

Content

Chapter 1 COMMANDS FOR SHOW	1-1
1.1 clear history all-users.....	1-1
1.2 history all-users max-length.....	1-1
1.3 logging executed-commands.....	1-1
1.4 ping.....	1-2
1.5 ping6.....	1-3
1.6 show boot-files.....	1-5
1.7 show debugging.....	1-5
1.8 show fan.....	1-6
1.9 show flash.....	1-6
1.10 show history.....	1-6
1.11 show history all-users.....	1-7
1.12 show logging executed-commands state.....	1-7
1.13 show memory.....	1-8
1.14 show running-config.....	1-8
1.15 show running-config current-mode.....	1-9
1.16 show startup-config.....	1-9
1.17 show switchport interface.....	1-10
1.18 show tcp.....	1-10
1.19 show tcp ipv6.....	1-11
1.20 show telnet login.....	1-11
1.21 show temperature.....	1-12
1.22 show tech-support.....	1-12
1.23 show udp.....	1-12
1.24 show udp ipv6.....	1-13
1.25 show version.....	1-13
1.26 traceroute.....	1-14
1.27 traceroute6.....	1-14
Chapter 2 COMMANDS FOR RELOAD SWITCH AFTER SPECIFIED TIME	2-1
2.1 reload after.....	2-1
2.2 reload cancel.....	2-1
2.3 show reload.....	2-2

Chapter 3 COMMANDS FOR DEBUGGING AND DIAGNOSIS FOR PACKETS RECEIVED AND SENT BY CPU.....	3-1
3.1 clear cpu-rx-stat protocol.....	3-1
3.2 cpu-rx-limitnotify enable interval.....	3-1
3.3 cpu-rx-limitnotify protocol (all WORD)(enable disable).....	3-2
3.4 cpu-rx-ratelimit channel.....	3-2
3.5 cpu-rx-ratelimit enhanced.....	3-2
3.6 cpu-rx-ratelimit protocol.....	3-2
3.7 cpu-rx-ratelimit queue-length.....	3-3
3.8 cpu-rx-ratelimit total.....	3-3
3.9 debug driver.....	3-3
3.10 protocol filter.....	3-4
3.11 show cpu-rx protocol.....	3-4
Chapter 4 COMMANDS FOR DCP.....	4-1
4.1 dcp enable.....	4-1
4.2 dcp disable.....	4-1
4.3 dcp limit-rate <20-50>.....	4-2
4.4 dcp no-limit-ip <ip_addr>.....	4-2
4.5 show dcp limit-rate.....	4-3
4.6 show cpu ip rate top10.....	4-3
4.7 show dcp limited ip.....	4-4
4.8 clear dcp speed limit rules.....	4-4
4.9 debug dcp packet.....	4-5
4.10 debug dcp event.....	4-6
Chapter 5 COMMANDS FOR COPP.....	5-1
5.1 copp-policy-map.....	5-1
5.2 service-policy output.....	5-1
5.3 show policy-map.....	5-2
5.4 policy packets-per-second.....	5-2
5.5 policy.....	5-4

Chapter 1 Commands for Show

1.1 clear history all-users

Command: clear history all-users

Function: Clear the command history of all users saved by the switch.

Command Mode: Admin mode

Usage Guide: Using this command can clear the command history of all users.

Example:

```
Switch#clear history all-users
```

1.2 history all-users max-length

Command: history all-users max-length <count>

Function: Set the max command history of all users saved by the switch.

Parameter: <count>: the command history number can be saved, ranging from 100 to 1000

Command Mode: Global mode

Usage Guide: The system can save 100 recent command history of all users at best by default, using this command can set the max command history number.

Example:

```
Switch(config)#history all-users max-length 500
```

1.3 logging executed-commands

Command: logging executed-commands {enable | disable}

Function: Enable or disable the logging executed-commands.

Parameter: None.

Command Mode: Global mode.

Default: Disable state.

Usage Guide: After enable this command, the commands executed by user at the console, telnet or ssh terminal will record the log.

Example: Enable the command executed by user.

```
Switch(Config)#logging executed-commands enable
```

1.4 ping

Command: ping [[src <source-address>] { <destination-address> | host <hostname> }]

Function: Issue ICMP request to remote devices, check whether the remote device can be reached by the switch.

Parameters: <source-address> is the source IP address where the ping command is issued, with IP address in dotted decimal format. <destination-address> is the target IP address of the ping command, with IP address in dotted decimal format. <hostname> is the target host name of the ping command, which should not exceed 64 characters.

Default: 5 ICMP echo requests will be sent. The default packet size and time out is 56 bytes and 2 seconds.

Command Mode: Admin mode

Usage Guide: When the ping command is entered without any parameters, interactive configuration mode will be invoked. And ping parameters can be entered interactively.

Example:

Example 1: To ping with default parameters.

```
Switch#ping 10.1.128.160
```

Type ^c to abort.

Sending 5 56-byte ICMP Echos to 10.1.128.160, timeout is 2 seconds.

```
...!!
```

Success rate is 40 percent (2/5), round-trip min/avg/max = 0/0/0 ms

In the example above, the switch is made to ping the device at 10.1.128.160. The command did not receive ICMP reply packets for the first three ICMP echo requests within default 2 seconds timeout. The ping failed for the first three tries. However, the last two ping succeeded. So the success rate is 40%. It is denoted on the switch "." for ping failure which means unreachable link, while "!" for ping success, which means reachable link.

Example 2: Use ping command with source address configuration, and leave other fields to default.

```
Switch#ping src 10.1.128.161 10.1.128.160
```

Type ^c to abort.

Sending 5 56-byte ICMP Echos to 10.1.128.160, using source address 10.1.128.161, timeout is 2 seconds.

```
!!!!
```

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

In the example above, 10.1.128.161 is configured as the source address of the ICMP

echo requests, while the destination device is configured to be at 10.1.128.160. The command receives all the ICMP reply packets for all of the five ICMP echo requests. The success rate is 100%. It is denoted on the switch “.” for ping failure which means unreachable link, while “!” for ping success, which means reachable link.

