system always assumes that a **Y** or **Yes** is entered. If a command requires a character string input, the system assumes that either the default character string (if any) or a null string is entered.

A job cannot contain the **telnet**, **ftp**, **ssh2**, or **monitor process** command.

Examples

Assign commands to the **backupconfig** job to back up the **startup.cfg** file to the TFTP server at 192.168.100.11.

```
<Sysname> system-view
[Sysname] scheduler job backupconfig
[Sysname-job-backupconfig] command 2 tftp 192.168.100.11 put flash:/startup.cfg
backup.cfg
```

Assign commands to the **shutdownGE** job to shut down Twenty-FiveGigE 1/0/1.

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

```
[Sysname] scheduler job shutdownGE
[Sysname-job-shutdownGE] command 1 system-view
[Sysname-job-shutdownGE] command 2 interface twenty-fivegige 1/0/1
[Sysname-job-shutdownGE] command 3 shutdown
```

Related commands

scheduler job

copyright-info enable

Use **copyright-info enable** to enable copyright statement display.

Use **undo copyright-info enable** to disable copyright statement display.

Syntax

copyright-info enable

undo copyright-info enable

Default

Copyright statement display is enabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable copyright statement display.

```
<Sysname> system-view
[Sysname] copyright-info enable
```

The device will display the following statement when a user logs in:

```
******************************************************************************
* Copyright (c) 2010-2020 Hewlett Packard Enterprise Development LP          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************
```

display alarm

Use **display alarm** to display alarm information.

Syntax

display alarm [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays alarm information for all IRF member devices.

Examples

Display alarm information.

```
<Sysname> display alarm
Slot CPU Level   Info
1    0   ERROR   faulty
```

Table 33 Command output

Field	Description
Slot	Slot that generated the alarm. If the alarm was generated by the frame, this field displays a hyphen (-).
Level	Alarm severity. Possible values include **ERROR**, **WARNING**, **NOTICE**, and **INFO**, in descending order.
Info	Detailed alarm information: • **faulty**—The slot is starting up or faulty. • **Fan** *n* **is absent**—The specified fan is absent. • **Power** *n* **is absent**—The specified power supply is absent. • **Power** *n* **is faulty**—The specified power supply is faulty. • **The temperature of sensor** *n* **exceeds the lower limit**—The temperature of the specified sensor is lower than the low-temperature threshold. • **The temperature of sensor** *n* **exceeds the upper limit**—The temperature of the specified sensor is higher than the high-temperature warning threshold.

display clock

Use **display clock** to display the system time, date, time zone, and daylight saving time.

Syntax

display clock

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the system time and date when the time zone is not specified.

```
<Sysname> display clock
10:09:00.258 UTC Fri 03/16/2015
```

The time is in the *hour*:*minute*:*second*.*milliseconds* format.

Display the system time and date when the time zone Z5 is specified.

```
<Sysname> display clock
15:10:00.152 Z5 Fri 03/16/2015
Time Zone : Z5 add 05:00:00
```

Display the system time and date when the time zone Z5 and daylight saving time PDT are specified.

```
<Sysname> display clock
15:11:00.211 Z5 Fri 03/16/2015
Time Zone : Z5 add 05:00:00
Summer Time : PDT 06:00:00 08/01 06:00:00 09/01 01:00:00
```

Related commands

clock datetime

clock timezone

clock summer-time

display copyright

Use **display copyright** to display the copyright statement.

Syntax

display copyright

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the copyright statement.

```
<Sysname> display copyright
...
```

display cpu-usage

Use **display cpu-usage** to display the current CPU usage statistics.

Syntax

display cpu-usage [**summary**] [**slot** *slot-number* [**cpu** *cpu-number* [**core** { *core-number*| **all** }]]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

summary: Displays CPU usage statistics in table form. If you do not specify this keyword, the command displays CPU usage statistics in text form.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays CPU usage statistics for all member devices.

cpu *cpu-number*: Specifies a CPU by its number.

core *core-number*: Specifies a CPU core by its number.

core all: Specifies all CPU cores.

Examples

Display the current CPU usage statistics in text form.

```
<Sysname> display cpu-usage
Slot 1 CPU 0 CPU usage:
       1% in last 5 seconds
       1% in last 1 minute
       1% in last 5 minutes
```

Display the current CPU usage statistics in table form.

```
<Sysname> display cpu-usage
Slot CPU        Last 5 sec        Last 1 min        Last 5 min
1    0          17%               29%               28%
```

Table 34 Command output

Field	Description
x% in last 5 seconds Last 5 sec	Average CPU or CPU core usage during the most recent 5-second interval.
y% in last 1 minute Last 1 min	Average CPU or CPU core usage during the most recent 1-minute interval.
z% in last 5 minutes Last 5 min	Average CPU or CPU core usage during the most recent 5-minute interval.

display cpu-usage configuration

Use **display cpu-usage configuration** to display CPU usage monitoring settings.

Syntax

display cpu-usage configuration [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the CPU usage monitoring settings for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Display the CPU usage monitoring settings.

```
<Sysname> display cpu-usage configuration
CPU usage monitor is enabled.
Current monitor interval is 60 seconds.
Current severe alarm threshold is 90%.
```

```
Current minor alarm threshold is 80%.
Current recovery-threshold is 40%.
```

Table 35 Command output

Field	Description
CPU usage monitor is *xxx*.	Whether CPU usage tracking is enabled.
Current monitor interval is *xxx*.	Sampling interval for CPU usage tracking.
Current severe alarm threshold is *xxx*.	Severe CPU usage alarm threshold.
Current minor alarm threshold is *xxx*.	Minor CPU usage alarm threshold.
Current recovery threshold is *xxx*.	CPU usage recovery threshold.

Related commands

monitor cpu-usage enable

monitor cpu-usage interval

monitor cpu-usage threshold

display cpu-usage history

Use **display cpu-usage history** to display the historical CPU usage statistics in a coordinate system.

Syntax

display cpu-usage history [**job** *job-id*] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

job *job-id*: Specifies a process by its ID. The value range for *job-id* is 1 to 2147483647. If you do not specify a process, this command displays the statistics for the entire system's CPU usage (the total CPU usage of all processes). To view the IDs and names of the running processes, use the **display process** command. For more information, see *Network Management and Monitoring Configuration Guide*.

slot *slot-number*: Specifies an IRF member device by its member ID. If you specify a process but do not specify a member device, this command displays the statistics for the process on the master device. If you do not specify any options, this command displays the statistics for all processes on all member devices.

cpu *cpu-number*: Specifies a CPU by its number. If you specify a process but do not specify a CPU, this command displays the statistics for the default CPU. If you do not specify a process or CPU, this command displays the historical statistics for all CPUs.

Usage guidelines

After CPU usage monitoring is enabled, the system regularly samples CPU usage and saves the samples to the history record buffer. This command displays the most recent 60 samples in a coordinate system as follows:

- The vertical axis represents the CPU usage. If a statistic is not a multiple of the usage step, it is rounded up or down to the closest multiple of the usage step. For example, if the CPU usage step is 5%, the statistic 53% is rounded up to 55%, and the statistic 52% is rounded down to 50%.
- The horizontal axis represents the time.
- Pound signs (#) indicate the CPU usage. The value on the vertical axis for the topmost pound sign at a specific time represents the CPU usage at that time.

Examples

Display the historical CPU usage statistics.

```
<Sysname> display cpu-usage history
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|
 20%|
 15%|              #
 10%|             ###  #
  5%|            ########
    ------------------------------------------------------------
              10        20        30        40        50        60  (minutes)
                     cpu-usage (Slot 1 CPU 0) last 60 minutes (SYSTEM)
```

The output shows the following items:

- Process name. The name **SYSTEM** represents the entire system.
- CPU that is holding the process: CPU 0 in slot 1.
- Historical CPU usage statistics for the entire system during the last 60 minutes.
  - **12 minutes ago**—Approximately 5%.
  - **13 minutes ago**—Approximately 10%.
  - **14 minutes ago**—Approximately 15%.
  - **15 minutes ago**—Approximately 10%.
  - **16 and 17 minutes ago**—Approximately 5%.
  - **18 minutes ago**—Approximately 10%.
  - **19 minutes ago**—Approximately 5%.
  - **Other time**—2% or lower.

Related commands

monitor cpu-usage enable

monitor cpu-usage interval

display device

Use **display device** to display device information.

Syntax

display device [**flash** | **usb**] [**slot** *slot-number* [**subslot** *subslot-number*] | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

flash: Displays flash memory information.

usb: Displays USB interface information.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

subslot *subslot-number*: Specifies a subcard by its subslot number. If you do not specify a subcard, this command does not display information about any subcards.

verbose: Displays detailed information. If you do not specify this keyword, this command displays brief information.

Usage guidelines

If you do not specify the **flash** and **usb** keywords, this command displays information about member devices.

Examples

Display device information.

```
<Sysname> display device
Slot 1
Slot Type             State    Subslot  Soft Ver            Patch Ver
1    FF 5945 48SFP28  Master   0        6607                None
     8QSFP28 Switch
```

Table 36 Command output

Field	Description
Type	Device type.
State	Role of the device in an IRF fabric: • **Master**—The device is the master. • **Standby**—The device is a subordinate member.
Soft Ver	Software version of the device.
Patch Ver	Most recently released patch image version that is running on the device. If no patch

Field	Description
	image is installed, this field displays **None**. If both incremental and non-incremental patch images are running on the device, this field displays the most recently released incremental patch image version. For more information about patch image types, see "Upgrading software."

display device manuinfo

Use **display device manuinfo** to display electronic label information for the device.

Syntax

display device manuinfo [**slot** *slot-number* [**subslot** *subslot-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays electronic label information for all member devices.

subslot *subslot-number*: Specifies a subcard by its subslot number. If you do not specify a subcard, this command does not display information about any subcards.

Usage guidelines

Silver fan trays of the following models support this command but black fan trays of the same models do not:

- LSWM1FANSA.
- LSWM1FANSAB.
- LSWM1BFANSC.
- LSWM1BFANSCB.

An electronic label contains the permanent configuration information, including the hardware serial number, manufacturing date, MAC address, and vendor name. The data is written to the storage component during hardware debugging or testing. This command displays only part of the electronic label information.

Examples

Display electronic label information for the device.

```
<Sysname> display device manuinfo
...
```

display device manuinfo fan

Use **display device manuinfo fan** to display electronic label information for a fan tray.

Syntax

display device manuinfo slot *slot-number* **fan** *fan-id*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

fan-id: Specifies a fan tray by its ID.

Silver fan trays of the following models support this command but black fan trays of the same models do not:

- LSWM1FANSA.
- LSWM1FANSAB.
- LSWM1BFANSC.
- LSWM1BFANSCB.

Examples

Display electronic label information for a fan tray.

```
<Sysname> display device manuinfo slot 1 fan 1
...
```

display device manuinfo power

Use **display device manuinfo power** to display electronic label information for a power supply.

Syntax

display device manuinfo slot *slot-number* **power** *power-id*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

power-id: Specifies a power supply by its ID.

Examples

Display electronic label information for a power supply.

```
<Sysname> display device manuinfo slot 1 power 1
...
```

display diagnostic-information

Use **display diagnostic-information** to display or save operating information for features and hardware modules.

Syntax

display diagnostic-information [**hardware** | **infrastructure** | **l2** | **l3** | **service**] [**key-info**] [*filename*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

hardware: Specifies hardware-related operating information.

infrastructure: Specifies operating information for the fundamental features.

l2: Specifies operating information for the Layer 2 features.

l3: Specifies operating information for the Layer 3 features.

service: Specifies operating information for Layer 4 and upper-layer features.

key-info: Displays or saves only critical operating information. The device might have a large amount of operating information if an exception occurs or after the device runs for a long period of time. Specifying this keyword reduces the command execution time and helps you focus on critical operating information. If you do not specify this keyword, the command displays or saves both critical and non-critical operating information.

filename: Saves the information to a file. The *filename* argument must use the **.tar.gz** extension. If you do not specify this argument, the command prompts you to choose whether to save the information to a file or display the information.

Usage guidelines

You can use one of the following methods to collect operating statistics for diagnostics and troubleshooting:

- Use separate **display** commands to collect operating information feature by feature or module by module.
- Use the **display diagnostic-information** command to collect operating information for multiple or all features and hardware modules.

