Content

Chapter 1 MONITOR AND DEBUG.....1-1-1

1.1 PING 1-1-1

1.2 PING6 1-1-1

1.3 TRACEROUTE.....1-1-1

1.4 TRACEROUTE6.....1-1-2

1.5 SHOW 1-1-2

1.6 DEBUG 1-1-3

1.7 LOGGING 1-1-4

Chapter 2 RELOAD SWITCH AFTER SPECIFIED TIME.....2-2-1

2.1 INTRODUCE TO RELOAD SWITCH AFTER SPECIFID TIME 2-2-1

2.2 RELOAD SWITCH AFTER SPECIFID TIME TASK LIST 2-2-1

Chapter 3 DEBUGGING AND DIAGNOSIS FOR PACKETS RECEIVED AND SENT BY CPU.....3-3-1

3.1 INTRODUCTION TO DEBUGGING AND DIAGNOSIS FOR PACKETS RECEIVED AND SENT BY CPU.....3-3-1

3.2 DEBUGGING AND DIAGNOSIS FOR PACKETS RECEIVED AND SENT BY CPU TASK LIST 3-3-1

Chapter 4 DEBUGGING FOR DCP.....4-4-1

4.1 INTRODUCTION TO DCP.....4-4-1

4.2 DCP CONFIGURATION 4-4-1

4.3 DCP CONFIGURATION EXAMPLES 4-4-2

4.4 DCP CONFIGURATION TROUBLESHOOTING 4-4-3

Chapter 5 DEBUGGING FOR COPP 5-5-1

5.1 INTRODUCTION TO COPP 5-5-1

5.2 COPP CONFIGURATION.....5-5-1

5.3 COPP CONFIGURATION EXAMPLES.....5-5-4

5.4 COPP CONFIGURATION TROUBLESHOOTING.....5-5-5

Chapter 1 Monitor and Debug

When the users configures the switch, they will need to verify whether the configurations are correct and the switch is operating as expected, and in network failure, the users will also need to diagnostic the problem. Switch provides various debug commands including ping, telnet, show and debug, etc. to help the users to check system configuration, operating status and locate problem causes.

1.1 Ping

Ping command is mainly used for sending ICMP query packet from the switches to remote devices, also for check the accessibility between the switch and the remote device. Refer to the Ping command chapter in the Command Manual for explanations of various parameters and options of the Ping command.

1.2 Ping6

Ping6 command is mainly used by the switch to send ICMPv6 query packet to the remote equipment, verifying the accessibility between the switch and the remote equipment. Options and explanations of the parameters of the Ping6 command please refer to Ping6 command chapter in the command manual.

1.3 Traceroute

Traceroute command is for testing the gateways through which the data packets travel from the source device to the destination device, so to check the network accessibility and locate the network failure.

Execution procedure of the Traceroute command consists of: first a data packet with TTL at 1 is sent to the destination address, if the first hop returns an ICMP error message to inform this packet can not be sent (due to TTL timeout), a data packet with TTL at 2 will be sent. Also the send hop may be a TTL timeout return, but the procedure will carries on till the data packet is sent to its destination. These procedures is for recording every source address which returned ICMP TTL timeout message, so to describe a path the IP data packets traveled to reach the destination.

Traceroute Options and explanations of the parameters of the Traceroute command

please refer to traceroute command chapter in the command manual.

1.4 Traceroute6

The Traceroute6 function is used on testing the gateways passed through by the data packets from the source equipment to the destination equipment, to verify the accessibility and locate the network failure. The principle of the Traceroute6 under IPv6 is the same as that under IPv4, which adopts the hop limit field of the ICMPv6 and IPv6 header. First, Traceroute6 sends an IPv6 datagram (including source address, destination address and packet sent time) whose HOPLIMIT is set to 1. When first route on the path receives this datagram, it minus the HOPLIMIT by 1 and the HOPLIMIT is now 0. So the router will discard this datagram and returns with a 「ICMPv6 time exceeded」 message (including the source address of the IPv6 packet, all content in the IPv6 packet and the IPv6 address of the router). Upon receiving this message, the Traceroute6 sends another datagram of which the HOPLIMIT is increased to 2 so to discover the second router. Plus 1 to the HOPLIMIT every time to discover another router, the Traceroute6 repeat this action till certain datagram reaches the destination.

Traceroute6 Options and explanations of the parameters of the Traceroute6 command please refer to traceroute6 command chapter in the command manual.