Example 3: Ping with parameters entered interactively.

Switch#ping

VRF name :

Target IP address: 10.1.128.160

Use source address option[n]: y

Source IP address: 10.1.128.161

Repeat count [5]: 100

Datagram size in byte [56]: 1000

Timeout in milli-seconds [2000]: 500

Extended commands [n]: n

Display Information	Explanation
VRF name	VRF name. If MPLS is not enabled, this field will be left empty.
Target IP address :	The IP address of the target device.
Use source address option[n]	Whether or not to use ping with source address.
Source IP address	To specify the source IP address for ping.
Repeat count [5]	Number of ping requests to be sent. The default value is 5.
Datagram size in byte [56]	The size of the ICMP echo requests, with default as 56 bytes.
Timeout in milli-seconds [2000]:	Timeout in milli-seconds, with default as 2 seconds.
Extended commands [n]:	Whether or to use other extended options.

1.5 ping6

Command: ping6 [<dst-ipv6-address> | host <hostname> | src <src-ipv6-address> {<dst-ipv6-address > | host <hostname>}]

Function: To check whether the destination network can be reached.

Parameters: *<dst-ipv6-address>* is the target IPv6 address of the ping command. *<src-ipv6-address>* is the source IPv6 address where the ping command is issued. *<hostname>* is the target host name of the ping command, which should not exceed 64 characters.

Default: Five ICMP6 echo request will be sent by default, with default size as 56 bytes, and default timeout to be 2 seconds.

Command Mode: Normal user mode

Usage Guide: When the ping6 command is issued with only one IPv6 address, other parameters will be default. And when the ipv6 address is a local data link address, the name of VLAN interface should be specified. When the source IPv6 address is specified, the command will fill the icmp6 echo requests with the specified source address for ping.

Example:

(1) To issue ping6 command with default parameters.

```
Switch>ping6 2001:1:2::4
```

Type ^c to abort.

Sending 5 56-byte ICMP Echos to 2001:1:2::4, timeout is 2 seconds.

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/320/1600 ms

(2) To issue the ping6 command with source IPv6 address specified.

```
switch>ping6 src 2001:1:2::3 2001:1:2::4
```

Type ^c to abort.

Sending 5 56-byte ICMP Echos to 2001:1:2::4, using src address 2001:1:2::3, timeout is 2 seconds.

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

(3) To issue the ping6 command with parameters input interactively.

```
switch>ping6
```

Target IPv6 address:fe80::2d0:59ff:feb8:3b27

Output Interface: vlan1

Use source address option[n]:y

Source IPv6 address: fe80::203:fff:fe0b:16e3

Repeat count [5]:

Datagram size in byte [56]:

Timeout in milli-seconds [2000]:

Extended commands [n]:

Type ^c to abort.

Sending 5 56-byte ICMP Echos to fe80::2d0:59ff:feb8:3b27, using src address fe80::203:fff:fe0b:16e3, timeout is 2 seconds.

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms

Display Information	Explanation
ping6	The ping6 command
Target IPv6 address	The target IPv6 address of the command.
Output Interface	The name of the VLAN interface, which should be specified when the target address is a local data link address.
Use source IPv6 address [n]:	Whether or not use source IPv6 address. Disabled by default.
Source IPv6 address	Source IPv6 address.
Repeat count[5]	Number of the ping packets.
Datagram size in byte[56]	Packet size of the ping command. 56 byte by default.
Timeout in milli-seconds[2000]	Timeout for ping command. 2 seconds by default.
Extended commands[n]	Extended configuration. Disabled by default.
!	The network is reachable.
.	The network is unreachable.
Success rate is 100 percent(8/8), round-trip min/avg/max = 1/1/1ms	Statistic information, success rate is 100 percent of ping packet.

1.6 show boot-files

This command is not supported by the switch.

1.7 show debugging

Command: show debugging {bgp | dvmrp | igmp | ipv6 | mld | nsm | ospf | other | pim | rip | spanning-tree | vrrp}

Function: Display the debug switch status.

Usage Guide: If the user needs to check what debug switches have been enabled, **show debugging** command can be executed.

Command mode: Admin Mode

Example: Check for currently enabled debug switch.

Switch#show debugging ospf

OSPF debugging status:

```

OSPF all IFSM debugging is on
OSPF packet Hello detail debugging is on
OSPF packet Database Description detail debugging is on
OSPF packet Link State Request detail debugging is on
OSPF packet Link State Update detail debugging is on
OSPF packet Link State Acknowledgment detail debugging is on
OSPF all LSA debugging is on
OSPF all NSM debugging is on
OSPF all events debugging is on
OSPF all route calculation debugging is on

```

Switch#

Relative command: debug

1.8 show fan

This command is not supported by switch.

1.9 show flash

Command: show flash

Function: Show the size of the files which are reserved in the system flash memory.

Command Mode: Admin Mode and Configuration Mode.

Example: To list the files and their size in the flash.

Switch#show flash

```

boot.rom                329, 828 1900-01-01 00:00:00 --SH
boot.conf                94 1900-01-01 00:00:00 --SH
nos.img                  2, 449, 496 1980-01-01 00:01:06 ----
startup-config           2, 064 1980-01-01 00:30:12 ----

```

1.10 show history

Command: show history

Function: Display the recent user command history.

Command mode: Admin Mode

Usage Guide: The system holds up to 20 commands the user entered, the user can use the UP/DOWN key or their equivalent (ctrl+p and ctrl+n) to access the command history.

Example:

```
Switch#show history
enable
config
interface ethernet 1/0/3
enable
dir
show ftp
```

1.11 show history all-users

Command: show history all-users [detail]

Function: Show the recent command history of all users.

Parameter: [detail] shows user name of the executing command. IP address of the user will be shown when logging in the executing command through Telnet or SSH.

Command Mode: Admin and configuration mode

Usage Guide: This command is used to show the recent command history of all users, including time, logging type, executing command, etc.

Notice: The user can only check the command history of other users whose purview should not be higher than oneself.