To save storage space, this command automatically compresses the information before saving the information to a file. To view the file content:

1. Use the **tar extract** command to extract the file.
2. Use the **gunzip** command to decompress the extracted file.
3. Use the **more** command to view the content of the decompressed file.

If you abort the **display diagnostic-information** command, the **gunzip** command might not be able to decompress the extracted file. To decompress the extracted file, export the extracted file to a PC that is running Linux, and use the **gunzip -c** command.

If you do not specify a file name for the command, the system prompts you to choose whether to display or save the information. If you choose to save the information, the system automatically assigns a file name and displays the file name in brackets. For file name uniqueness, the file name includes the device name and the current system time. If the device name contains any of the following special characters, the system uses an underscore (_) to replace each special character: forward slashes (/), backward slashes (\), colons (:), asterisks (*), question marks (?), less than signs (<), greater than signs (>), pipeline signs (|), and quotation marks ("). For example, device name **A/B** will change to **A_B** in the file name, as in **flash:/diag_A_B_20160101-000438.tar.gz**.

If you do not specify any feature parameters, this command displays or saves the operating information for all features and modules.

This command does not support the |, **>**, and **>>** options.

While the device is executing this command, do not execute any other commands. Executing other commands might affect the collected operating information.

Examples

Display the operating information for all features and modules.

```
<Sysname> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:n
================================================
  ===============display clock===============
14:03:55 UTC Thu 01/05/2015
================================================
  ===============display version===============
...
```

Save the operating information to the default file.

```
<Sysname> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)? [Y/N]:y
Please input the file name(*.tar.gz)[flash:/diag_Sysname_20160101-024601.tar.gz]:
Diagnostic information is outputting to flash:/diag_Sysname_20160101-024601.tar.gz.
Please wait...
Save successfully.
```

Press **Enter** when the system prompts you to enter the file name.

Save the operating information for all features and modules to file **test.tar.gz**.

```
<Sysname> display diagnostic-information test.tar.gz
Diagnostic information is outputting to flash:/test.tar.gz.
Please wait...
Save successfully.
```

Related commands

gunzip

more

tar extract

display environment

Use **display environment** to display temperature information.

Syntax

display environment [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays temperature information for all member devices.

Examples

Display information about all temperature sensors on the device.

```
<Sysname> display environment
 System temperature information (degree centigrade):
 ---------------------------------------------------------------------------
Slot  Sensor    Temperature  Lower  Warning  Alarm  Shutdown
 1     hotspot 1 31           0      55       60     NA
 1     hotspot 2 58           0      80       85     NA
 1     hotspot 3 51           0      85       97     NA
 1     hotspot 4 69           0      88       102    107
 1     hotspot 5 63           0      125      130    140
 1     hotspot 6 30           NA     NA       NA     NA
```

Table 37 Command output

Field	Description
System Temperature information (degree centigrade)	Temperature information (°C).
sensor	Temperature sensor: **hotspot**—Hotspot sensor.
Slot	Sensor position.
Temperature	Current temperature.
Lower	Lower temperature limit. If the device does not support this field, this field displays **NA**.
Warning	Warning temperature threshold. If the device does not support this field, this field displays **NA**.
Alarm	Alarming temperature threshold. If the device does not support this field, this field displays **NA**.
Shutdown	Shutdown temperature threshold. When the sensor temperature reaches the limit, the system shuts down automatically. If the device does not support this field, this field displays **NA**.

display fan

Use **display fan** to display fan tray operating status information.

Syntax

display fan [**slot** *slot-number* [*fan-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays fan tray operating status information for all member devices.

fan-id: Specifies a fan tray by its ID. If you do not specify a fan tray, this command displays operating status information for all fan trays at the specified position.

Examples

Display the operating states of all fan trays.

```
<Sysname> display fan
 Slot 1:
 Fan 1:
 State    : Normal
 Airflow Direction: Port-to-power
 Prefer Airflow Direction: Port-to-power
```

Table 38 Command output

Field	Description
Slot 1	Number of the member device.
Fan 1	Fan tray number.
State	Fan status: • **Absent**—The slot is not installed with a fan tray. • **Fault**—The fan is faulty. • **Normal**—The fan is operating correctly. • **FanDirectionFault**—The actual airflow direction is not the preferred direction.
Airflow Direction	Actual airflow direction: • **Port-to-power**—From the port side to the power supply side. • **Power-to-port**—From the power supply side to the port side.
Prefer Airflow Direction	Preferred airflow direction: • **Port-to-power**—From the port side to the power supply side. • **Power-to-port**—From the power supply side to the port side.

display hardware-failure-detection

Use **display hardware-failure-detection** to display the hardware failure detection settings and the latest 10 fix records for each card.

Syntax

display hardware-failure-detection

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

In standalone mode, the fix records are stored on the active MPU. You can use the **display hardware-failure-detection** command to display the records for a card even if the card is removed or replaced. The fix records are lost only when you remove or power cycle the active MPU.

In IRF mode, the fix records are stored on the local active MPU. You can use the **display hardware-failure-detection** command to display the records for a card even if the card is removed or replaced. The fix records are lost only when you remove or power cycle the local active MPU.

Examples

Display hardware failure detection settings and fix records.

```
<Sysname> display hardware-failure-detection
Current level:
    chip       : isolate
    board      : isolate
    forwarding : warning
Recent record:
-------------------------Slot  0 executed records:----------------------------
                There is no record.
-------------------------Slot  0 trapped records:-----------------------------
                There is no record.
```

Table 39 Command output

Field	Description
Current level	Fix actions specified for hardware failures.
chip	Fix action for hardware failures on components of cards.
board	Fix action for hardware failures on control paths.
forwarding	Fix action for hardware failures on the forwarding plane.
Recent record	Recent failure fix records.
xxx executed records	Fix records stored on an MPU.
xxx trapped records	Trap records stored on an MPU.

display hardware-resource switch-mode

Use **display hardware-resource switch-mode** to display hardware resource operating mode information for the MAC address table, ARP and ND tables, and routing tables.

Syntax

display hardware-resource [**switch-mode**]

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

If you do not specify the **switch-mode** keyword, the command displays hardware resource operating mode information for all hardware resources.

If the **hardware-resource routing-mode ipv6-128** command is not configured and the routing mode is used, the capacity of the routing table is 324K.

If the **hardware-resource routing-mode ipv6-128** command is configured and the routing mode is used, the capacity of the routing table is 160K.

Examples

Display the hardware resource operating mode information for the MAC address table, ARP and ND tables, and routing tables.

```
<HPE>display hardware-resource switch-mode
Switch-mode resource(switch-mode), all supported modes:
  NORMAL            MAC table:96K,  ARP and ND tables:80K,  routing table:160K
  MAC               MAC table:288K, ARP and ND tables:16K,  routing table:32K
  ROUTING           MAC table:32K,  ARP and ND tables:16K,  routing table:324K
  ARP               MAC table:32K,  ARP and ND tables:272K, routing table:32K
  DUAL-STACK        MAC table:32K,  ARP and ND tables:16K,  routing:v4-87k,v6-86
k
  EM                MAC table:32K,  ARP and ND tables:16K,  routing table:32K

  ----------------------------------------------
  Default         Current         Next
  NORMAL          ARP             ARP
```

NOTE:

The device does not support the EM mode.

Related commands

hardware-resource switch-mode

display memory

Use **display memory** to display memory usage information.

Syntax

display memory [**summary**] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

summary: Displays brief information about memory usage. If you do not specify this keyword, the command displays detailed information about memory usage.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays memory usage for all member devices.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Display detailed memory usage information.

```
<Sysname> display memory
Memory statistics are measured in KB:
Slot 1:
             Total      Used      Free    Shared   Buffers    Cached   FreeRatio
Mem:       8090436   1633592   6456844         0      3672    187888       79.8%
-/+ Buffers/Cache:   1442032   6648404
Swap:            0         0         0
```

Display brief memory usage information.

```
<Sysname> display memory summary
Memory statistics are measured in KB:
Slot CPU        Total      Used      Free  Buffers    Caches FreeRatio
   1   0      8090436   1648708   6441728     3672    187908     79.6%
```

Table 40 Command output

Field	Description
Mem	Memory usage information.
Total	Total size of the physical memory space that can be allocated. The memory space is virtually divided into two parts. Part 1 is solely used for kernel code, kernel management, and ISSU functions. Part 2 can be allocated and used for such tasks as running service modules and storing files. The size of part 2 equals the total size minus the size of part 1.
Used	Used physical memory.
Free	Free physical memory.
Shared	Physical memory shared by processes. If this field is not supported, two hyphens (--) are displayed.
Buffers	Physical memory used for buffers. If this field is not supported, two hyphens (--) are displayed.
Cached Caches	Physical memory used for caches. If this field is not supported, two hyphens (--) are displayed.
FreeRatio	Free memory ratio.
-/+ Buffers/Cache	-/+ Buffers/Cache:used = Mem:Used – Mem:Buffers – Mem:Cached, which indicates the physical memory used by applications. -/+ Buffers/Cache:free = Mem:Free + Mem:Buffers + Mem:Cached, which indicates the physical memory available for applications.
Swap	Memory space for swapping.

display memory-threshold

Use **display memory-threshold** to display memory alarm thresholds and statistics.

Syntax

display memory-threshold [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the memory usage thresholds and statistics for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

For more information about memory usage notifications, see log information containing **MEM_EXCEED_THRESHOLD** or **MEM_BELOW_THRESHOLD**.

Examples

Display memory alarm thresholds and statistics.

```
<Sysname> display memory-threshold
Memory usage threshold: 100%
Free-memory thresholds:
    Minor: 96M
    Severe: 64M
    Critical: 48M
    Normal: 128M
    Early-warning: 256M
    Secure: 304M

Current free-memory state: Normal (secure)
Free-memory event statistics:
 [Back to secure state]
    First notification: 0.0
    Latest notification: 0.0
    Total number of notifications sent: 0
 [Entered early-warning state]
    First notification at: 0.0
    Latest notification at: 0.0
    Total number of notifications sent: 0
 [Back to normal state]
    First notification: 0.0
    Latest notification: 0.0
    Total number of notifications sent: 0
 [Entered minor alarm state]
    First notification at: 0.0
    Latest notification at: 0.0
    Total number of notifications sent: 0
 [Back to minor alarm state]
    First notification at: 0.0
    Latest notification at: 0.0
    Total number of notifications sent: 0
```

```
[Entered severe alarm state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
[Back to severe alarm state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
[Entered critical alarm state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
```

display power

Use **display power** to display power supply information.

Syntax

display power [**slot** *slot-number* [*power-id* | **verbose**]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays power supply information for all member devices.

power-id: Specifies a power supply by its ID. If you do not specify a power supply, this command displays information about all power supplies at the specified position.

verbose: Displays detailed information. If you do not specify this keyword, the command displays brief information.

Examples

Display brief power supply information.

```
<Sysname> display power
Slot 1:
 Input Power: 117(W)
 PowerID State         Mode   Current(A)  Voltage(V)  Power(W)
 1       Absent        --        --          --          --
 2       Normal        AC        --          --          --
```

Table 41 Command output

Field	Description
Input Power	Rated power.
PowerID	Power supply ID.
State	Power supply status.

Field	Description
	• **Absent**—The slot is not installed with a power supply. • **Fault**—The power supply is faulty. • **Normal**—The power supply is operating correctly.
Mode	Mode of the power supply: • **AC**—AC power supply. • **DC**—DC power supply.
Current(A)	Output current of the power supply, in amperes. If this field is not supported, two hyphens (--) are displayed.
Voltage(V)	Output voltage of the power supply, in volts. If this field is not supported, two hyphens (--) are displayed.
Power(W)	Output power of the power supply, in watts. If this field is not supported, two hyphens (--) are displayed.

Display detailed power supply information.

```
<Sysname> display power slot 1 verbose
Slot 1:
 Input Power: 117(W)
 PowerID State         Mode   Current(A)  Voltage(V)  Power(W)
 1       Absent        --        --          --          --
 2       Normal        AC        --          --          --
```

Table 42 Command output

Field	Description
Input Power	Rated power of the device.
PowerID	Power supply ID.
State	Power supply status: • **Absent**—The slot is not installed with a power supply. • **Faulty**—The power supply is faulty. • **Normal**—The power supply is operating correctly.
Mode	Power supply type: • **AC**—AC power supply. • **DC**—DC power supply.
Current(A)	Input current of the card, in amperes. If this field is not supported, two hyphens (--) are displayed.
Power(W)	Rated power of the card, in watts. If this field is not supported, two hyphens (--) are displayed.

display resource-monitor

Use **display resource-monitor** to display resource monitoring information.