1.5 Show

show command is used to display information about the system, port and protocol operation. This part introduces the **show** command that displays system information, other **show** commands will be discussed in other chapters.

Command	Explanation
Admin Mode	
show debugging	Display the debugging state.
show flash	Display the files and the sizes saved in the flash.
show history	Display the recent user input history command.

show history all-users [detail]	Show the recent command history of all users. Use **clear history all-users** command to clear the command history of all users saved by the system, the max history number can be set by **history all-users max-length** command.
show memory	Display content in specified memory area.
show running-config	Display the switch parameter configuration validating at current operation state.
show running-config current-mode	Show the configuration under the current mode.
show startup-config	Display the switch parameter configuration written in the Flash Memory at current operation state, which is normally the configuration file applied in next time the switch starts up.
show switchport interface [ethernet <*IFNAME*>]	Display the VLAN port mode and the belonging VLAN number of the switch as well as the Trunk port information.
show tcp **show tcp ipv6**	Display the TCP connection status established currently on the switch.
show udp **show udp ipv6**	Display the UDP connection status established currently on the switch.
show telnet login	Display the information of the Telnet client which currently establishes a Telnet connection with the switch.
show tech-support	Display the operation information and the state of each task running on the switch. It is used by the technicians to diagnose whether the switch operates properly.
show version	Display the version of the switch.
show temperature	Show CPU temperature of the switch.
show fan	This command is not supported by switch.

1.6 Debug

All the protocols switch supports have their corresponding debug commands. The users can use the information from debug commands for troubleshooting. Debug

commands for their corresponding protocols will be introduced in the later chapters.

1.7 Logging

All the protocols switch supports record the commands executed by user at the console, telnet or ssh terminal and send the log to info-center.

Command	Description
Global mode	
logging executed-commands {enable | disable}	Enable or disable the logging executed-commands
Admin mode	
show logging executed-commands state	Show the state of logging executed-commands

Chapter 2 Reload Switch after Specified Time

2.1 Introduce to Reload Switch after Specifid Time

Reload switch after specified time is to 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.

2.2 Reload Switch after Specifid Time Task List

1. Reload switch after specified time

Command	Explanation
Admin mode	
reload after {[<*HH:MM:SS*>] [days <*days*>]}	Reload the switch after a specified time period.
reload cancel	Cancel the specified time period to reload the switch.

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

3.1 Introduction to Debugging and Diagnosis for Packets Received and Sent by CPU

The following commands are used to debug and diagnose the packets received and sent by CPU, and are supposed to be used with the help of the technical support.

3.2 Debugging and Diagnosis for Packets Received and Sent by CPU Task List

Command	Explanation
Global Mode	
cpu-rx-ratelimit total <*packets*> **no cpu-rx-ratelimit total**	Set the total rate of the CPU receiving packets, the no command sets the total rate of the CPU receiving packets to default.
cpu-rx-ratelimit protocol <*protocol-type*> <*packets*> **no cpu-rx-ratelimit protocol [<*protocol- type*>]**	Set the max rate of the CPU receiving packets of the protocol type, the no command set the max rate to default.
clear cpu-rx-stat protocol [<*protocol-type*>]	Clear the statistics of the CPU received packets of the protocol type.
Admin Mode	
show cpu-rx protocol [<*protocol-type*>]	Show the information of the CPU received packets of the protocol type.
debug driver {receive|send} [interface {<*interface-name*> |all}] [protocol {<*protocol-type*> |discard |all}] [detail]	Turn on the showing of the CPU receiving or sending packet informations.

no debug driver {receive | send}	Turn off the showing of the CPU receiving or sending packet informations.

Command	Explanation
Admin Mode	
protocol filter {protocol-type} **no Protocol filter {protocol-type}**	Turn on/off the treatment of the named protocol packets, the named protocol contains: **{arp|bgp|dhcp|dhcpv6|hsrp|http|igmp|ip|ldp|mpls|ospf|pim|rip|snmp|telnet|vrrp}**

Chapter 4 Debugging for DCP

4.1 Introduction to DCP

The dynamic CPU protection is also named as dynamic CPU limit-rate. When the rate of the packet with the special source IP going up the CPU is detected exceeding the certain value, these packets will be limited the rate. The allowed maximum rate of the packet going up the CPU is named as limit-rate. The limit-rate can be the configured default value or the configured value by user.