Example:

```
Switch(config)#show history all-users detail
```

Time	Type	User	Command
0w 0d 0h 2m	Telnet/SSH	admin	show history all-users detail 192.168.1.2:1419
0w 0d 0h 1m	Telnet/SSH	admin	show history all-users 192.168.1.2:1419
0w 0d 0h 1m	Console	Null	show history all-users
0w 0d 0h 1m	Console	Null	end
0w 0d 0h 1m	Console	Null	ip address 192.168.1.1 255.255.255.0
0w 0d 0h 0m	Console	Null	in v 1
0w 0d 0h 0m	Console	Null	telnet-server enable

1.12 show logging executed-commands state

Command: show logging executed-commands state

Function: Show the state of logging executed-commands.

Parameter: None.

Command Mode: Admin mode.

Default: None.

Usage Guide: Use this command to display the state (enable or disable).

Example:

```
Switch#show logging executed-commands state
Logging executed command state is enable
```

1.13 show memory

Command: show memory [usage]

Function: Display the contents in the memory.

Parameter: usage means memory use information.

Command mode: Admin Mode

Usage Guide: This command is used for switch debug purposes. The command will interactively prompt the user to enter start address of the desired information in the memory and output word number. The displayed information consists of three parts: address, Hex view of the information and character view.

Example:

```
Switch#show memory
start address : 0x2100
number of words[64]:
```

```
002100:  0000 0000 0000 0000  0000 0000 0000 0000  *.....*
002110:  0000 0000 0000 0000  0000 0000 0000 0000  *.....*
002120:  0000 0000 0000 0000  0000 0000 0000 0000  *.....*
002130:  0000 0000 0000 0000  0000 0000 0000 0000  *.....*
002140:  0000 0000 0000 0000  0000 0000 0000 0000  *.....*
002150:  0000 0000 0000 0000  0000 0000 0000 0000  *.....*
002160:  0000 0000 0000 0000  0000 0000 0000 0000  *.....*
002170:  0000 0000 0000 0000  0000 0000 0000 0000  *.....*
```

1.14 show running-config

Command: show running-config

Function: Display the current active configuration parameters for the switch.

Default: If the active configuration parameters are the same as the default operating parameters, nothing will be displayed.

Command mode: Admin Mode

Usage Guide: When the user finishes a set of configuration and needs to verify the configuration, show running-config command can be used to display the current active parameters.

Example:

```
Switch#show running-config
```

1.15 show running-config current-mode

Command: show running-config current-mode

Function: Show the configuration under the current mode.

Command mode: All configuration modes.

Default: None.

Usage Guide: Enter into any configuration mode and input this command under this mode, it can show all the configurations under the current mode.

Example:

```
Switch(config-if-ethernet1/0/1)#show run c
```

```
!
```

```
Interface Ethernet1/0/1  
switchport access vlan 2
```

```
!
```

1.16 show startup-config

Command: show startup-config

Function: Display the switch parameter configurations written into the Flash memory at the current operation; those are usually also the configuration files used for the next power-up.

Default: If the configuration parameters read from the Flash are the same as the default operating parameter, nothing will be displayed.

Command mode: Admin Mode

Usage Guide: The **show running-config** command differs from **show startup-config** in that when the user finishes a set of configurations, **show running-config** displays the added-on configurations whilst **show startup-config** won't display any configurations. However, if **write** command is executed to save the active configuration to the Flash

memory, the displays of **show running-config** and **show startup-config** will be the same.

1.17 show switchport interface

Command: **show switchport interface [ethernet <IFNAME>]**

Function: Show the VLAN port mode, VLAN number and Trunk port messages of the VLAN port mode on the switch.

Parameter: <IFNAME> is the port number.

Command mode: Admin mode

Example: Show VLAN messages of port ethernet 1/0/1.

```
Switch#show switchport interface ethernet 1/0/1
```

```
Ethernet1/0/1
```

```
Type :Universal
```

```
Mac addr num : No limit
```

```
Mode :Trunk
```

```
Port VID :1
```

```
Trunk allowed Vlan :ALL
```

Displayed Information	Description
Ethernet1/0/1	Corresponding interface number of the Ethernet.
Type	Current interface type.
Mac addr num	Numbers of interfaces with MAC address learning ability.
Mode: Trunk	Current interface VLAN mode.
Port VID :1	Current VLAN number the interface belongs.
Trunk allowed Vlan :ALL	VLAN permitted by Trunk.

1.18 show tcp

Command: **show tcp**

Function: Display the current TCP connection status established to the switch.

Command mode: Admin Mode

Example:

```
Switch#show tcp
```

LocalAddress	LocalPort	ForeignAddress	ForeignPort	State
0.0.0.0	23	0.0.0.0	0	LISTEN
0.0.0.0	80	0.0.0.0	0	LISTEN

Displayed information	Description
LocalAddress	Local address of the TCP connection.
LocalPort	Local port number of the TCP connection.
ForeignAddress	Remote address of the TCP connection.
ForeignPort	Remote port number of the TCP connection.
State	Current status of the TCP connection.

1.19 show tcp ipv6

Command: show tcp ipv6

Function: Show the current TCP connection.

Command mode: Admin and configuration mode.

Example:

Switch#show tcp ipv6

LocalAddress	LocalPort	RemoteAddress	RemotePort	State
IF VRF				
::	80	::	0	LISTEN
0 0				
::	23	::	0	LISTEN
0 0				

Displayed Information	Explanation
LocalAddress	Local IPv6 address of TCP connection
LocalPort	Local port of TCP connection
RemoteAddress	Remote IPv6 address of TCP connection
RemotePort	Remote Port of TCP connection
State	The current state of TCP connection
IF	Local port index of TCP connection
VRF	Virtual route forward instance

1.20 show telnet login

Command: show telnet login

Function: List information of currently available telnet clients which are connected to the switch.

Command Mode: Admin Mode and Configuration Mode.

Usage Guide: This command used to list the information of currently available telnet clients which are connected to the switch.

Example:

```
Switch#show telnet login
Authenticate login by local.
Login user:
aa
```

1.21 show temperature

Command: show temperature

Function: Show the temperature of the CPU.