Syntax

display resource-monitor [**resource** *resource-name*] [**slot** *slot-number* [**cpu** *cpu-number*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

resource *resource-name*: Specifies a resource type by its name. Table 52 shows the resource types that can be monitored.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays resource monitoring information for all member devices.

cpu *cpu-number*: Specifies a CPU by its number.

Examples

Display ARP resource monitoring information.

```
<Sysname> display resource-monitor resource arp
Minor alarms resending: Enabled

Slot 1:
Resource                        Minor Severe Free/Total
                                (%)   (%)    (absolute)
arp                             50    20     90095/90098
```

Table 43 Command output

Field	Description
Minor alarms resending	Status of the minor resource depletion alarm resending feature, **Enabled** or **Disabled.**
Resource	Monitored resource type.
Minor (%)	Minor resource depletion threshold, in percentage.
Severe (%)	Severe resource depletion threshold, in percentage.
Free/Total (absolute)	Numbers of available resources and total resources, in absolute values.

Related commands

resource-monitor minor resend enable

resource-monitor resource

display scheduler job

Use **display scheduler job** to display job configuration information.

Syntax

display scheduler job [*job-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

job-name: Specifies a job by its name, a case-sensitive string of 1 to 47 characters. If you do not specify a job, this command displays configuration information for all jobs.

Examples

Display configuration information for all jobs.

```
<Sysname> display scheduler job
Job name: saveconfig
 copy startup.cfg backup.cfg

Job name: backupconfig

Job name: creat-VLAN100
 system-view
 vlan 100
```

// The output shows that the device has three jobs: the first has one command, the second does not have any commands, and the third has two commands. Jobs are separated by blank lines.

display scheduler logfile

Use **display scheduler logfile** to display job execution log information.

Syntax

display scheduler logfile

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display job execution log information.

```
<Sysname> display scheduler logfile
Logfile Size: 1902 Bytes.

Job name        : shutdown
Schedule name   : shutdown
Execution time  : Tue Dec 27 10:44:42 2015
Completion time : Tue Dec 27 10:44:47 2015
--------------------------------- Job output ----------------------------------
<Sysname>system-view
System View: return to User View with Ctrl+Z.
```

```
[Sysname]interface rang twenty-fivegige 1/0/1 to twenty-fivegige 1/0/3
[Sysname-if-range]shutdown
```

Table 44 Command output

Field	Description
Logfile Size	Size of the log file, in bytes.
Schedule name	Schedule to which the job belongs.
Execution time	Time when the job was started.
Completion time	Time when the job was completed. If the job has never been executed or the job does not have any commands, this field is blank.
Job output	Commands in the job and their output.

Related commands

reset scheduler logfile

display scheduler reboot

Use **display scheduler reboot** to display the automatic reboot schedule.

Syntax

display scheduler reboot

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the automatic reboot schedule.

```
<Sysname> display scheduler reboot
System will reboot at 16:32:00 05/23/2015 (in 1 hours and 39 minutes).
```

Related commands

scheduler reboot at

scheduler reboot delay

display scheduler schedule

Use **display scheduler schedule** to display schedule information.

Syntax

display scheduler schedule [*schedule-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

schedule-name: Specifies a schedule by its name, a case-sensitive string of 1 to 47 characters. If you do not specify a schedule, this command displays information about all schedules.

Examples

Display information about all schedules.

```
<Sysname> display scheduler schedule
Schedule name        : shutdown
Schedule type        : Run once after 0 hours 2 minutes
Start time           : Tue Dec 27 10:44:42 2015
Last execution time  : Tue Dec 27 10:44:42 2015
Last completion time : Tue Dec 27 10:44:47 2015
Execution counts     : 1
------------------------------------------------------------------------
Job name                                          Last execution status
shutdown                                          Successful
```

Table 45 Command output

Field	Description
Schedule type	Execution time setting of the schedule. If no execution time is specified, this field is not displayed.
Start time	Time to execute the schedule for the first time. If no execution time is specified, this field is not displayed.
Last execution time	Last time when the schedule was executed. If no execution time is specified, this field is not displayed. If the schedule has never been executed, "Yet to be executed" is displayed for this field.
Last completion time	Last time when the schedule was completed. If no execution time is specified, this field is not displayed.
Execution counts	Number of times the schedule has been executed. If the schedule has never been executed, this field is not displayed.
Job name	Name of a job under the schedule.
Last execution status	Result of the most recent execution: • **Successful**. • **Failed**. • **Waiting**—The device is executing the schedule and the job is waiting to be executed. • **In process**—The job is being executed. • **-NA-**—The execution time has not arrived yet. To view information about whether the commands in the job has been executed and the execution results, execute the **display scheduler logfile** command.

display system stable state

Use **display system stable state** to display system stability and status information.

Syntax

display system stable state [**summary**]

Views

Any view

Predefined user roles

network-admin

network-operator

summary: Displays brief information about system status, redundancy status, and NSR status. If you do not specify this keyword, the command displays detailed information about system status, redundancy status, and CPU role and status.

Usage guidelines

Before performing an ISSU or a switchover, execute this command multiple times to identify whether the system is operating stably. If the value of the **System State** field is not **Stable**, you cannot perform an ISSU. If the value of the **Redundancy Stable** field is not **Stable**, you cannot perform a switchover.

The device startup process takes some time. If the values of the status fields do not change to **Stable**, execute this command multiple times to identify the devices that are not in **Stable** state. You can also use other commands to identify the faulty components. For example:

- Use the **display device** command to identify the device operating status.
- Use the **display ha service-group** command to display the status of HA service groups and identify the groups in batch backup state.
- Use the **display system internal process state** command in probe view to display service operating status.

Examples

Display brief system stability and status information.

```
<Sysname> display system stable state summary
System state      : Stable
Redundancy state  : No redundance
NSR     state     : No standby
```

Display system stability and status information.

```
<Sysname> display system stable state
System state    : Stable
Redundancy state: No redundance
  Slot   CPU   Role      State
  1      0     Active    Stable
```

Table 46 Command output

Field	Description
System state	Operating status of all member devices: • **Stable**—All member devices are operating stably. • **Not ready**—The system is not operating stably. You cannot perform an ISSU when the system is in this state.
Redundancy state	System redundancy status: • **Stable**—Member devices are operating stably. You can perform a switchover. • **No redundance**—The system has only one member device. You cannot perform a switchover. • **Not ready**—The system is not operating stably. You cannot perform a switchover.
NSR state	NSR status of all member devices:

Field	Description
	• **Stable**—NSR is operating correctly on all member devices where it is enabled. • **Not ready**—NSR is not operating correctly on all member devices where it is enabled. You cannot perform a process or member switchover or an ISSU. • **No standby**—The IRF fabric has only one member device. • **Not configured**—NSR is not enabled.
Role	Role of the member device in the system: • **Active**—The member device is the master. • **Standby**—The member device is a subordinate member.
State	Member device status: • **Stable**—The member device is operating stably. • **Board inserted**—The member device has just been installed. • **Kernel initiating**—Member device kernel is being initialized. • **Service starting**—Services are starting on the member device. • **Service stopping**—Services are stopping on the member device. • **HA Batch backup**—An HA batch backup is going on. • **Interface data batch backup**—An interface data batch backup is in progress.
*	The object is not operating stably.

Related commands

`display device`

`display ha service-group` (*High Availability Command Reference*)

display system-working-mode

Use **`display system-working-mode`** to display system working mode information.

Syntax

`display system-working-mode`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display system working mode information.

```
<Sysname> display system-working-mode
The current system working mode is standard.
The system working mode for next startup is standard.
```

display transceiver alarm

Use **`display transceiver alarm`** to display transceiver alarms.

Syntax

`display transceiver alarm interface` [*`interface-type interface-number`*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface [*interface-type interface-number*]: Specifies an interface by its type and number. If no interface is specified, this command displays the alarms present on every transceiver module.

Usage guidelines

Table 47 shows the common transceiver alarm components. If no error occurs, "None" is displayed.

Table 47 Common transceiver alarm components

Field	Description
APD	Avalanche photo diode
PCS	Physical coding sublayer
PHY XS	PHY extended sublayer
PMA/PMD	Physical medium attachment/physical medium dependent
power	Optical power
REFCLK	Reference clock
RX	Receive
TEC	Thermoelectric cooler
Temp	Temperature
TX	Transmit
WIS	WAN interface sublayer

Examples

Display the alarms present on the transceiver module in interface Twenty-FiveGigE 1/0/1.

```
<Sysname> display transceiver alarm interface twenty-fivegige 1/0/1
Twenty-FiveGigE1/0/1 transceiver current alarm information:
  RX signal loss
  RX power low
```

Table 48 Command output

Field	Description
transceiver current alarm information	Alarms present on the transceiver module.
RX signal loss	Inbound signal loss occurred.
RX power low	Received power is low.

display transceiver diagnosis

Use **display transceiver diagnosis** to display the current values of the digital diagnosis parameters on transceiver modules.

Syntax

display transceiver diagnosis interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface [*interface-type interface-number*]: Specifies an interface by its type and number. If no interface is specified, this command displays the current values of the digital diagnosis parameters on every transceiver module.

Usage guidelines

After you install a CFP2-200G-DCO-Tunable transceiver module in an interface, the system creates two 100G Ethernet interfaces, such as HundredGigE 1/0/1:1 and HundredGigE 1/0/1:2. Specifying any of the interfaces for this command displays the same information.

Examples

Display the current values of the digital diagnosis parameters on the transceiver module in interface Twenty-FiveGigE 1/0/1.

```
<Sysname> display transceiver diagnosis interface twenty-fivegige 1/0/1
Twenty-FiveGigE1/0/1 transceiver diagnostic information:
  Current diagnostic parameters:
    Temp(°C)  Voltage(V)  Bias(mA)  RX power(dBm)  TX power(dBm)
    36        3.31        6.13      -35.64          -5.19
  Alarm thresholds:
            Temp(°C)   Voltage(V)  Bias(mA)  RX power(dBM)  TX power(dBM)
    High    50         3.55        1.44      -10.00         5.00
    Low     30         3.01        1.01      -30.00         0.00
```

Table 49 Command output

Field	Description
transceiver diagnostic information	Digital diagnosis information for the transceiver module in the interface.
Temp.(°C)	Temperature in °C, accurate to 1°C.
Voltage(V)	Voltage in V, accurate to 0.01 V.
Bias(mA)	Bias current in mA, accurate to 0.01 mA.
RX power(dBm)	Receive power in dBm, accurate to 0.01 dBm.
TX power(dBm)	Transmit power in dBm, accurate to 0.01 dBm.

display transceiver interface

Use **display transceiver interface** to display the key parameters of transceiver modules.

Syntax

display transceiver interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command displays the key parameters of every transceiver module.

Examples

Display the key parameters of the transceiver module in interface Twenty-FiveGigE 1/0/1.

```
<Sysname> display transceiver interface twenty-fivegige 1/0/1
...
```

display transceiver manuinfo

Use **display transceiver manuinfo** to display electronic label information for transceiver modules.

Syntax

display transceiver manuinfo interface [*interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface [*interface-type interface-number*]: Specifies an interface by its type and number. If no interface is specified, this command displays electronic label information for all transceiver modules.

Examples

Display electronic label information for the transceiver module in interface Twenty-FiveGigE1/0/1.

```
<Sysname> display transceiver manuinfo interface twenty-fivegige 1/0/1
...
```

display version

Use **display version** to display system version information.