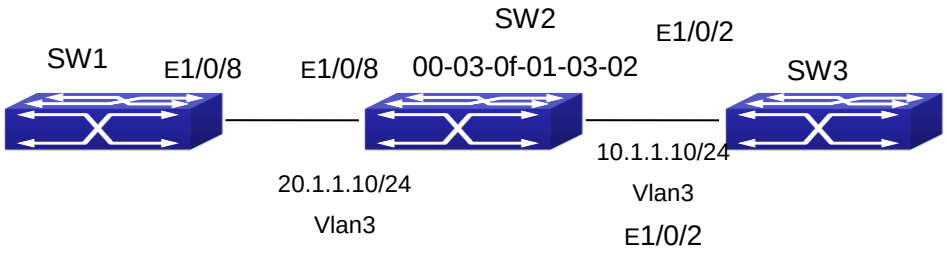
DCP is used to limit the rate for the network segment IP to prevent one IP occupying the bandwidth. DCP (Dynamic CPU Protection) means to control the rate of the packet going up the CPU through monitoring the other-ipuc packet going up the CPU for avoiding that the rate is too fast and causes overload. It can protect the CPU. When the flow is less than the half of the limit-rate in 5s, the rate limiting will be canceled. DCP is only for the other-ipuc packet, for the management packet or protocol packet, DCP is not adopted.

4.2 DCP Configuration

Command	Explanation
Global Configuration Mode	
dcp enable **dcp disable**	Enable/disable the dcp function.
dcp limit-rate <20-50> **no dcp limit-rate**	Configure the limit-rate value of dcp. The no command cancels it and recovers it to be the default value.
dcp no-limit-ip <ip_addr> **no dcp no-limit-ip <ip_addr>**	Configure the IP that the dcp does not limit its rate. The no command cancels it.
show dcp limit-rate	Show the limit-rate configured by user.
show cpu ip rate top10 [slot <1-9>|member <1-16>]	Show the first 10 IP with the maximum rate of going on cpu in 5s and show the limit-rate value.

show dcp limited ip [slot <1-9>|member <1-16>]	Show the node information of the ip which is limited the rate.
Admin Mode	
clear dcp speed limit rules {member <1-16>}	Clear the rate limiting rule that the DCP sent to the drive.
debug dcp packet **no debug dcp packet**	Show the process that the DCP deals with and monitor the packet going up the CPU, the no command cancels printing.
debug dcp event **no debug dcp event**	Show the process that the DCP deals with the events. The no command cancels printing.

4.3 DCP Configuration Examples



As shown in the above topology, send from E1/0/8 of SW1 to SW2, the destination mac is the one of SW2 which is 00-03-0f-01-03-02, the non-protocol and non-management packet with the destination ip of 10.1.1.X/24 (this ip address cannot be achieved) will be identified as other-ipuc packet. This packet will be sent to CPU. When a lot of packets like this are sent to the CPU, the CPU will be under the heavy load and it will cause that the normal business cannot be dealt with.

If enabled the DCP, when the rate of the packet with the special source IP going up the CPU is detected exceeding the certain value, these packets will be limited the rate. The CPU can be protected.

Configuration:

1. Enable DCP
2. Configure the limit-rate
3. Configure the IP address with no rate limiting
4. Show the configured limit-rate

5. Show the first 10 IP with maximum rates of going up the CPU in 5s and show the limit-rate
6. Show the node information of the ip which is limited the rate
7. Clear the rate limiting rule that the DCP sent to the drive
8. Show the process that the DCP deals with and monitor the packet going up the CPU
9. Cancel the process that the DCP deals with and monitor the packet going up the CPU
10. Show the process that the DCP deals with the events
11. Cancel printing of the process that the DCP deals with the events

Configuration steps:

Switch(Config)# dcp enable

Switch(Config)# dcp limit-rate 50

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

Switch(config)#show dcp limit-rate
Switch(config)#show cpu ip rate top10

Switch(config)#show dcp limited ip

Switch#clear dcp speed limit rules
Switch#debug dcp packet
Switch#no debug dcp packet
Switch#debug dcp event
Switch#no debug dcp event

4.4 DCP Configuration Troubleshooting

Please pay attention to the following points when using and configuring DCP:

- ☞ Under the default configuration, dcp is disabled. It can be effective only after configured the command of dcp enable.
- ☞ DCP is only for the other-ipuc packet, for the management packet or protocol packet, DCP is not adopted.
- ☞ DCP no-limited-ip can configure the maximum of 1024, if exceeds this value, it cannot be issued.
- ☞ Under the default configuration, the limit-rate for other-ipuc packet is 20.
- ☞ When the flow is less than the half of the limit-rate in 5s, the rate limiting will be canceled.
- ☞ Show the first 10 IP with maximum rates of going up the CPU in 5s and show the

limit-rate through the command of show cpu ip rate top10.