Parameters: None.

Command Mode: Any modes

Usage Guide: This command can be used to monitor the CPU temperature of the switch.

Example: Show the temperature of the CPU of the switch.

```
Switch(Config)#show temperature
Temperature: 47.0625 度
```

1.22 show tech-support

Command: show tech-support

Function: Display various information about the switch and the running tasks. This command is used to diagnose the switch by the technical support specialist.

Command Mode: Admin mode and configuration mode

Usage Guide: When failure occurred on the switch, this command can be used to get related information, in order to diagnose the problems.

Example:

```
Switch#show tech-support
```

1.23 show udp

Command: show udp

Function: Display the current UDP connection status established to the switch.

Command mode: Admin Mode

Example:

Switch#show udp

LocalAddress	LocalPort	ForeignAddress	ForeignPort	State
0.0.0.0	161	0.0.0.0	0	CLOSED
0.0.0.0	123	0.0.0.0	0	CLOSED
0.0.0.0	1985	0.0.0.0	0	CLOSED

Displayed information	Description
LocalAddress	Local address of the UDP connection.
LocalPort	Local port number of the UDP connection.
ForeignAddress	Remote address of the UDP connection.
ForeignPort	Remote port number of the UDP connection.
State	Current status of the UDP connection.

1.24 show udp ipv6

Command: show udp ipv6

Function: Show the current UDP connection.

Command mode: Admin and configuration mode.

Example:

LocalAddress	LocalPort	RemoteAddress	RemotePort	State
::	69	::	0	CLOSED
::	1208	::	0	CLOSED

Displayed Information	Explanation
LocalAddress	Local IPv6 address of UDP connection
LocalPort	Local port of UDP connection
RemoteAddress	Remote IPv6 address of UDP connection
RemotePort	Remote Port of UDP connection
State	The current state of UDP connection

1.25 show version

Command: show version

Function: Display the switch version.

Command mode: Admin Mode

Usage Guide: Use this command to view the version information for the switch, including hardware version and software version.

Example:

```
Switch#show version
```

1.26 traceroute

Command: traceroute [source <ipv4-addr>] { <ip-addr> | host <hostname> } [hops <hops>] [timeout <timeout>]

Function: This command is tests the gateway passed in the route of a packet from the source device to the target device. This can be used to test connectivity and locate a failed sector.

Parameter: <ipv4-addr> is the assigned source host IPv4 address in dot decimal format. <ip-addr> is the target host IP address in dot decimal format. <hostname> is the hostname for the remote host. <hops> is the maximum gateway number allowed by Traceroute command. <timeout> Is the timeout value for test packets in milliseconds, between 100 -10000.

Default: The default maximum gateway number is 30, timeout in 2000 ms.

Command mode: Admin Mode

Usage Guide: Traceroute is usually used to locate the problem for unreachable network nodes.

1.27 traceroute6

Command: traceroute6 [source <addr>] {<ipv6-addr> | host <hostname>} [hops <hops>] [timeout <timeout>]

Function: This command is for testing the gateways passed by the data packets from the source device to the destination device, so to check the accessibility of the network and further locating the network failure.

Parameter: <addr> is the assigned source host IPv6 address in colonned hex notation.

<ipv6-addr> is the IPv6 address of the destination host, shown in colonned hex notation; **<hostname>** is the name of the remote host; **<hops>** is the max number of the gateways the traceroute6 passed through, ranging between 1-255; **<timeout>** is the timeout period of the data packets, shown in millisecond and ranging between 100~10000.

Default: Default number of the gateways passes by the data packets is 30, and timeout period is defaulted at 2000ms.

Command Mode: Admin Mode

Usage Guide: Traceroute6 is normally used to locate destination network inaccessible failures.

Example:

```
Switch# traceroute6 2004:1:2:3::4
```

Relevant Command: ipv6 host

Chapter 2 Commands for Reload Switch after Specified Time

2.1 reload after

Command: reload after {[<HH:MM:SS>] [days <days>]}

Function: Reload the switch after a specified period of time.

Parameters: <HH:MM:SS> the specified time, HH (hours) ranges from 0 to 23, MM (minutes) and SS (seconds) range from 0 to 59.

<days> the specified days, unit is day, range from 1 to 30.

time and day may be configured at the same time or configured solely.

Command Mode: Admin mode

Usage Guide: With this command, users can reboot the switch without shutdown its power after a specified period of time, usually when updating the switch version. The switch can be rebooted after a period of time instead of immediately after its version being updated successfully. This command will not be reserved, which means that it only has one-time effect. After this command is configured, it will prompt the reboot information when user logging in the switch by telnet.

Example: Set the switch to automatically reload after 2 days, 10 hours and 1 second.

```
Switch#reload after 10:00:01 days 2
```

```
Process with reboot after? [Y/N] y
```

Related Commands: reload, reload cancel, show reload

2.2 reload cancel

Command: reload cancel

Function: Cancel the specified time period to reload the switch.

Parameters: None

Command Mode: Admin mode.

Usage Guide: With this command, users can cancel the specified time period to reload the switch, that is, to cancel the configuration of command "reload after". This command will not be reserved.

Example: Prevent the switch to automatically reboot after the specified time.

```
Switch#reload cancel
```

Reload cancel successful.

Related Commands: reload, reload after, show reload

2.3 show reload

Command: show reload

Function: Display the user's configuration of command "reload after".

Parameters: None.

Command Mode: Admin and configuration mode

Usage Guide: With this command, users can view the configuration of command "reload after" and check how long a time is left before rebooting the switch.

Example: View the configuration of command "reload after". In the following case, the user set the switch to be rebooted in 10 hours and 1 second, and there are still 9 hours 59 minutes and 48 seconds left before rebooting it.

Switch#show reload

The original reload after configuration is 10:00:01.

System will be rebooted after 09:59:48 from now.

Related Commands: reload, reload after, reload cancel

Chapter 3 Commands for Debugging and Diagnosis for Packets Received and Sent by CPU

3.1 clear cpu-rx-stat protocol

Command: clear cpu-rx-stat protocol[<protocol-type>]

Function: Clear the statistics of the CPU received packets of the protocol type.