Syntax

display version

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display system version information.

```
<Sysname> display version
HPE Comware Software, Version 7.1.070, Release 6607
Copyright (c) 2010-2020 Hewlett Packard Enterprise Development LP
HPE FF 5945 48SFP28 8QSFP28 Switch uptime is 0 weeks, 0 days, 3 hours, 3 minutes
Last reboot reason : User reboot

Boot image: flash:/5945-cmw710-boot-r6607.bin
Boot image version: 7.1.070, Release 6607
  Compiled Mar 15 2018 11:00:00
System image: flash:/5945-cmw710-system-r6607.bin
System image version: 7.1.070, Release 6607
  Compiled Mar 15 2018 11:00:00
...
```

Table 50 Command output

Field	Description
Last reboot reason	Reason for the last reboot: • **User reboot**—The reboot was manually initiated from a user interface, such as the CLI or SNMP. • **Cold reboot**—The reboot was caused by a power cycle. • **Kernel abnormality reboot**—The reboot was caused by kernel exceptions. • **DeadLoop reboot**—The reboot was caused by a kernel thread dead loop. • **DEV HandShake reboot**—The reboot was caused by a device management handshake failure. • **SlaveSwitch reboot**—The reboot was caused by a master/subordinate switchover. • **IRF Merge reboot**—The reboot was caused by an IRF merge. • **Auto Update reboot**—The reboot was caused by an automatic software upgrade. • **Memory exhaust reboot**—The reboot was caused by a memory-exhausted event.

display version-update-record

Use **display version-update-record** to display startup software image upgrade records.

Syntax

display version-update-record

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

The device records its current startup software version information whenever it starts up, and records all software version update information. Such information can survive reboots.

Examples

Display the startup software image upgrade records.

```
<Sysname> display version-update-record
Record 1  (updated on Apr 18 2015 at 06:23:54):
 *Name        : simware-cmw710-boot.bin
  Version     : 7.1.070 Test 0001
  Compile time: Mar 25 2015 15:52:43
 *Name        : simware-cmw710-system.bin
  Version     : 7.1.070 Test 0001
  Compile time: Mar 25 2015 15:52:43
```

Table 51 Command output

Field	Description
Record *n*	Number of the startup software image upgrade record. Record 1 is the most recent record.
Name	Software image file name.
*	The software image version changed during the upgrade.

Related commands

reset version-update-record

download manuinfo fan

Use **download manuinfo fan** to set the serial number for a fan tray.

Syntax

download manuinfo slot *slot-number* **fan** *fan-id* **serial-num** *serial-number*

Default

The fan trays do not have serial numbers.

Views

System view

Predefined user roles

network-admin

parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

fan *fan-id*: Specifies a fan tray by its ID.

serial-num *serial-number*: Specifies the serial number of the fan tray.

Usage guidelines

To set the serial number for a fan tray, read the label on the fan tray for its serial number and enter the correct serial number for the command.

The **display device manuinfo** and **display device manuinfo fan** commands display **NONE** for the serial number and manufacturing date fields of a fan tray in the following situations:

- The fan tray does not have a serial number configured.
- The configured serial number is incorrect.

Examples

Set the serial number for a fan tray.

```
<Sysname> system-view
[Sysname] download manuinfo slot 1 fan 2 serial-num 21020000000000000000
```

fan prefer-direction

Use **fan prefer-direction** to specify the preferred airflow direction for the device.

Use **undo fan prefer-direction** to restore the default.

Syntax

fan prefer-direction slot *slot-number* { **port-to-power** | **power-to-port** }

undo fan prefer-direction slot *slot-number*

Default

The preferred airflow direction is from the port side to the power supply side..

Views

System view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

port-to-power: Specifies the airflow direction from the port side to the power supply side.

power-to-port: Specifies the airflow direction from the power supply side to the port side.

Examples

Set the preferred airflow direction to **port-to-power** for member device 1.

```
<Sysname> system-view
[Sysname] fan prefer-direction slot 1 port-to-power
```

Related commands

display fan

hardware-failure-detection

Use **hardware-failure-detection** to specify the action to be taken in response to hardware failures.

Use **undo hardware-failure-detection** to restore the default.

Syntax

hardware-failure-detection { **board** | **chip** | **forwarding** } { **isolate** | **off** | **reset** | **warning** }

undo hardware-failure-detection { **board** | **chip** | **forwarding** }

Default

The system takes the action of **warning** in response to hardware failures on chips, cards, and the forwarding plane.

Views

System view

Predefined user roles

network-admin

Parameters

board: Specifies failures on control paths and cards.

chip: Specifies failures on components of cards such as the chips, capacitances, resistances.

forwarding: Specifies failures on the forwarding plane (including services and other relevant items).

isolate: Takes one or more of the following actions:

- Shuts down the relevant ports.
- Prohibits loading software for the relevant cards.
- Isolates the relevant cards.
- Powers off the relevant cards to reduce impact from the failures.

off: Takes no action.

reset: Restarts the relevant components or cards to recover from failures.

warning: Sends traps to notify you of the failures.

Usage guidelines

The device automatically detects hardware failures on components, cards, and the forwarding plane. You can specify the actions to be taken in response to detected failures.

Examples

Configure the device to send traps in response to failures on components.

```
<Sysname> system-view
[Sysname] hardware-failure-detection chip warning
```

hardware-resource switch-mode

Use **hardware-resource switch-mode** to set the hardware resource operating mode for the MAC address table, ARP and ND tables, and routing tables.

Use **undo hardware-resource switch-mode** to restore the default.

Syntax

hardware-resource switch-mode { **ARP** | **DUAL-STACK** | **MAC** | **NORMAL** | **ROUTING** }

undo hardware-resource switch-mode

Default

The hardware resource operating mode is **NORMAL** for the MAC address table, ARP and ND tables, and routing tables.

Views

System view

Predefined user roles

network-admin

Parameters

ARP: Specifies the ARP mode.

DUAL-STACK: Specifies the dual-stack mode.

MAC: Specifies the MAC mode.

NORMAL: Specifies the normal mode.

ROUTING: Specifies the routing mode.

Usage guidelines

The device supports multiple hardware resource operating modes for the MAC address table, ARP/ND table, and routing tables. The capacities of the tables vary by hardware resource operating mode. For more information, see device management in *Fundamentals Configuration Guide*.

This setting takes effect after you save the running configuration and reboot the device. Before rebooting the device, make sure you know the possible impact on the network.

Examples

Set the hardware resource operating mode to routing.

```
<Sysname> system-view
[Sysname] hardware-resource switch-mode routing
Do you want to change the specified hardware resource working mode? [Y/N]:y
The hardware resource working mode is changed, please save the configuration and
 reboot the system to make it effective.
```

Related commands

display hardware-resource switch-mode

header

Use **header** to configure a banner.

Use **undo header** to delete a banner.

Syntax

header { **legal** | **login** | **motd** | **shell** } *text*

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

Default

The device does not have banners.

Views

System view

Predefined user roles

network-admin

Parameters

legal: Configures the banner to be displayed before a user inputs the username and password to access the CLI.

login: Configures the banner to be displayed before password or scheme authentication is performed for a login user.

motd: Configures the greeting banner to be displayed before the legal banner appears.

shell: Configures the banner to be displayed before a user accesses user view.

text: Specifies the banner message. You can enter the banner message on the same line as the keywords or on different lines. For more information, see *Fundamentals Configuration Guide*.

Examples

Configure the legal banner.

```
<Sysname> system-view
[Sysname] header legal
Please input banner content, and quit with the character '%'.
Welcome to use the legal banner%
```

job

Use **job** to assign a job to a schedule.

Use **undo job** to revoke a job.

Syntax

job *job-name*

undo job *job-name*

Default

No job is assigned to a schedule.

Views

Schedule view

Predefined user roles

network-admin

Parameters

job-name: Specifies the job name, a case-sensitive string of 1 to 47 characters.

Usage guidelines

You can assign multiple jobs to a schedule. The jobs in a schedule are executed concurrently.

The jobs to be assigned to a schedule must already exist. To create a job, use the **scheduler job** command.

Examples

Assign job **save-job** to schedule **saveconfig**.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] job save-job
```

Related commands

scheduler job

scheduler schedule

locator blink

Use **locator blink** *blink-time* to start LED flashing to locate devices.

Use **locator blink stop** to stop LED flashing.

Syntax

locator [**slot** *slot-number*] **blink** *blink-time*

locator [**slot** *slot-number*] **blink stop**

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, the command applies to all member devices.

blink-time: Specifies the flash duration in seconds. The value range is 5 to 120.

stop: Stops flashing.

Usage guidelines

The device supports using the SYS LED for device locating. The **locator blink** *blink-time* command flashes the specified SYS LEDs quickly for a period of time unless you execute the **locator blink stop** command. You can observe the SYS LEDs to locate the devices.

Examples

Start LED flashing to locate devices.

```
<Sysname> locator blink 30
```

Stop LED flashing.

```
<Sysname> locator blink stop
```

memory-threshold

Use **memory-threshold** to set free-memory thresholds.

Use **undo memory-threshold** to restore the defaults.

Syntax

memory-threshold [**slot** *slot-number* [**cpu** *cpu-number*]] [**ratio**] **minor** *minor-value* **severe** *severe-value* **critical** *critical-value* **normal** *normal-value* [**early-warning** *early-warning-value* **secure** *secure-value*]

undo memory-threshold [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

Minor alarm threshold: 448 MB.

Severe alarm threshold: 224 MB.

Critical alarm threshold: 128 MB.

Normal state threshold: 496 MB.

Early-warning threshold: 512 MB.

Sufficient-memory threshold: 576 MB.

Views

System view

Predefined user roles

network-admin

Parameters

ratio: Specifies free-memory thresholds in percentage. If you do not specify this keyword, the command sets free-memory thresholds in MB.

minor *minor-value*: Specifies the minor alarm threshold. To view the value range for this threshold, enter a question mark (?) in the place of the *minor-value* argument. Setting this threshold to 0 disables the minor alarm feature.

severe *severe-value*: Specifies the severe alarm threshold. To view the value range for this threshold, enter a question mark (?) in the place of the *severe-value* argument. Setting this threshold to 0 disables the severe alarm feature.

critical *critical-value*: Specifies the critical alarm threshold. To view the value range for this threshold, enter a question mark (?) in the place of the *critical-value* argument. Setting this threshold to 0 disables the critical alarm feature.

normal *normal-value*: Specifies the normal state threshold. To view the value range for this threshold, enter a question mark (?) in the place of the *normal-value* argument.

early-warning *early-warning-value*: Specifies the early-warning threshold. To view the value range for this threshold, enter a question mark (?) in the place of the *early-warning-value* argument. Setting this threshold to 0 disables the early warning feature.

secure *secure-value*: Specifies the sufficient-memory threshold. To view the value range for this threshold, enter a question mark (?) in the place of the *secure-value* argument.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets free-memory thresholds for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

To ensure correct operation and improve memory efficiency, the system monitors the amount of free memory space in real time. If the amount of free memory space decreases to or below the minor, severe, or critical alarm threshold, the system issues an alarm to affected service modules or processes.

The early warning feature warns you of an approaching insufficient-memory condition.

If a memory alarm occurs, delete unused configuration items or disable some features to increase the free memory space. Because the memory space is insufficient, some configuration items might not be able to be deleted.

For more information about the thresholds, see *Fundamentals Configuration Guide*.

Examples

Set the minor alarm, severe alarm, critical alarm, and normal state thresholds to 64 MB, 48 MB, 32 MB, and 96 MB, respectively.

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

```
[Sysname] memory-threshold minor 64 severe 48 critical 32 normal 96
```

Set the minor alarm, severe alarm, critical alarm, and normal state thresholds to 3%, 2%, 1%, and 5% of the total memory size, respectively.

```
<Sysname> system-view
[Sysname] memory-threshold ratio minor 3 severe 2 critical 1 normal 5
```

Related commands

display memory-threshold

memory-threshold usage

Use **memory-threshold usage** to set the memory usage threshold.

Use **undo memory-threshold usage** to restore the default.

Syntax

memory-threshold [**slot** *slot-number* [**cpu** *cpu-number*]] **usage** *memory-threshold*

undo memory-threshold [**slot** *slot-number* [**cpu** *cpu-number*]] **usage**

Default

The memory usage threshold is 100%.

Views

System view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets the memory usage threshold for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

memory-threshold: Specifies the memory usage threshold in percentage. The value range is 0 to 100.

Usage guidelines

The device samples memory usage at 1-minute intervals. If the sample is greater than the memory usage threshold, the device sends a trap.

Examples

Set the memory usage threshold to 80%.

