QTECH
МИР ДОСТУПНЕЕ

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Debugging and Diagnosis

Оглавление

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 usage`	Show the memory usage.

`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`	Show fan information of 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 System log

1.7.1 System Log Introduction

The system log takes all information output under it control, while making detailed catalogue, so to select the information effectively. Combining with Debug programs, it will provide a powerful support to the network administrator and developer in monitoring the network operation state and locating the network failures.

The switch system log has following characteristics

- Log output from four directions (or log channels) of the Console, Telnet terminal and monitor, log buffer zone, and log host.
- The log information is classified to four level of severities by which the information will be filtered
- According to the severity level the log information can be auto outputted to corresponding log channel.

1.7.1.1 Log Output Channel

So far the system log can be outputted the log information through four channels:

- Through Console port to the local console
- Output the log information to remote Telnet terminal or monitor, this function is good for remote maintenance
- Assign a proper log buffer zone inside the switch, for record the log information permanently or temporarily
- Configure the log host, the log system will directly send the log information to the log host, and save it in files to be viewed at any time

Among above log channels, users rarely use the console monitor, but will commonly choose the Telnet terminal to monitor the system operation status. However information outputted from these channels are of low traffic capacity and can not be recorded for later view. The other two channels---the log buffer zone and log host channel are two important channels

SDRAM (Synchronous Dynamic Random Access Memory) and NVRAM (Non Vulnerable Random Access Memory) is provided inside the switch as two part of the log buffer zone, The two buffer zone record the log information in a circuit working pattern, namely when log information need to be recorded exceeds the buffer size, the oldest log information will be erased and replaced by the new log information, information saved in NVRAM will stay permanently while those in SDRAM will lost when the system restarts or encounter an power failure. Information in the log buffer zone is critical for monitoring the system operation and detecting abnormal states.

Note: the NVRAM log buffer may not exist on some switches, which only have the SDRAM log buffer zone.

It is recommended to use the system log server. By configuring the log host on the switch, the log can be sent to the log server for future examination.

1.7.1.2 Format and Severity of the Log Information

The log information format is compatible with the BSD syslog protocol, so we can record and analyze the log by the systlog (system log protect session) on the UNIX/LINUX, as well as syslog similar applications on PC.

The log information is classified into eight classes by severity or emergency procedure. One level per value and the higher the emergency level the log information has, the smaller its value will be. For example, the level of critical is 2, and warning is 4, debugging is leveled at 7, so the critical is higher than warnings which no doubt is high than debugging. The rule applied in filtering the log information by severity level is that: only the log information with level equal to or higher than the threshold will be outputted. So when the severity threshold is set to debugging, all information will be outputted and if set to critical, only critical, alerts and emergencies will be outputted.

Follow table summarized the log information severity level and brief description. **Note:** these severity levels are in accordance with the standard UNIX/LINUX syslog.

Table 1-1 Severity of the log7information

Severity	Value	Description
emergencies	0	System is unusable
alerts	1	Action must be taken immediately
critical	2	Critical conditions
errors	3	Error conditions
warnings	4	Warning conditions
notifications	5	Normal but significant condition
informational	6	Informational messages
debugging	7	Debug-level messages

Right now the switch can generate information of following four levels

- Restart the switch, mission abnormal, hot plug on the CHASSIS switch chips are classified critical
- Up/down interface, topology change, aggregate port state change of the interface are notifications warnings

- Outputted information from the CLI command is classified informational
- Information from the debugging of CLI command is classified debugging

Log information can be automatically sent to corresponding channels with regard to respective severity levels. Amongst the debugging information can only be sent to the monitor. Those with the Informational level can only be sent to current monitor terminal, such as the information from the Telnet terminal configuration command can only be transmitted to the Telnet terminal. Warnings information can be sent to all terminal with also saved in the SDRAM log buffer zone. And the critical information can be save both in SDRAM and the NVRAM (if exists) besides sent to all terminals. To check the log save in SDRAM and the NVRAM, we can use the show logging buffered command. To clear the log save in NVRAM and SDRAM log buffer zone, we can use the clear logging command.

1.7.2 System Log Configuration

System Log Configuration Task Sequence:

1. Display and clear log buffer zone
2. Configure the log host output channel
3. Enable/disable the log executed-commands
4. Display the log source
5. Display executed-commands state

1. Display and clear log buffer zone

Command	Description
Admin Mode	
`show logging buffered [ level {critical | warnings} | range <begin-index> <end-index>]`	Show detailed log information in the log buffer channel.
`clear logging {sdram | nvram}`	Clear log buffer zone information.

2. Configure the log host output channel

Command	Description
Global Mode	
`logging {<ipv4-addr> | <ipv6-addr>} [ facility <local-number> ] [level <severity>]` `no logging {<ipv4-addr> | <ipv6-addr>} [ facility <local-number>]`	Enable the output channel of the log host. The “no” form of this command will disable the output at the output channel of the log host.
`logging loghost sequence-number` `no logging loghost sequence-number`	Add the loghost sequence-number for the log, the no command does not include the loghost sequence-number.

3. Enable/disable the log executed-commands

Command	Description
Global mode	
`logging executed-commands {enable | disable}`	Enable or disable the logging executed-commands

4. Display the log source

Command	Description
Admin and configuration mode	
`show logging source mstp`	Show the log information source of MSTP module.

5. Display executed-commands state

Command	Description
Admin mode	
`show logging executed-commands state`	Show the state of logging executed-commands

1.7.3 System Log Configuration Example

Example 1: When managing VLAN the IPv4 address of the switch is 100.100.100.1, and the IPv4 address of the remote log server is 100.100.100.5. It is required to send the log information with a severity equal to or higher than warnings to this log server and save in the log record equipment local1.

Configuration procedure:

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)# ip address 100.100.100.1 255.255.255.0
Switch(Config-if-Vlan1)#exit
Switch(config)#logging 100.100.100.5 facility local1 level warnings
```

- **Example 2:** When managing VLAN the IPv6 address of the switch is 3ffe:506::1, and the IPv4 address of the remote log server is 3ffe:506::4. It is required to send the log information with a severity equal to or higher than critical to this log server and save the log in the record equipment local7.

Configuration procedure

```
Switch(config)#interface vlan 1
Switch(Config-if-Vlan1)#ipv6 address 3ffe:506::1/64
Switch(Config-if-Vlan1)#exit
Switch(config)#logging 3ffe:506::4 facility local7 level critical
```

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.

3. EBUGGING 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}