Parameter: <protocol-type> is the type of the protocol of the packet, including dot1x, stp, snmp, arp, telnet, http, dhcp, igmp, ssh, bgp, bgp4plus, rip, ripng, ospf, ospfv3, pim, pimv6, unknown-mcast, unknow-mcast6, mld

Command Mode: Global Mode

Usage Guide: This command clear the statistics of the CPU received packets of the protocol type, it is supposed to be used with the help of the technical support.

Example: Clear the statistics of the CPU receives ARP packets.

```
Switch(config)#clear cpu-rx-stat protocol arp
```

3.2 cpu-rx-limitnotify enable interval

Command: cpu-rx-limitnotify enable interval<180-86400>
no cpu-rx-limitnotify enable

Function: Enable cpu-rxlimitnotify function and specified the time interval of trigger. The no command disables cpu-rxlimitnotify function.

Parameters: *interval* interval time, the default time is 86400s.

Command Mode: Configuration mode.

Usage Guide: This command used for diagnosing protocol information that switch received. Please using under the guidance of manufacturer technical staff

Example:

```
Switch(config)#cpu-rx-limitnotify enable interval 180
```

3.3 cpu-rx-limitnotify protocol

(all|WORD)(enable|disable)

Command: `cpu-rx-limitnotify protocol (all|WORD)(enable|disable)`

Function: Open or close all protocols or specified protocols. After open, cpu-rx-limitnotify detected cpu-rx happened deny in interval period, sending the deny amount in the time to users by snmp trap.

Command Mode: Configuration mode.

Example:

Close all protocols

```
Switch(config)# cpu-rx-limitnotify protocol all disable
```

Open all protocols

```
Switch(config)# cpu-rx-limitnotify protocol all enable
```

Open specified protocols

```
Switch(config)# cpu-rx-limitnotify protocol snmp enable
```

Close specified protocols

```
Switch(config)# cpu-rx-limitnotify protocol snmp disable
```

3.4 cpu-rx-ratelimit channel

This command is not supported by the switch.

3.5 cpu-rx-ratelimit enhanced

This command is not supported by the switch.

3.6 cpu-rx-ratelimit protocol

Command: `cpu-rx-ratelimit protocol <protocol-type> <packets>`

`no cpu-rx-ratelimit protocol <protocol-type>`

Function: Set the max rate of the CPU receiving packets of the protocol type, the no command set the max rate to default.

Parameter: `<protocol-type>` is the type of the protocol, including dot1x, stp, snmp, arp, telnet, http, dhcp, igmp, ssh, bgp, bgp4plus, rip, ripng, ospf, ospfv3, pim, pimv6, unknown-mcast, unknow-mcast6, mld; `<packets>` is the max rate of CPU receiving

packets of the protocol type, its range is 1-2000 pps.

Command Mode: Global Mode

Default: A different default rate is set for the different type of protocol.

Usage Guide: The rate limit set by this command have an effect on CPU receiving packets, so it is supposed to be used with the help of the technical support.

Example: Set the rate of the ARP packets to 500pps.

Switch(config)#cpu-rx-ratelimit protocol arp 500

3.7 cpu-rx-ratelimit queue-length

This command is not supported by the switch.

3.8 cpu-rx-ratelimit total

Command: `cpu-rx-ratelimit total <packets>`

`no cpu-rx-ratelimit total`

Function: Set the total rate of the CPU receiving packets, the no command sets the total rate of the CPU receiving packets to default.

Parameter: <packets> is the max number of CPU receiving packets per second.

Command Mode: Global Mode

Default: 1200pps.

Usage Guide: The total rate set by the command have an effect on CPU receiving packets, so it is supposed to be used with the help of the technical support.

Example: Set the total rate of the CPU receive packets to 1500pps.

Switch(config)#cpu-rx-ratelimit total 1500

3.9 debug driver

Command: `debug driver {receive | send} [interface {<interface-name> | all}] [protocol {<protocol-type> | discard | all}] [detail]`

`no debug driver {receive | send}`

Function: Turn on the on-off of showing the information of the CPU receiving or sending packets, the “no debug driver {receive | send}” command turns off the on-off.

Parameter: receive | send show the information of receiving or sending packets;

interface {<interface-list>| all}: interface-list is the Ethernet port number, all indicate all the Ethernet ports.

protocol {<protocol-type> | discard | all}: protocol-type is the type of the protocol of the packet, including snmp, telnet, http, dhcp, igmp, hsrp, arp, bgp, rip, ospf, pim, ssh, vrrp, ripng, ospfv3, pimv6, icmpv6, bgp4plus, unknown-mcast, unknown-mcast6, ttl0-2cpu, isis, dot1x, gvrp, stp, lacp, cluster, mld, vrrpv3, ra, uldp, lldp, eapou **all** means all of the protocol types, **discard** means all the discarded packets. **Detail** show detail information.

Command Mode: Admin Mode

Usage Guide: This command is used to debug, it is supposed to be used with the help of the technical support.

Example: Turn on the on-off for showing the receiving packets.

Switch#debug driver receive

3.10 protocol filter

Command: protocol filter {protocol-type}

no Protocol filter {protocol-type}

Function: Turn on/off the corresponding treatment of the named protocol packets.

Parameter: <protocol-type> stands for protocol type, it can be configured:

{arp|bgp|dhcp|dhcpv6|hsrp|http|igmp|ip|ldp|mpls|ospf|pim|rip|snmp|telnet|vrrp}

Command Mode: Admin Mode

Usage Guide: This command turns on/off the corresponding treatment of the named protocol packets, and it is used to debug and diagnose the switch. Please use it with direction of the manufacturers technical personnel.

Example: Turn on the treatment of the arp protocol packets.

Switch#protocol filter arp

3.11 show cpu-rx protocol

Command: show cpu-rx protocol [<protocol-type>]

Function: Show the statistics of the CPU received packets of the specified protocol type.