```
<Sysname> system-view
[Sysname] memory-threshold usage 80
```

Related commands

display memory-threshold

monitor cpu-usage enable

Use **monitor cpu-usage enable** to enable CPU usage monitoring.

Use **undo monitor cpu-usage enable** to disable CPU usage monitoring.

Syntax

monitor cpu-usage enable [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor cpu-usage enable [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

CPU usage monitoring is enabled.

Views

System view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command enables CPU usage monitoring for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

After CPU usage monitoring is enabled, the system samples and saves CPU usage at the interval specified by the **monitor cpu-usage interval** command. You can use the **display cpu-usage history** command to view recent CPU usage.

Examples

Enable CPU usage monitoring.

```
<Sysname> system-view
[Sysname] monitor cpu-usage enable
```

Related commands

display cpu-usage configuration

display cpu-usage history

monitor cpu-usage interval

monitor cpu-usage interval

Use **monitor cpu-usage interval** to set the sampling interval for CPU usage monitoring.

Use **undo monitor cpu-usage interval** to restore default settings.

Syntax

monitor cpu-usage interval *interval* [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor cpu-usage interval [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

The system samples CPU usage every 1 minute.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the sampling interval for CPU usage monitoring. Valid values include **5Sec** (5 seconds), **1Min** (1 minute), and **5Min** (5 minutes), case insensitive.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets the interval for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

After CPU usage monitoring is enabled, the system samples and saves CPU usage at the specified interval. You can use the **display cpu-usage history** command to view recent CPU usage.

Examples

Set the sampling interval for CPU usage monitoring to 5 seconds.

```
<Sysname> system-view
[Sysname] monitor cpu-usage interval 5Sec
```

Related commands

display cpu-usage configuration

display cpu-usage history

monitor cpu-usage enable

monitor cpu-usage threshold

Use **monitor cpu-usage threshold** to set CPU usage alarm thresholds.

Use **undo monitor cpu-usage threshold** to restore default settings.

Syntax

monitor cpu-usage threshold *severe-threshold* **minor-threshold** *minor-threshold* **recovery-threshold** *recovery-threshold* [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor cpu-usage threshold minor-threshold recovery-threshold [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

Severe CPU usage alarm threshold: 99%.

Minor CPU usage alarm threshold: 90%.

CPU usage recovery threshold: 60%.

Views

System view

Predefined user roles

network-admin

Parameters

severe-threshold: Specifies the severe CPU usage alarm threshold in percentage. The value range for this argument is 2 to 100.

minor-threshold *minor-threshold*: Specifies the minor CPU usage alarm threshold in percentage. The value range for this argument is 1 to the severe CPU usage alarm threshold minus 1.

recovery-threshold *recovery-threshold*: Specifies the CPU usage recovery threshold in percentage. The value range for this argument is 0 to the minor CPU usage alarm threshold minus 1.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets the CPU usage threshold for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

The device samples CPU usage at 1-minute intervals. If the sample is greater than the CPU usage threshold, the device sends a trap.

Examples

Set the severe CPU usage alarm threshold to 90%, minor CPU usage alarm threshold to 80%, and CPU usage recovery threshold to 70%.

```
<Sysname> system-view
[Sysname] monitor cpu-usage threshold 90 minor-threshold 80 recovery-threshold 70
```

Related commands

display cpu-usage configuration

monitor resend cpu-usage

Use **monitor resend cpu-usage** to set CPU usage alarm resending intervals.

Use **undo monitor resend cpu-usage** to restore default settings.

Syntax

monitor resend cpu-usage { **minor-interval** *minor-interval* | **severe-interval** *severe-interval* } * [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor resend cpu-usage [**minor-interval** | **severe-interval**] [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

The minor alarm resending interval is 300 seconds. The severe alarm resending interval is 60 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

minor-interval *minor-interval*: Specifies the minor alarm resending interval in seconds, a multiple of five in the range of 10 to 3600.

severe-interval *severe-interval*: Specifies the severe alarm resending interval in seconds, a multiple of five in the range of 10 to 3600.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets alarm resending intervals for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

The device samples CPU usage periodically and compares the sample with the CPU usage threshold. If the sample increases above an alarm threshold, the CPU usage enters an alarm state and the device sends an alarm.

While the CPU usage is in minor alarm state, the device sends minor alarms periodically until the CPU usage increases above the severe threshold or the minor alarm is removed.

While the CPU usage is in severe alarm state, the device sends severe alarms periodically until the severe alarm is removed.

You can use this command to change CPU usage alarm resending intervals.

If you do not specify the **minor-interval** or **severe-interval** keyword, the **undo monitor resend cpu-usage** command restores default settings for both the minor and severe alarm resending intervals.

Examples

Set the CPU usage minor alarm resending interval to 60 seconds for CPU 0 in slot 1.

```
<Sysname> system-view
[Sysname] monitor resend cpu-usage minor-interval 60 slot 1 cpu 0
```

monitor resend memory-threshold

Use **monitor resend memory-threshold** to set memory depletion alarm resending intervals.

Use **undo monitor resend memory-threshold** to restore default settings.

Syntax

monitor resend memory-threshold { **critical-interval** *critical-interval* | **early-warning-interval** *early-warning-interval* | **minor-interval** *minor-interval* | **severe-interval** *severe-interval* } * [**slot** *slot-number* [**cpu** *cpu-number*]]

undo monitor resend memory-threshold [**critical-interval** | **early-warning-interval** | **minor-interval** | **severe-interval**] * [**slot** *slot-number* [**cpu** *cpu-number*]]

Default

- Early warning resending interval: 1 hour.
- Minor alarm resending interval: 12 hours.
- Severe alarm resending interval: 3 hours.
- Critical alarm resending interval: 1 hour.

Views

System view

Predefined user roles

network-admin

Parameters

critical-interval *critical-interval*: Specifies the critical alarm resending interval in hours, in the range of 1 to 48.

early-warning-interval *early-warning-interval*: Specifies the early warning resending interval in hours, in the range of 1 to 48.

minor-interval *minor-interval*: Specifies the minor alarm resending interval in hours, in the range of 1 to 48.

severe-interval *severe-interval*: Specifies the severe alarm resending interval in hours, in the range of 1 to 48.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command sets alarm resending intervals for the master device.

cpu *cpu-number*: Specifies a CPU by its number.

Usage guidelines

The device samples the amount of free memory space periodically and compares the sample with free-memory thresholds. If the sample decreases to or below a threshold, the device enters a memory depletion alarm state and sends an alarm.

In critical alarm state, the device sends critical alarm notifications periodically until the critical alarm is removed.

In a lower alarm state, the device sends notifications for the alarm state periodically until it enters a higher alarm state or the current alarm is removed.

You can use this command to change the alarm resending intervals.

If you do not specify any memory depletion alarm resending intervals, the **undo monitor resend memory-threshold** command restores default settings for all memory depletion alarm resending intervals.

Examples

Set the minor memory depletion alarm resending interval to 12 hours for CPU 0 in slot 1.

```
<Sysname> system-view
[Sysname] monitor resend memory-threshold minor-interval 12 slot 1 cpu 0
```

parity-error consistency-check log enable

Use **parity-error consistency-check log enable** to enable consistency error logging for software and hardware forwarding entries.

Use **undo parity-error consistency-check log enable** to disable consistency error logging for software and hardware forwarding entries.

Syntax

parity-error consistency-check log enable

undo parity-error consistency-check log enable

Default

Consistency error logging is disabled for software and hardware forwarding entries.

Views

System view

Predefined user roles

network-admin

Usage guidelines

To forward packets, the device generates hardware forwarding entries in forwarding chips and software forwarding entries in memory at the same time. The device automatically detects whether the hardware forwarding entries and the software forwarding entries are consistent.

After you execute this command, the device collects consistency errors periodically. If the number of consistency errors in a statistics period reaches or exceeds the logging threshold, the device generates a log message.

Examples

Enable consistency error logging for software and hardware forwarding entries.

```
<Sysname> system-view
[Sysname] parity-error consistency-check log enable
```

Related commands

parity-error consistency-check period

parity-error consistency-check threshold

parity-error consistency-check period

Use **parity-error consistency-check period** to set the statistics period for consistency errors between software and hardware forwarding entries.

Use **undo parity-error consistency-check period** to restore the default.

Syntax

parity-error consistency-check period *value*

undo parity-error consistency-check period

Default

The statistics period is 3600 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the statistics period (in seconds) for consistency errors between software and hardware forwarding entries, in the range of 600 to 31536000.

Usage guidelines

To forward packets, the device generates hardware forwarding entries in forwarding chips and software forwarding entries in memory at the same time. The device automatically detects whether the hardware forwarding entries and the software forwarding entries are consistent.

This command determines the period for the device to collect consistency error statistics.

As a best practice, set the consistency error statistics period to a value greater than 3600 seconds.

Examples

Set the statistics period to 600 seconds for consistency errors between software and hardware forwarding entries.

```
<Sysname> system-view
[Sysname] parity-error consistency-check period 600
```

Related commands

parity-error consistency-check log enable

parity-error consistency-check threshold

parity-error consistency-check threshold

Use **parity-error consistency-check period** to set the logging threshold for consistency errors between software and hardware forwarding entries.

Use **undo parity-error consistency-check period** to restore the default.

Syntax

parity-error consistency-check threshold *value*

undo parity-error consistency-check threshold

Default

The logging threshold is 10.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the logging threshold for consistency errors between software and hardware forwarding entries, in the range of 1 to 2147483647.

Usage guidelines

To forward packets, the device generates hardware forwarding entries in forwarding chips and software forwarding entries in memory at the same time. The device automatically detects whether the hardware forwarding entries and the software forwarding entries are consistent.

After you enable consistency error logging for software and hardware forwarding entries, the device collects statistics for consistency errors periodically. If the number of consistency errors reaches or exceeds the logging threshold, the device generates a log message.

Examples

Set the logging threshold to 20 for consistency errors between software and hardware forwarding entries.

```
<Sysname> system-view
[Sysname] parity-error consistency-check threshold 20
```

Related commands

parity-error consistency-check log enable

parity-error consistency-check period

parity-error monitor log enable

Use **parity-error monitor log enable** to enable parity error logging for entries on forwarding chips.

Use **undo parity-error monitor log enable** to disable parity error logging for entries on forwarding chips.

Syntax

parity-error monitor log enable

undo parity-error monitor log enable

Default

Parity error logging is disabled for entries on forwarding chips.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The device detects parity errors in entries on forwarding chips. The parity error logging feature collects parity error statistics periodically and generates log messages as defined.

Examples

Enable parity error logging for entries on forwarding chips.

```
<Sysname> system-view
[Sysname] parity-error monitor log enable
```

Related commands

parity-error monitor period

parity-error monitor threshold

parity-error monitor period

Use **parity-error monitor period** to set the parity error statistics period for entries on forwarding chips.

Use **undo parity-error monitor period** to restore the default.

Syntax

parity-error monitor period *value*

undo parity-error monitor period

Default

The parity error statistics period is 60 seconds for entries on forwarding chips.

Views

System view

Parameters

value: Specifies the parity error statistics period in seconds, in the range of 1 to 86400.

Predefined user roles

network-admin

Usage guidelines

The device detects parity errors in entries on forwarding chips. The parity error logging feature collects parity error statistics periodically. This command sets the statistics period.

Examples

Set the parity error statistics period to 120 seconds.

```
<Sysname> system-view
[Sysname] parity-error monitor period 120
```

Related commands

parity-error monitor log enable

parity-error monitor threshold

parity-error monitor threshold

Use **parity-error monitor threshold** to set the parity error logging threshold for entries on forwarding chips.

Use **undo parity-error monitor threshold** to restore the default.

Syntax

parity-error monitor threshold *value*

undo parity-error monitor threshold

Default

The parity error logging threshold is 5000 for entries on forwarding chips.

Views

System view

Parameters

value: Specifies the parity error logging threshold for entries on forwarding chips, in the range of 1 to 1000000.

Predefined user roles

network-admin

Usage guidelines

The device detects parity errors in entries on forwarding chips. The parity error logging feature collects parity error statistics periodically, and generates a log message if the number of parity errors exceeds the logging threshold. This command sets the logging threshold.

Examples

Set the parity error logging threshold to 8000 for entries on forwarding chips.

```
<Sysname> system-view
[Sysname] parity-error monitor threshold 8000
```

Related commands

parity-error monitor log enable

parity-error monitor period

password-recovery enable

Use **password-recovery enable** to enable password recovery capability.

Use **undo password-recovery enable** to disable password recovery capability.

Syntax

password-recovery enable

undo password-recovery enable

Default

Password recovery capability is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

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

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

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

To enhance system security, disable password recovery capability.

To access the device configuration without authentication, you must connect to the master device and access the BootWare menu while the master device is starting up.

Availability of BootWare menu options depends on the password recovery capability setting. For more information, see the release notes.

Examples

Disable password recovery capability.