- ☞ Show the node information of the ip which is limited the rate through the command of show dcp limited ip. Limited-IP is the ip which is limited the rate, Rate(pkts/s) is the current rate.
- ☞ Enable the on-off of debug dcp packet or debug dcp event to view the process that the DCP deals with the packet going up the CPU. The command of debug dcp packet can be used to view the detailed information of the packet including source IP, destination IP, source port, destination port, protocol number, etc. The command of debug dcp event can be used to print the process that the DCP deals with the events.

Chapter 5 Debugging for COPP

5.1 Introduction to COPP

CPU is the brain of the device and it can deal with the information of all control planes. So the CPU should be protected through the appropriate measures. The CPU rate limiting keeps the previous protocol rate limiting function, and CPU rate limiting is changed to hardware rate limiting. The new function of COPP (control plane policing) can protect the control and management panel for ensuring the stability of the routing function and the normal transmission of the packets. Configure the ACL first, multiple ACL rules are supported, classify the specific packets which should be limited rate or filtered through the ACL rules. And then configure the ACL rule matching to the COPP policy map to filter the specific packets or limit the rate. The COPP supports single bucket mode, dual bucket mode and multiple configurations.

5.2 COPP Configuration

1. Configuire the ACL rule, the digital standard IP access-list is as the example
2. Create the class-map
3. Create the copp-policy-map
4. Create the policy
5. Apply to the port

1. Configuire the ACL rule

Command	Explanation
Global Configuration Mode	
access-list *<num>* {deny | permit} {{*<slpAddr>* *<sMask>*} | any-source | {host-source *<slpAddr>*}} **no access-list *<num>***	Create a digital standard IP access list. If this list has existed, add a rule entry. The no command deletes the access list.

2. Create the class-map

Command	Explanation
Global Configuration Mode	
class-map *<class-map-name>* **no class-map *<class-map-name>***	Create a class-map and enter the class-map mode. The no command deletes the

	appointed class-map.
match {access-group <acl-index-or-name> | ip dscp <dscp-list>| ip precedence <ip-precedence-list>| ipv6 access-group <acl-index-or-name> | ipv6 dscp <dscp-list> | ipv6 flowlabel <flowlabel-list> | vlan <vlan-list> | cos <*cos-list*>| vlan range <vlan-list>} **no match {access-group | ip dscp | ip precedence | ipv6 access-group | ipv6 dscp | ipv6 flowlabel | vlan |cos| vlan range}**	Configure the matching standard of the class-map and classify the data according to ACL. The no command deletes it.

3. Create the copp-policy-map

Command	Explanation
Global Configuration Mode	
copp-policy-map <*policy-map name*> **no policy-map <*policy-map-name*>**	Create a copp-policy-map and enter the copp-policy-map mode. The no command deletes the appointed copp-policy-map.
class <*class-map-name*> **no class <*class-map-name*>**	After create a copp-policy-map, it can be corresponding to a class, and different policies can be adopted for different data flow after enter the policy class map configuration mode. The no command deletes the appointed policy class map.
pps mode: **policy packets-per-second <pps> normal-burst-packets <pps> { conform-action | exceed-action } <ACTION>** **no policy** **bps mode:** **1. Single Bucket Mode:** **Policy <bits_per_second> <normal_burst_bytes> ({action{{policied-cos-to-cos-transmit{ policied-cos-to-dscp-transmit|violate-a**	pps mode: 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. bps mode: It supports the non-aggregation policy command of three colors, analyze the

ction}|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-action}|policied-dscp-exp-to-dscp-transmit{policied-dscp-exp-to-cos-transmit| violate-action }}violate-action {drop| transmit}} | exceed-action ACTION }) **2. 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-action}|policied-dscp-exp-to-dscp-transmit{policied-dscp-exp-to-cos-transmit| violate-action }} | exceed-action | violate-action ACTION }]** **ACTION definition:** **drop | transmit | set-internal-priority <intp_value> | policied-intp-transmit** **no policy**	working mode of the token bucket, whether it is single rate singe bucket, singe 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.
Policy Class Map Configuration Mode	
drop **no drop** **transmit** **no transmit**	Choose dropping or transmitting for the classified flow. The no command cancels it.