Parameter: <protocol-type> is the protocol type of the packets, if do not input parameters, show all statistic packets.

Command Mode: Admin and configuration mode

Default: None.

Usage Guide: This command is used to debug, it is supposed to be used with the help of the technical support.

Example: Show the statistics of CPU receiving ARP packets.

Switch#show cpu-rx protocol arp

Type	Rate-limit	TotPkts	CurState
arp	500	3	allowed

Chapter 4 Commands for DCP

4.1 dcp enable

Command: dcp enable

Function: This command is used to enable the dcp function.

Parameters: None.

Default: Disable.

Command Mode: Global Configuration Mode.

Usage Guide: dcp enable is used to enable the dcp function. After enabled this command, the rate that IP packets going on CPU will be counted and limited. The device can stop the other-ipuc packets whose flow is too large dynamically and protect the CPU. The type of other-ipuc packet is that the destination mac is the one of CPU, the destination ip is the one which can not achieved and is in the same network segment with the ip that it is not this interface. For example, the mac address of the CPU of switch is 00-03-0f-ff-3e-1e, there is interface vlan 1 on the switch and the address is 10.1.1.1, the address of interface vlan 10 is 20.1.1.1. So, the destination mac from interface vlan 1 is 00-03-0f-ff-3e-1e, the destination ip is 20.1.1.x and the packets that the ip cannot achieve will be distinguished as other-ipuc packets.

Example: Enable the dcp function.

```
Switch(Config)# dcp enable
```

4.2 dcp disable

Command: dcp disable

Function: Disable the dcp function.

Parameters: None.

Default: Disable.

Command Mode: Global Configuration Mode.

Usage Guide: The command of dcp disable is used to disable the dcp function. After the command is effective, the dcp function of the device will be disabled. All the configurations of dcp will be cleared.

Example: Disable the dcp function.

```
Switch(Config)#dcp disable
```

4.3 dcp limit-rate <20-50>

Command: dcp limit-rate <20-50>

no dcp limit-rate

Function: Configure the limit-rate value of dcp. The no command cancels it and recovers it to be the default value.

Parameters: <20-50> is the limit-rate value.

Default: 20.

Command Mode: Global Configuration Mode.

Usage Guide: After configured the limit-rate value, if the rate of ip going on CUP is larger than this value, conduct the rate limiting. The limit-rate is 20-50. When the number of packets is smaller than the half of the configured limit-rate in 5s, the rate limiting will be canceled.

Example: Configure the global limit-rate as 50.

```
Switch(Config)# dcp limit-rate 50
```

Cancel the configuration of the limit-rate and recover it to be the default value of 20.

```
Switch(Config)# no dcp limit-rate
```

4.4 dcp no-limit-ip <ip_addr>

Command: dcp no-limit-ip <ip_addr>

no dcp no-limit-ip <ip_addr>

Function: Configure the IP that the dcp does not limit its rate. The no command cancels it.

Parameters: <ip_addr> is the appointed IP address.

Default: Limit rate for all IP after enabled dcp.

Command Mode: Global Configuration Mode.

Usage Guide: After configured not to limit the rate for the specific IP, dcp will not limit rate for this IP, but for other IP, the rate limiting is still effective. The no command cancels this configuration and recovers to be rate limiting. This command can configure the maximum value as 1024, it cannot be issued when exceeds this value.

Example: dcp does not limit rate for 1.1.1.1.

```
Switch(Config)# dcp no-limit-ip 1.1.1.1
```

Cancel the above configuration and recover to be rate limiting.

```
Switch(Config)# no dcp no-limit-ip 1.1.1.1
```

4.5 show dcp limit-rate

Command: show dcp limit-rate

Function: Show the limit-rate configured by user.

Parameters: None.

Command Mode: Global and Admin Mode.

Usage Guide: Show the limit-rate configured by user.

Example:

```
Switch(config)#show dcp limit-rate
DCP limit rate is 50.
```

4.6 show cpu ip rate top10

Command: show cpu ip rate top10 [slot <1-9>|member <1-16>]

Function: Show the first 10 IP with the maximum rate of going on cpu in 5s and show the limit-rate value.

Parameters: slot<1-9> is the slot id, member<1-16> is the member number.

Command Mode: Global and Admin Mode.

Usage Guide: Show the first 10 IP with the maximum rate of going on cpu in 5s and show the limit-rate value.

Example:

```
Switch(config)#show cpu ip rate top10
-----member:16-----
```

```
-----
No.   IP                               Rate(pkts/s)
-----
1     11.11.11.21                       5s    96
2     11.11.11.12                       5s    52
3     11.11.11.13                       5s    50
4     11.11.11.11                       5s    39
5     11.11.11.14                       5s    24
6     11.11.11.15                       5s    21
7     11.11.11.20                       5s    12
8     11.11.11.17                       5s     8
9     11.11.11.16                       5s     8
10    11.11.11.19                       5s     7
```

-----member:10-----

No. IP Rate(pkts/s)

4.7 show dcp limited ip

Command: show dcp limited ip [slot <1-9>|member <1-16>]

Function: Show the node information of the ip which is limited the rate.

Parameters: slot<1-9> is the slot id, member<1-16> is the member number.

Command Mode: Global and Admin Mode.

Usage Guide: Show the node information of the ip which is limited the rate.

Example:

Switch(config)#show dcp limited ip

-----member:16-----

No. Limited-IP Rate(pkts/s)

1	11.11.11.16	1s	64
2	11.11.11.13	1s	61
3	11.11.11.19	1s	3
4	11.11.11.17	1s	3
5	11.11.11.14	1s	6
6	11.11.11.12	1s	26
7	11.11.11.11	1s	34
8	11.11.11.21	1s	51

-----member:10-----

No. Limited-IP Rate(pkts/s)

4.8 clear dcp speed limit rules

Command: clear dcp speed limit rules {member <1-16>}

Function: Clear the rate limiting rule that the DCP sent to the drive.

Parameters: member<1-16> is the member number.

Command Mode: Admin Mode.

Usage Guide: Clear the rate limiting rule that the DCP sent to the drive. User can appoint the slot id or ip.