```
<Sysname> system-view
[Sysname] undo password-recovery enable
```

reboot

Use **reboot** to reboot the device.

Syntax

reboot [**slot** *slot-number*] [**force**]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify an IRF member device, the command reboots all IRF member devices.

force: Reboots the device immediately without performing software or hard disk check. If this keyword is not specified, the system first identifies whether the reboot might result in data loss or a system failure. For example, the system identifies whether the main system software image file exists and whether a write operation is in progress on a storage medium. If the reboot might cause problems, the system does not reboot the device.

Usage guidelines

CAUTION:

- A reboot might interrupt network services.
- Use the **force** keyword only when the device fails or a **reboot** command without the **force** keyword cannot perform a reboot correctly. A **reboot** command with the **force** keyword might result in file system corruption because it does not perform data protection.

If the main startup software images are corrupt or missing, you must re-specify a set of main startup software images before executing the **reboot** command.

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

If the IRF fabric has only one member device, rebooting the member device reboots the entire IRF fabric. If the IRF fabric has a subordinate member and the member is operating correctly, rebooting the master triggers a master/subordinate switchover.

To ensure correct operation of the IRF fabric and member devices, do not trigger a switchover by rebooting the master if no subordinate member devices are in **Stable** state. To view the status of subordinate member devices, execute the **display system stable state** command.

Examples

Reboot the device. Save the running configuration at prompt.

```
<Sysname> reboot
Start to check configuration with next startup configuration file, please
wait.........DONE!
Current configuration will be lost after the reboot, save current configuration? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Configuration is saved to mainboard device successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

Reboot the device immediately without performing software check.

```
<Sysname> reboot force
A forced reboot might cause the storage medium to be corrupted. Continue? [Y/N]:y
Now rebooting, please wait...
```

Related commands

display system stable state

reset scheduler logfile

Use **reset scheduler logfile** to clear job execution log information.

Syntax

reset scheduler logfile

Views

User view

Predefined user roles

network-admin

Examples

Clear job execution log information.

```
<Sysname> reset scheduler logfile
```

Related commands

display scheduler logfile

reset version-update-record

Use **reset version-update-record** to clear startup software image upgrade records.

Syntax

reset version-update-record

Views

System view

Predefined user roles

network-admin

Examples

Clear the startup software image upgrade records.

```
<Sysname> system-view
[Sysname] reset version-update-record
This command will delete all records of version update. Continue? [Y/N]:y
```

Related commands

display version-update-record

resource-monitor minor resend enable

Use **resource-monitor minor resend enable** to enable resending of minor resource depletion alarms.

Use **undo resource-monitor minor resend enable** to disable resending of minor resource depletion alarms.

Syntax

resource-monitor minor resend enable

undo resource-monitor minor resend enable

Default

Resending of minor resource depletion alarms is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When a resource type enters minor alarm state, the device issues a minor alarm. If the resource type stays in minor alarm state or changes from severe alarm state to minor alarm state, the device identifies whether resending of minor resource depletion alarms is enabled. If the feature is disabled, the device does not issue additional minor alarms. If the feature is enabled, the device resends minor alarms periodically.

The resending period is fixed at 24 hours for a severe alarm and is fixed at 7 * 24 hours for a minor alarm.

Examples

Enable resending of minor resource depletion alarms.

```
<Sysname> system-view
[Sysname] resource-monitor minor resend enable
```

Related commands

display resource-monitor

resource-monitor output

resource-monitor resource

resource-monitor output

Use **resource-monitor output** to specify destinations for resource depletion alarms.

Use **undo resource-monitor output** to remove destinations for resource depletion alarms.

Syntax

resource-monitor output { **netconf-event** | **snmp-notification** | **syslog** } *

undo resource-monitor output [**netconf-event** | **snmp-notification** | **syslog**] *

Default

Resource depletion alarms are sent to NETCONF, SNMP, and the information center.

Views

System view

Predefined user roles

network-admin

Parameters

netconf-event: Sends resource depletion alarms to the NETCONF feature to encapsulate the alarms in NETCONF events. For more information, see NETCONF in *Network Management and Monitoring Configuration Guide*.

snmp-notification: Sends resource depletion alarms to the SNMP feature to encapsulate the alarms in SNMP traps and informs. For more information, see SNMP in *Network Management and Monitoring Configuration Guide*.

syslog: Sends resource depletion alarms to the information center to encapsulate the alarms in log messages. For more information, see information center in *Network Management and Monitoring Configuration Guide*.

Usage guidelines

If you do not specify any keywords for the **undo resource-monitor output** command, the command disables resource depletion alarm output.

Examples

Specify the information center module as the output destination for resource depletion alarms.

```
<Sysname> system-view
[Sysname] resource-monitor output syslog
```

Related commands

resource-monitor minor resend enable

resource-monitor resource

resource-monitor resource

Use **resource-monitor resource** to set resource depletion thresholds.

Use **undo resource-monitor resource** to disable resource depletion thresholds.

Syntax

resource-monitor resource *resource-name* **slot** *slot-number* **cpu** *cpu-number* **by-percent minor-threshold** *minor-threshold* **severe-threshold** *severe-threshold*

undo resource-monitor resource *resource-name* **slot** *slot-number* **cpu** *cpu-number*

Default

The default settings vary by resource type. Use the **display resource-monitor** command to display the resource depletion thresholds.

Views

System view

Predefined user roles

network-admin

Parameters

resource-name: Specifies a resource type by its name. The values for this argument are case insensitive and cannot be abbreviated. Table 52 shows the resource types that can be monitored.

Table 52 Resource types that can be monitored

Resource type	Description
ac	Ethernet service instances.
agg_group	Aggregation group resources.
arp	ARP resources.
ecmpgroup	ECMP group resources.
ecmpgroup_overlay	ECMP group resources for the overlay network.
g_rsvd_vlan	Reserved global VLAN interface resources.
ipv6_127	Resources for IPv6 routes with a prefix length of 65 to 127 bits.
ipv6_128	Resources for IPv6 routes with a prefix length of 128 bits.
ipv6_64	Resources for IPv6 routes with a prefix length of 0 to 64 bits.
mac	MAC address table resources.

Resource type	Description
mqcin	Inbound MQC resources.
mqcin_c0_p0	Inbound MQC resources of Pipe 0 on Chip 0.
mqcin_c0_p1	Inbound MQC resources of Pipe 1 on Chip 0.
mqcout	Outbound MQC resources.
mqcout_c0	Outbound MQC resources of Chip 0.
nd	ND resources.
nexthoppool1	Next-hop pool resources for the underlay network.
nexthoppool2	Next-hop pool resources for the overlay network.
nexthoppool3	Layer 3 ECMP pool resources.
nexthoppool4	Layer 3 ECMP pool resources for the overlay network.
openflow	OpenFlow resources.
openflowin_c0_p0	OpenFlow resources of Pipe 0 on Chip 0.
openflowin_c0_p1	OpenFlow resources of Pipe 1 on Chip 0.
pbr	PBR resources.
pbrin_c0_p0	PBR resources of Pipe 0 on Chip 0.
pbrin_c0_p1	PBR resources of Pipe 1 on Chip 0.
pfilterin	Inbound packet filter resources.
pfilterin_c0_p0	Inbound packet filter resources of Pipe 0 on Chip 0.
pfilterin_c0_p1	Inbound packet filter resources of Pipe 1 on Chip 0.
pfilterout	Outbound packet filter resources.
pfilterout_ c0	Outbound packet filter resources of Chip 0.
route	Routing resources.
rport	Layer 3 Ethernet interface resources.
subrport	Layer 3 Ethernet subinterface resources.
vlaninterface	VLAN interface resources.
vrf	VPN instance resources.
vsi	VSIs.
vsiintf	VSI interface resources.

slot *slot-number*: Specifies an IRF member device by its member ID.

cpu *cpu-number*: Specifies a CPU by its number.

by-percent: Specifies resource depletion thresholds in percentage.

minor-threshold *minor-threshold*: Specifies the minor resource depletion threshold. To view the value range, enter a question mark (?) in the place of the *minor-threshold* argument.

severe-threshold *severe-threshold*: Specifies the severe resource depletion threshold. To view the value range, enter a question mark (?) in the place of the *severe-threshold* argument.

Usage guidelines

After you execute this command for a resource type, the device monitors the available amount of the type of resources. The device samples the available amount at intervals, compares the sample with the resource depletion thresholds to identify the resource depletion status, and sends alarms as configured.

Examples

Set the minor resource depletion threshold to 30% and the severe resource depletion threshold to 10% for ARP entry resources on slot 1.

```
<Sysname> system-view
[Sysname] resource-monitor resource arp slot 1 cpu 0 by-percent minor-threshold 30
severe-threshold 10
```

Related commands

display resource-monitor

resource-monitor minor resend enable

resource-monitor output

restore factory-default

Use **restore factory-default** to restore the factory-default configuration for the device.

Syntax

restore factory-default

Views

User view

Predefined user roles

network-admin

Usage guidelines

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

Examples

Restore the factory-default configuration for the device.

```
<Sysname> restore factory-default
This command will restore the system to the factory default configuration and clear the
operation data. Continue [Y/N]:y
Restoring the factory default configuration. This process might take a few minutes. Please
wait.....................................................................................
.......................Done.
Please reboot the system to place the factory default configuration into effect.
```

Related commands

reboot

scheduler job

Use **scheduler job** to create a job and enter its view, or enter the view of an existing job.

Use **undo scheduler job** to delete a job.

Syntax

scheduler job *job-name*

undo scheduler job *job-name*

Default

No job exists.

Views

System view

Predefined user roles

network-admin

Parameters

job-name: Specifies the job name, a case-sensitive string of 1 to 47 characters.

Usage guidelines

A job can be referenced by multiple schedules. In job view, you can assign commands to the job.

Examples

Create a job named **backupconfig** and enter job view.

```
<Sysname> system-view
[Sysname] scheduler job backupconfig
[Sysname-job-backupconfig]
```

Related commands

command

scheduler schedule

scheduler logfile size

Use **scheduler logfile size** to set the size of the job execution log file.

Syntax

scheduler logfile size *value*

Default

The size of the job execution log file is 16 KB.

Views

System view

Predefined user roles

network-admin

Parameters

value: Specifies the size of the job execution log file, in KB. The value range is 16 to 1024.

Usage guidelines

The job execution log file saves the execution information of jobs. If the file is full, old records are deleted to make room for new records. If the size of the log information to be written to the file is greater than the file size, the excessive information is not written to the file.

Examples

Set the size of the job execution log file to 32 KB.

```
<Sysname> system-view
[Sysname] scheduler logfile size 32
```

Related commands

display scheduler logfile

scheduler reboot at

Use **scheduler reboot at** to specify the reboot date and time.

Use **undo scheduler reboot** to delete the reboot schedule configuration.

Syntax

scheduler reboot at *time* [*date*]

undo scheduler reboot

Default

No reboot date or time is specified.

Views

User view

Predefined user roles

network-admin

Parameters

time: Specifies the reboot time in the *hh:mm* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59.

date: Specifies the reboot date in the *MM/DD/YYYY* or *YYYY/MM/DD* format. The value range for *YYYY* is 2000 to 2035. The value range for *MM* is 1 to 12. The value range for *DD* varies by month.

Usage guidelines

CAUTION:
Device reboot interrupts network services.

When the *date* argument is not specified, the system uses the following rules to determine the reboot time:

- If the reboot time is later than the current time, a reboot occurs at the reboot time of the current day.
- If the reboot time is earlier than the current time, a reboot occurs at the reboot time the next day.

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

For data security, the system does not reboot at the reboot time if a file operation is being performed.

Examples

Configure the device to reboot at 12:00 p.m. This example assumes that the current time is 11:43 a.m. on June 6, 2015.

```
<Sysname> scheduler reboot at 12:00
Reboot system at 12:00:00 06/06/2015 (in 0 hours and 16 minutes). Confirm? [Y/N]:
```

Related commands

scheduler reboot delay

scheduler reboot delay

Use **scheduler reboot delay** to specify the reboot delay time.

Use **undo scheduler reboot** to delete the reboot schedule configuration.