4. Apply to the port

Command	Explanation
Port Configuration Mode	
service-policy output *<policy-map name>* **no service-policy output *<policy-map-name>***	Apply a policy map to the egress of the port. The no command deletes the policy map.

5.3 COPP Configuration Examples

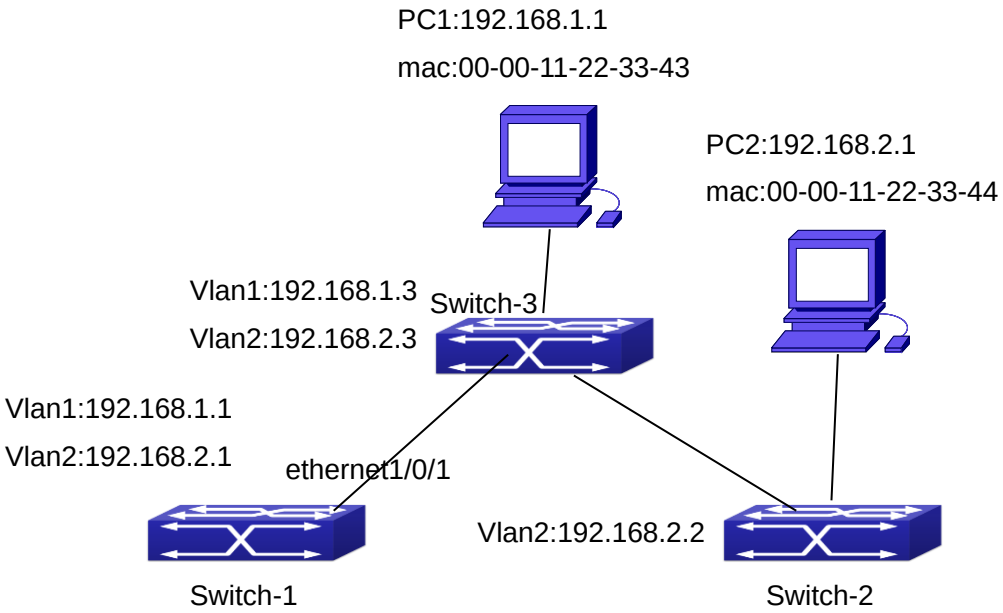


Fig 4-1 COPP function

Example 1: Configure the COPP policy map on ethernet1/0/1 of Switch-1, limit the packets in 192.168.1.0 as 10pps, and configure the burst threshold as 20pps. Drop all the packets whose bandwidth exceeds the value.

Configuration steps:

Switch#config

Switch(config)#access-list 1 permit 192.168.1.0 0.0.0.255

Switch(config)#class-map c1

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

Switch(config-classmap)# exit

Switch(config)#copp-policy-map p1

Switch(config-copp-policymap-p1)#class c1

Switch(config-copp-policymap-p1-class-c1)#policy packets-per-second 10 normal-burst-packets 20 exceed-action drop
Switch(config-copp-policymap-p1-class-c1)#exit
Switch(config-copp-policymap-p1)# #exit
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# service-policy output p1

Example 2: Configure the COPP policy map on ethernet1/0/1 of Switch-1, limit the packets of the source mac address of 00-00-11-22-33-44 as 10pps, and configure the burst threshold as 20pps. Configure the priority as 1 and forward the packets whose bandwidth exceeds the value.
Configuration steps:
Switch#config
Switch(config)#access-list 1100 permit host-source-mac 00-00-11-22-33-44 any-destination-mac
Switch(config)#class-map c1
Switch(config-classmap-c1)#match access-group 1100
Switch(config)#copp-policy-map p1
Switch(config-copp-policymap-p1)#class c1
Switch(config-copp-policymap-p1-class-c1)# policy packets-per-second 10 normal-burst-packets 20 exceed-action set-internal-priority 1 transmit
Switch(config-copp-policymap-p1-class-c1)#exit
Switch(config-copp-policymap-p1)# #exit
Switch(config)#interface ethernet 1/0/1
Switch(config-if-ethernet1/0/1)# service-policy output p1

5.4 COPP Configuration Troubleshooting

- If the packets which belong to this network segment went on the cpu correctly. This function can limit the rate of the packets going on the cpu, user can check if the packets went on the cpu through the command of debug driver receive.
- If the ACL is matched correctly. The ACL rule must be permit.
- If the COPP policy map is configured correctly. COPP must be on the egress direction on the port, it does not support the ingress direction.
- User can view the packets statistics and check if the rate limiting is effective through the command of show cpu-rx protocol all.