Example:

Clear all the rate limiting rules that the DCP sent including all the slots and ip.

```
Switch#clear dcp speed limit rules
```

Clear all of the speed limit rules successfully!

Clear the rate limiting rules that the DCP sent of member 16.

```
Switch#clear dcp speed limit rules member 16
```

Clear all of the speed limit rules successfully!

Clear the rate limiting rule that the DCP sent to the IP of 1.1.1.1.

```
Switch#clear dcp speed limit rules ip 11.11.11.14
```

Clear the speed limit rules of [11.11.11.14] successfully!

4.9 debug dcp packet

Command: debug dcp packet

no debug dcp packet

Function: Show the process that the DCP deals with and monitor the packet going up the CPU, the no command cancels printing.

Parameters: None.

Command Mode: Admin Mode.

Usage Guide: When user wants to know the situation of each packet received by dcp, please use this command to view the detailed information including source IP, destination IP, source port, destination port, protocol number, etc.

Example:

```
Switch#debug dcp packet
```

```
Switch#packet DCP_PKT debug is on
```

```
Switch#%Jan 01 08:12:05 2006 %DCP-PKT:Receive a packet:
```

source ip	dest ip	source mac	dest mac
source port	dest port	protocol	
11.11.11.21	20.1.1.21	00-00-0b-00-02-0b	00-03-0f-29-28-3e
0	84		0

```
%Jan 01 08:12:05 2006 %DCP-PKT:Receive a packet:
```

source ip	dest ip	source mac	dest mac
source port	dest port	protocol	
11.11.11.20	20.1.1.20	00-00-0b-00-02-0a	00-03-0f-29-28-3e
			0

0

86

4.10 debug dcp event

Command: debug dcp event

no debug dcp event

Function: Show the process that the DCP deals with the events. The no command cancels printing.

Parameters: None.

Command Mode: Admin Mode.

Usage Guide: When user wants to know the detailed information of the IP rate limiting, please use this command to view.

Example:

```
Switch#debug dcp event
```

```
Switch#event DCP_EVENT debug is on
```

```
Switch#%Jan 01 08:17:21 2006 %DCP-EVENT:Current ip info node num is: [11].
```

```
%Jan 01 08:17:27 2006 %DCP-EVENT:The current rate of [11.11.11.19] is 57pkts/s, out of the limited value(50)!
```

```
%Jan 01 08:17:27 2006 %DCP-EVENT:[11.11.11.19] is denied successful by drv!
```

```
%Jan 01 08:17:27 2006 %DCP-EVENT:[11.11.11.19] is added to deny list.
```

```
%Jan 01 08:17:27 2006 DCP:The current rate of [11.11.11.19] is 57pkts/s, out of the limited value(50). DCP denies it successfully!
```

```
%Jan 01 08:17:27 2006 %DCP-EVENT:The current rate of [11.11.11.20] is 60pkts/s, out of the limited value(50)!
```

```
%Jan 01 08:17:27 2006 %DCP-EVENT:[11.11.11.20] is denied successful by drv!
```

```
%Jan 01 08:17:27 2006 %DCP-EVENT:[11.11.11.20] is added to deny list.
```

Chapter 5 Commands for COPP

5.1 copp-policy-map

Command: `copp-policy-map <policy-map name>`
`no policy-map <policy-map-name>`

Function: Create a copp-policy-map and enter the copp-policy-map mode. The no command deletes the appointed copp-policy-map.

Parameters: `<policy-map-name>` is the name of the policy map.

Default: There is no copp-policy-map as default.

Command Mode: Global Configuration Mode.

Usage Guide: Create the copp-policy-map under the global mode and enter the copp-policy-map mode, user can conduct to classify and match.

Example: Create and delete the copp-policy-map whose name is p1.

```
Switch(config)#copp-policy-map p1
```

```
Switch(config-copp-policy-map-p1)#exit
```

```
Switch(config)#no policy-map p1
```

5.2 service-policy output

Command: `service-policy output <policy-map name>`
`no service-policy output <policy-map-name>`

Function: Apply a policy map to the egress of the port. The no command deletes the policy map.

Parameters: `output <policy-map-name>`: Apply the policy map with the appointed name to the egress of the port.

Default: There is no policy map bound.

Command Mode: Port Mode.

Usage Guide: When the copp policy map is bound to the egress of the port, finally it is bound to the cpu port actually and it is effective on the cpu port, it cannot affect the egress of the port. Only one policy map can be applied to each direction of each port, the ingress does not support the policy map.

Example: Bind the p1 to the egress of ethernet1/0/1.

```
Switch(config)#interface ethernet 1/0/1
```

```
Switch(config-if-ethernet1/0/1)# service-policy output p1
```

5.3 show policy-map

Command: `show policy-map <policy-map-name>`

Function: Show the policy-map information of QoS.

Parameters: `<policy-map-name>` is the name of the policy map.

Default: None.

Command Mode: Admin and Configuration Mode.

Usage Guide: Show the information of all the configured copp-policy-map or the appointed copp-policy-map.

Example:

```
Switch#show policy-map
```

```
COPP Policy Map p1, used by 1 time(s)
```

```
  Class Map name: c1
    policy CIR: 10 CBS: 11
    exceed-action:
      drop
```

```
COPP Policy Map p2, used by 0 time(s)
```

```
  Class Map name: c1
    Drop
```

```
Switch#show policy-map p1
```

```
COPP Policy Map p1, used by 1 time(s)
```

```
  Class Map name: c1
    policy CIR: 10 CBS: 11
    exceed-action:
      drop
```

5.4 policy packets-per-second

Command: `policy packets-per-second <pps> normal-burst-packets <pps>`
`{ conform-action | exceed-action } <ACTION>`
`no policy`

ACTION definition:

```
      drop | transmit | policied-intp-transmit {drop|transmit|
set-internal-priority } | set-internal-priority <inp_value> {drop|transmit|
```

policied-intp-transmit }

Function: It supports the policy command of single bucket two colors and the limit-rate is pps mode, divide the packets into different colors according to the configuration, and set the corresponding action for different color packets. The no operation will delete the mode configuration.