Syntax

scheduler reboot delay *time*

undo scheduler reboot

Default

No reboot delay time is specified.

Views

User view

Predefined user roles

network-admin

Parameters

time: Specifies the reboot delay time in the *hh:mm* or *mm* format. This argument can contain up to six characters. When in the *hh:mm* format, *mm* must be in the range of 0 to 59.

Usage guidelines

CAUTION:
Device reboot interrupts network services.

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

For data security, the system does not reboot at the reboot time if a file operation is being performed.

Examples

Configure the device to reboot after 88 minutes. This example assumes that the current time is 11:48 a.m. on June 6, 2015.

```
<Sysname> scheduler reboot delay 88
Reboot system at 13:16 06/06/2015(in 1 hours and 28 minutes). Confirm? [Y/N]:
```

scheduler schedule

Use **scheduler schedule** to create a schedule and enter its view, or enter the view of an existing schedule.

Use **undo scheduler schedule** to delete a schedule.

Syntax

scheduler schedule *schedule-name*

undo scheduler schedule *schedule-name*

Default

No schedule exists.

Views

System view

Predefined user roles

network-admin

Parameters

schedule-name: Specifies the schedule name, a case-sensitive string of 1 to 47 characters.

Usage guidelines

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

To configure a schedule:

1. Use the **scheduler job** command to create a job and enter job view.
2. Use the **command** command to assign commands to the job.
3. Use the **scheduler schedule** command to create a schedule and enter schedule view.
4. Use the **job** command to assign the job to the schedule. You can assign multiple jobs to a schedule. The jobs must already exist.
5. Use the **user-role** command to assign user roles to the schedule. You can assign up to 64 user roles to a schedule.
6. Use the **time at**, **time once**, or **time repeating** command to specify an execution time for the schedule. You can specify only one execution time for a schedule.

Examples

Create a schedule named **saveconfig**.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
```

Related commands

job

time at

time once

shutdown-interval

Use **shutdown-interval** to set the port status detection timer.

Use **undo shutdown-interval** to restore the default.

Syntax

shutdown-interval *interval*

undo shutdown-interval

Default

The port status detection timer setting is 30 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the port status detection timer value in seconds. The value range is 0 to 300. To disable port status detection, set this argument to 0.

Usage guidelines

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

If you change the timer setting during port detection, the device compares the new setting (T1) with the time that elapsed since the port was shut down (T).

If T < T1, the port will be brought up after T1 – T seconds.

If T ≥ T1, the port is brought up immediately.

For example, the timer setting is 30 seconds. If you change it to 10 seconds 2 seconds after the port is shut down, the port will come up 8 seconds later. If you change the timer setting to 2 seconds 10 seconds after the port is shut down, the port comes up immediately.

Examples

Set the port status detection timer to 100 seconds.

```
<Sysname> system-view
[Sysname] shutdown-interval 100
```

sysname

Use **sysname** to set the device name.

Use **undo sysname** to restore the default.

Syntax

sysname *sysname*

undo sysname

Default

The device name is **HPE**.

Views

System view

Predefined user roles

network-admin

Parameters

sysname: Specifies a name for the device, a string of 1 to 64 characters.

Usage guidelines

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

Examples

Set the name of the device to **R2000**.

```
<Sysname> system-view
[Sysname] sysname R2000
```

```
[R2000]
```

system-working-mode

Use **system-working-mode** to set the system operating mode.

Use **undo system-working-mode** to restore the default.

Syntax

system-working-mode { **advance** | **standard** }

undo system-working-mode

Default

The device operates in standard mode.

Views

System view

Predefined user roles

network-admin

Parameters

advance: Sets the system operating mode to advanced.

standard: Sets the system operating mode to standard.

Usage guidelines

The system operating mode determines the supported features and the feature specifications. For more information, see device management in *Fundamentals Configuration Guide*.

Change to the operating mode takes effect after a reboot.

Examples

Set the system operating mode to advanced.

```
<Sysname> system-view
[Sysname] system-working-mode advance
Do you want to change the system working mode? [Y/N]:y
System working mode changed. For the change to take effect, save the running configuration
and reboot the device.
```

temperature-limit

Use **temperature-limit** to set the temperature alarm thresholds.

Use **undo temperature-limit** to restore the default.

Syntax

temperature-limit slot *slot-number* **hotspot** *sensor-number lowlimit warninglimit* [*alarmlimit*]

undo temperature-limit slot *slot-number* **hotspot** *sensor-number*

Default

The defaults vary by temperature sensor model. To view the defaults, execute the **undo temperature-limit** and **display environment** commands in turn.

Views

System view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

hotspot: Configures temperature alarm thresholds for hotspot sensors. A hotspot sensor is typically located near a high-heat chip to monitor the chip temperature.

sensor-number: Specifies a sensor by its number. To view the value range, enter a question mark (?) in the place of this argument.

lowlimit: Specifies the low-temperature threshold in Celsius degrees. The value range varies by temperature sensor. To view the value range, enter a question mark (?) in the place of this argument.

warninglimit: Specifies the high-temperature warning threshold in Celsius degrees. This threshold must be greater than the low-temperature threshold. To view the value range, enter a question mark (?) in the place of this argument.

alarmlimit: Specifies the high-temperature alarming threshold in Celsius degrees. This threshold must be greater than the warning threshold. To view the value range, enter a question mark (?) in the place of this argument.

Usage guidelines

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

- Sends log messages and traps.
- Sets LEDs on the device panel.

Examples

Set temperature alarm thresholds for hotspot sensor 1 in a slot.

```
<Sysname> system-view
[Sysname] temperature-limit slot 1 hotspot 1 -10 50 60
```

Related commands

display environment

time at

Use **time at** to specify an execution date and time for a non-periodic schedule.

Use **undo time** to delete the execution date and time configuration for a non-periodic schedule.

Syntax

time at *time date*

undo time

Default

No execution time or date is specified for a non-periodic schedule.

Views

Schedule view

Predefined user roles

network-admin

Parameters

time: Specifies the schedule execution time in the *hh:mm* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59.

date: Specifies the schedule execution date in the *MM/DD/YYYY* or *YYYY/MM/DD* format. The value range for *YYYY* is 2000 to 2035. The value range for *MM* is 1 to 12. The value range for *DD* varies by month.

Usage guidelines

The specified time (date plus time) must be later than the current system time.

The **time at** command, the **time once** command, and the **time repeating** command overwrite one another. The most recently configured command takes effect.

Examples

Configure the device to execute schedule **saveconfig** at 01:01 a.m. on May 11, 2015.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time at 1:1 2015/05/11
```

Related commands

scheduler schedule

time once

Use **time once** to specify one or more execution days and the execution time for a non-periodic schedule.

Use **undo time** to delete the execution day and time configuration for a non-periodic schedule.

Syntax

time once at *time* [**month-date** *month-day* | **week-day** *week-day*&<1-7>]

time once delay *time*

undo time

Default

No execution time or day is specified for a non-periodic schedule.

Views

Schedule view

Predefined user roles

network-admin

Parameters

at *time*: Specifies the execution time in the *hh:mm* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59.

month-date *month-day*: Specifies a day in the current month, in the range of 1 to 31. If you specify a day that does not exist in the current month, the configuration takes effect on that day in the next month.

week-day *week-day*&<1-7>: Specifies a space-separated list of up to seven week days for the schedule. Valid week day values include **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat**, and **Sun**.

delay *time*: Specifies the delay time for executing the schedule, in the *hh:mm* or *mm* format. This argument can have up to six characters. When in the *hh:mm* format, *mm* must be in the range of 0 to 59.

Usage guidelines

If the specified time has already occurred, the schedule will be executed at the specified time the following day.

If the day in the month has already occurred, the schedule will be executed at the specified day in the following month.

If the specified day in a week has already occurred, the schedule will be executed at the specified day in the following week.

The **time at** command, the **time once** command, and the **time repeating** command overwrite one another. The most recently configured command takes effect.

Examples

Configure the device to execute schedule **saveconfig** once at 15:00.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time once at 15:00
Schedule starts at 15:00 5/11/2011.
```

Configure the device to execute schedule **saveconfig** once at 15:00 on the coming 15th day in a month.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time once at 15:00 month-date 15
```

Configure the device to execute schedule **saveconfig** at 12:00 p.m. on the coming Monday and Friday.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time once at 12:00 week-day mon fri
```

Configure the device to execute schedule **saveconfig** after 10 minutes.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time once delay 10
```

Related commands

scheduler schedule

time repeating

Use **time repeating** to specify an execution time table for a periodic schedule.

Use **undo time** to delete the execution time table configuration for a periodic schedule.

Syntax

time repeating [**at** *time* [*date*]] **interval** *interval*

time repeating at *time* [**month-date** [*month-day* | **last**] | **week-day** *week-day*&<1-7>]

undo time

Default

No execution time table is specified for a periodic schedule.

Views

Schedule view

Predefined user roles

network-admin

Parameters

at *time*: Specifies the execution time in the *hh:mm* format. The value range for *hh* is 0 to 23. The value range for *mm* is 0 to 59. If you do not specify this option, the current system time is used as the execution time.

date: Specifies the start date for the periodic schedule, in the *MM/DD/YYYY* or *YYYY/MM/DD* format. The value range for *YYYY* is 2000 to 2035. The value range for *MM* is 1 to 12. The value range for *DD* varies by month. If you do not specify this argument, the execution start date is the first day when the specified time arrives.

interval *interval*: Specifies the execution time interval in the *hh:mm or mm* format. This argument can have up to six characters. When in the *hh:mm* format, *mm* must be in the range of 0 to 59. When in the *mm* format, this argument must be equal to or greater than 1 minute.

month-date [*month-day* | **last**]: Specifies a day in a month, in the range 1 to 31. The **last** keyword indicates the last day of a month. If you specify a day that does not exist in a month, the configuration takes effect on that day in the next month.

week-day *week-day*&<1-7>: Specifies a space-separated list of up to seven week days for the schedule. Valid week day values include **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat**, and **Sun**.

Usage guidelines

The **time repeating** [**at** *time* [*date*]] **interval** *interval* command configures the device to execute a schedule at intervals from the specified time on.

The **time repeating at** *time* [**month-date** [*month-day* | **last**] | **week-day** *week-day*&<1-7>] command configures the device to execute a schedule at the specified time on every specified day in a month or week.

The **time at** command, the **time once** command, and the **time repeating** command overwrite one another, whichever is configured most recently takes effect.

Examples

Configure the device to execute schedule **saveconfig** once an hour from 8:00 a.m. on.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time repeating at 8:00 interval 60
```

Configure the device to execute schedule **saveconfig** at 12:00 p.m. every day.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time repeating at 12:00
```

Configure the device to execute schedule **saveconfig** at 8:00 a.m. on the 5th of every month.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time repeating at 8:00 month-date 5
```

Configure the device to execute schedule **saveconfig** at 8:00 a.m. on the last day of every month.

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

```
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time repeating at 8:00 month-date last
```

Configure the device to execute schedule **saveconfig** at 8:00 a.m. every Friday and Saturday.

```
<Sysname> system-view
[Sysname] scheduler schedule saveconfig
[Sysname-schedule-saveconfig] time repeating at 8:00 week-day fri sat
```

Related commands

scheduler schedule

user-role

Use **user-role** to assign user roles to a schedule.

Use **undo user-role** to remove user roles from a schedule.

Syntax

user-role *role-name*

undo user-role *role-name*

Default

A schedule has the user roles of the schedule creator.

Views

Schedule view

Predefined user roles

network-admin

Parameters

role-name: Specifies a user role name, a case-sensitive string of 1 to 63 characters. The user role can be user-defined or predefined. Predefined user roles include network-admin, network-operator, and level-0 to level-15.

Usage guidelines

A schedule must have one or more user roles. A command in a schedule can be executed if it is permitted by one or more user roles of the schedule. For more information about user roles, see the RBAC configuration in *Fundamentals Configuration Guide*.

A schedule can have a maximum of 64 user roles. After the limit is reached, you cannot assign additional user roles to the schedule.

Examples

Assign user role **rolename** to schedule **test**.