Parameters:

packets-per-second: The committed information rate – CIR (Committed Information Rate), in pps, ranging from 1 to 12800, when the configured value exceeds the max limit of the chip, CLI prompts the error information;

normal-burst-packets: The committed burst size – CBS (Committed Burst Size), in pps, ranging from 1 to 12800, when the configured value exceeds the max limit of the chip, CLI prompts the error information;

conform-action: The actions to take when the CIR is not exceeded, which means the messages are green, the default as transmit;

exceed-action: The actions to take when the CIR is exceeded, which means the messages are red, the default as drop.

ACTION include:

drop/transmit: Drop/transmit the packets;

policied-intp-transmit: sends the packets whose internal priority mapping is changed through qos policy;

set-internal-priority: sets the internal priority of the packets.

Command Mode: Policy class map configuration Mode.

Default: No policy action; the default action of conform-action is transmit, the default action of exceed-action is drop.

Usage Guide: This command is used to configure the policy actions. Pps limit-rate only supports single rate single bucket, it supports double colors packets and it can configure the policy actions for the packets with different colors.

Example: In the policy class table configuration mode, set the CIR as 10kbps, CBS as 20kBps and the action when CIR is not exceeded as transmitting as default, and the action triggered by exceeding CIR as dropping.

```
Switch(config)#class-map c1
```

```
Switch(config-classmap-c1)#match access-group 1
```

```
Switch(config-classmap-c1)#exit
```

```
Switch(config)#copp-policy-map p1
```

```
Switch(config-copp-policy-map-p1)#class c1
```

```
Switch(config-copp-policy-map-p1-class-c1)#policy          packets-per-second          10
```

normal-burst-packets 20 exceed-action drop

5.5 policy

Command:

Single Bucket Mode:

```
Policy <bits_per_second> <normal_burst_bytes>
({action{{policied-cos-to-cos-transmit{policied-cos-to-dscp-transmit|violate-action}
|policied-cos-to-dscp-transmit{policied-cos-to-cos-transmit|violate-action }}
policied-dscp-exp-to-cos-transmit{policied-dscp-exp-to-dscp-transmit|violate-actio
n}}|policied-dscp-exp-to-dscp-transmit{policied-dscp-exp-to-cos-transmit|
violate-action }}|violate-action {drop| transmit}} | exceed-action ACTION ) )
```

Dual Bucket Mode:

```
policy <bits_per_second> <normal_burst_bytes> [pir <peak_rate_bps>] |
<maximum_burst_bytes>
[{{action{{policied-cos-to-cos-transmit{policied-cos-to-dscp-transmit|violate-action}
|policied-cos-to-dscp-transmit{policied-cos-to-cos-transmit|violate-action }}
policied-dscp-exp-to-cos-transmit{policied-dscp-exp-to-dscp-transmit|violate-actio
n}}|policied-dscp-exp-to-dscp-transmit{policied-dscp-exp-to-cos-transmit|
violate-action }} | exceed-action | violate-action ACTION ]]
```

ACTION definition:

```
drop | transmit | policied-intp-transmit {drop|transmit| set-internal-priority } |
set-internal-priority <inp_value> {drop|transmit| policied-intp-transmit }
```

no policy

Function: It supports the non-aggregation policy command of three colors, analyze the working mode of the token bucket, whether it is single rate single bucket, single rate dual bucket or dual rate dual bucket, and set the corresponding action for different color packets. The no operation will delete the mode configuration.

Parameters:

bits_per_second: The committed information rate – CIR (Committed Information Rate), in Kbps, ranging from 1 to 10000000;

normal_burst_bytes: The committed burst size – CBS (Committed Burst Size), in Kbyte, ranging from 1 to 1000000. When the configured CBS value is smaller than 11 or larger than 100, it is applied to the port, CLI prompts the error information;

maximum_burst_bytes: The peak burst size – PBS (Peak Burst Size), in byte, ranging

from 1 to 10000000. When the configured PBS value exceeds the max limit of the chip, configure the hardware with max number supported by the chip without any CLI prompt. Notice: this configuration only exists in dual bucket mode;

pir peak_rate_bps: The peak information rate – PIR (Peak Information Rate), in kbps, ranging from 1 to 10000000. Without configuring PIR, the Police works in the single rate dual bucket mode; otherwise in the dual rate dual bucket mode. Notice: this configuration only exists in dual bucket mode;

violate-action: The actions to take when the PIR is exceeded, which means the messages are red, the default as drop;

action: The actions to take when the CIR is not exceeded, which means the messages are green, the default as transmit;

exceed-action: The actions to take when the CIR is exceeded but PIR isn't, which means the messages are yellow, the default as drop.

ACTION include:

drop/transmit: Drop/transmit the packets;

policed-intp-transmit: sends the packets whose internal priority mapping is changed through qos policy;

set-internal-priority: sets the internal priority of the packets.

Command Mode: Policy class map configuration Mode.

Default: No policy action; the default action of exceed-action and violate-action are both drop.

Usage Guide: The CLI can support both single bucket and dual bucket configuration, and determine which one to select by checking whether PIR or PBS is configured. When configuring with CLI, after configuring CBS, if the action is directly configured, the mode is single bucket dual color; if only PBS is configured, the mode is single rate dual bucket three color; if PIR and PBS are configured, the mode is dual rate dual bucket three color.

Example: In the policy class table configuration mode, set the CIR as 10kbps, CBS as 20kBps and the action when CIR is not exceeded as transmitting as default, and the action triggered by exceeding CIR as transmitting the messages after changing DSCP to 23.

```
Switch(config)#class-map c1
```

```
Switch(config-classmap-c1)#match access-group 1
```

```
Switch(config-classmap-c1)#exit
```

```
Switch(config)#copp-policy-map p1
```

```
Switch(config-copp-policy-map-p1)#class c1
```

```
Switch(config-copp-policy-map-p1-class-c1)#policy      10      20      exceed-action
```

set-internal-priority 23 transmit