```
<Sysname> system-view
[Sysname] scheduler schedule test
[Sysname-schedule-test] user-role rolename
```

Related commands

command

scheduler schedule

Tcl commands

cli

Use **cli** to enable a Comware command to be executed in Tcl configuration view when it conflicts with a Tcl command.

Syntax

cli *command*

Views

Tcl configuration view

Predefined user roles

network-admin

Parameters

command: Specifies the commands to be executed. They must be complete command lines.

Usage guidelines

In Tcl configuration view, if a Comware command conflicts with a Tcl command, the Tcl command will be executed. To execute the Comware command when a conflict occurs, execute the **cli** command.

Examples

Perform the following steps to execute a Comware command that conflicts with a Tcl command in Tcl configuration view.

1. Execute a Comware command in Tcl configuration view. The output shows that the Comware command cannot be executed because it conflicts with a Tcl command.

```
<Sysname> tclsh
<Sysname-tcl> system-view
[Sysname-tcl] route-policy 1 permit node 10
[Sysname-tcl-route-policy-1-10] apply cost 10
can't interpret "cost" as a lambda expression
```

2. Configure the **cli** command to execute the Comware command again.

```
[Sysname-tcl-route-policy-1-10] cli apply cost 10
```

Execute multiple Comware commands in one operation.

```
<Sysname> tclsh
<Sysname-tcl> system-view
```

- Method 1:

```
[Sysname-tcl] cli "vlan 2 ; description Tech"
```

- Method 2:

```
[Sysname-tcl] cli vlan 2 ; cli description Tech
```

tclquit

Use **tclquit** to return from Tcl configuration view to user view.

Syntax

tclquit

Views

Tcl configuration view

Predefined user roles

network-admin

Usage guidelines

To return from Tcl configuration view to user view, you can also use the **quit** command.

To return to the upper-level view after you execute Comware commands to enter system view or a Comware feature view, use the **quit** command.

Examples

Return from Tcl configuration view to user view.

```
<Sysname-tcl> tclquit
<Sysname>
```

Related commands

tclsh

tclsh

Use **tclsh** to enter Tcl configuration view from user view.

Syntax

tclsh

Views

User view

Predefined user roles

network-admin

Usage guidelines

In Tcl configuration view, you can execute the following commands:

- All Tcl 8.5 commands.
- Comware commands. The Tcl configuration view is equivalent to the user view. You can use Comware commands in Tcl configuration view in the same way they are used in user view.

Examples

Enter Tcl configuration view from user view.

```
<Sysname> tclsh
<Sysname-tcl>
```

Related commands

tclquit

Python commands

exit()

Use **exit()** to exit the Python shell.

Syntax

exit()

Views

Python shell

Predefined user roles

network-admin

Usage guidelines

To return to user view from the Python shell, you cannot use the **quit** command. You must use the **exit()** command.

Examples

Exit the Python shell.

```
Python 2.7.3 (default)
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
>>> exit()
<Sysname>
```

python

Use **python** to enter the Python shell.

Syntax

python

Views

User view

Predefined user roles

network-admin

Usage guidelines

In the Python shell, you can use the following items:

- Python 2.7 commands.
- Python 2.7 standard API.
- Comware 7 extended API.

Examples

Enter the Python shell.

```
<Sysname> python
Python 2.7.3 (default)
```

```
[GCC 4.4.1] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

python *filename*

Use **python** *filename* to execute a Python script.

Syntax

python *filename* [*param*]

Views

User view

Predefined user roles

network-admin

Parameters

filename: Specifies the name of a Python script on a storage medium of the device. The script name is case sensitive and must use the extension .py. The extension .py is case insensitive.

param: Specifies the parameters to be passed to the script. To enter multiple parameters, use spaces as the delimiter.

Usage guidelines

You cannot perform any operations while you are executing a Python script.

Make sure the statements in the script meet the syntax requirements. The system stops executing a Python script if it finds a statement with syntax errors.

When executing a script, the system uses the defaults for interactive statements. The system does not stop for human input.

Examples

Execute Python script **test.py**.

```
<Sysname> python test.py 1 2
['/flash:/test.py', '1', '2']
```

Document conventions and icons

Conventions

This section describes the conventions used in the documentation.

Command conventions

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

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
⚠ **WARNING!**	An alert that calls attention to important information that if not understood or followed can result in personal injury.
△ **CAUTION:**	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
ⓘ **IMPORTANT:**	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

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

  www.hpe.com/support/hpesc

Information to collect

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

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
  - Hewlett Packard Enterprise Support Center **Get connected with updates** page:

    www.hpe.com/support/e-updates
  - Software Depot website:

    www.hpe.com/support/softwaredepot
- To view and update your entitlements, and to link your contracts, Care Packs, and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  www.hpe.com/support/AccessToSupportMaterials

IMPORTANT:

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

Websites

Website	Link
Networking websites	
Hewlett Packard Enterprise Information Library for Networking	www.hpe.com/networking/resourcefinder
Hewlett Packard Enterprise Networking website	www.hpe.com/info/networking
Hewlett Packard Enterprise My Networking website	www.hpe.com/networking/support
Hewlett Packard Enterprise My Networking Portal	www.hpe.com/networking/mynetworking
Hewlett Packard Enterprise Networking Warranty	www.hpe.com/networking/warranty
General websites	
Hewlett Packard Enterprise Information Library	www.hpe.com/info/enterprise/docs
Hewlett Packard Enterprise Support Center	www.hpe.com/support/hpesc
Hewlett Packard Enterprise Support Services Central	ssc.hpe.com/portal/site/ssc/
Contact Hewlett Packard Enterprise Worldwide	www.hpe.com/assistance
Subscription Service/Support Alerts	www.hpe.com/support/e-updates
Software Depot	www.hpe.com/support/softwaredepot
Customer Self Repair (not applicable to all devices)	www.hpe.com/support/selfrepair
Insight Remote Support (not applicable to all devices)	www.hpe.com/info/insightremotesupport/docs

Customer self repair

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

For more information about CSR, contact your local service provider or go to the CSR website:

www.hpe.com/support/selfrepair

Remote support

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

For more information and device support details, go to the following website:

www.hpe.com/info/insightremotesupport/docs

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title,

part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Index

A B C D E F G H I J L M N O P Q R S T U V W

A

activation-key,47
alias,1
append,101
archive configuration,160
archive configuration interval,161
archive configuration location,162
archive configuration max,163
archive configuration server,164
archive configuration server password,166
archive configuration server user,166
ascii,102
authentication-mode,49
auto-execute command,51

B

backup startup-configuration,167
binary,102
boot-loader file,187
boot-loader update,189
bye,103

C

cd,103
cd,138
cdup,104
cli,301
clock datetime,232
clock protocol,233
clock summer-time,233
clock timezone,235
close,105
command,236
command accounting,52
command authorization,53
configuration commit,168
configuration commit delay,169
configuration encrypt,170
configuration replace file,170
copy,139
copyright-info enable,237
Customer self repair,308

D

databits,54
debug,105
delete,106
delete,142
description,15
dir,143
dir,106
disconnect,107
display [| [by-linenum] { begin | exclude | include }],2
display >,4
display >>,5
display alarm,237
display alias,6
display archive configuration,171
display boot-loader,190
display clock,238
display copyright,239
display cpu-usage,239
display cpu-usage configuration,240
display cpu-usage history,241
display current-configuration,172
display current-configuration diff,174
display default-configuration,175
display device,243
display device manuinfo,244
display device manuinfo fan,244
display device manuinfo power,245
display diagnostic-information,245
display diff,176
display environment,247
display fan,248
display ftp client source,108
display ftp-server,93
display ftp-user,93
display hardware-failure-detection,249
display hardware-resource switch-mode,250
display history-command,6
display history-command all,7
display hotkey,8
display install active,192
display install backup,193
display install committed,195
display install inactive,196
display install ipe-info,197
display install job,198

display install log,198
display install package,200
display install rollback,201
display install which,201
display issu rollback-timer,203
display issu state,203
display line,54
display memory,251
display memory-threshold,252
display power,254
display provision failed-config,229
display resource-monitor,255
display role,15
display role feature,22
display role feature-group,25
display saved-configuration,177
display scheduler job,256
display scheduler logfile,257
display scheduler reboot,258
display scheduler schedule,258
display startup,178
display system stable state,259
display system-working-mode,261
display telnet client,56
display this,179
display transceiver alarm,261
display transceiver diagnosis,263
display transceiver interface,264
display transceiver manuinfo,264
display user-interface,56
display users,58
display version,264
display version comp-matrix,206
display version-update-record,265
Documentation feedback,308
download manuinfo fan,266

E

escape-key,59
execute,144
exit(),303

F

fan prefer-direction,267
fdisk,144
feature,27
file prompt,146
fixdisk,147
flow-control,60
format,147
free ftp user,94
free ftp user-ip,95
free ftp user-ip ipv6,95
free line,61
free user-interface,62
ftp,108
ftp client ipv6 source,110
ftp client source,111
ftp ipv6,111
ftp server acl,96
ftp server acl-deny-log enable,97
ftp server dscp,97
ftp server enable,98
ftp server ipv6 dscp,98
ftp server ssl-server-policy,99
ftp timeout,99

G

get,113
gunzip,148
gzip,149

H

hardware-failure-detection,267
hardware-resource switch-mode,268
header,269
help,114
history-command max-size,62
hotkey,9
http acl,63
https acl,64

I

idle-timeout,65
install abort,207
install activate,208
install add,210
install commit,211
install deactivate,212
install remove,213
install rollback to,213
install verify,215
interface policy deny,28
issu accept,216
issu commit,216
issu load,218
issu one-step,221
issu quit,223
issu rollback,223
issu rollback-timer,224
issu run switchover,225

J

job,270

L

lcd,115
line,66
line class,66
locator blink,271
lock,68
lock reauthentication,69
lock-key,69
ls,115

M

md5sum,150
memory-threshold,271
memory-threshold usage,273
mkdir,150
mkdir,117
monitor cpu-usage enable,273
monitor cpu-usage interval,274
monitor cpu-usage threshold,275
monitor resend cpu-usage,276
monitor resend memory-threshold,277
more,151
mount,151
move,152

N

newer,117

O

open,118

P

parity,70
parity-error consistency-check log enable,278
parity-error consistency-check period,279
parity-error consistency-check threshold,280
parity-error monitor log enable,280
parity-error monitor period,281
parity-error monitor threshold,282
passive,118
password-recovery enable,282
permit interface,29
permit vlan,31
permit vpn-instance,32
protocol inbound,71
provision,229
put,119
pwd,153
pwd,120
python,303
python filename,304

Q

quit,11
quit,120

R

reboot,283
reget,121
Remote support,308
rename,153
rename,121
repeat,11
reset,122
reset install log-history oldest,227
reset install rollback oldest,227
reset provision failed-config,230
reset recycle-bin,153
reset saved-configuration,180
reset scheduler logfile,284
reset version-update-record,285
resource-monitor minor resend enable,285
resource-monitor output,286
resource-monitor resource,287
restart,123
restful http enable,73
restful http port,74
restful https enable,74
restful https port,75
restore factory-default,289
restore startup-configuration,181
return,13
rhelp,123
rmdir,154
rmdir,125
role,34
role default-role enable,34
role feature-group,35
rstatus,125
rule,36

S

save,182
scheduler job,289
scheduler logfile size,290
scheduler reboot at,291
scheduler reboot delay,292
scheduler schedule,292
screen-length,75
screen-length disable,13
send,76

set authentication password,77
sha256sum,155
shell,78
shutdown-interval,293
slot,231
speed,79
standby auto-update config,185
startup saved-configuration,185
status,127
stopbits,79
super,40
super authentication-mode,41
super default role,42
super password,42
super use-login-username,44
sysname,294
system,128
system-view,14
system-working-mode,295

T

tar create,155
tar extract,156
tar list,157
tclquit,301
tclsh,302
telnet,80
telnet client source,81
telnet ipv6,82
telnet server acl,83
telnet server acl-deny-log enable,84
telnet server dscp,84
telnet server enable,85
telnet server ipv6 acl,85
telnet server ipv6 dscp,86
telnet server ipv6 port,87
telnet server port,87
temperature-limit,295
terminal type,88
tftp,131
tftp client ipv6 source,133
tftp client source,133
tftp ipv6,134
tftp-server acl,136
tftp-server ipv6 acl,136
time at,296
time once,297
time repeating,298

U

umount,158
undelete,159
user,128
user-interface,89
user-interface class,90
user-role,300
user-role,91

V

verbose,129
vlan policy deny,44
vpn-instance policy deny,45

W

Websites,308