SIGNAMAX

C-310 Series Gigabit Managed Switch

CLI Reference Guide

SOFTWARE RELEASE
v1.0.2.6

www.signamax.com

CLI Reference Guide

SC31020

C-310 24 Port Gigabit 740W PoE+ Managed Switch

E122020-MR-R01

How to Use This Guide

This guide includes detailed information on the switch software, including how to operate and use the management functions of the switch. To deploy this switch effectively and ensure trouble-free operation, you should first read the relevant sections in this guide so that you are familiar with all of its software features.

Who Should Read This Guide?

This guide is for network administrators who are responsible for operating and maintaining network equipment. The guide assumes a basic working knowledge of LANs (Local Area Networks), the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

How This Guide is Organized

This guide describes the switch's command line interface (CLI). For more detailed information on the switch's key features or information about the web browser management interface refer to the *Web Management Guide*.

The guide includes these sections:

- Section I "Command Line Interface" — Includes all management options available through the CLI.
- Section II "Appendices" — Includes information on troubleshooting switch management access.

Related Documentation

This guide focuses on switch software configuration through the CLI.

For information on how to manage the switch through the Web management interface, see the following guide:

Web Guide

For information on how to install the switch, see the following guide:

Quick Start Guide

For all safety information and regulatory statements, see the following documents:

Safety and Regulatory Information

Conventions

The following conventions are used throughout this guide to show information:

Note: Emphasizes important information or calls your attention to related features or instructions.

Caution: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Revision History

This section summarizes the changes in each revision of this guide.

Revision	*Date*	*Change Description*
v1.0.2.6	12/2020	Initial release

Contents

Tables

Section I

Command Line Interface

This section provides a detailed description of the Command Line Interface, along with examples for all of the commands.

This section includes these chapters:

1 Using the Command Line Interface

This chapter describes how to use the Command Line Interface (CLI).

Accessing the CLI

When accessing the management interface for the switch via a Telnet or Secure Shell connection (SSH), the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

Telnet Connection

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion. For example, the IP address assigned to this switch, 10.1.0.1, consists of a network portion (10.1.0) and a host portion (1).

Note: The default IP address for this switch is 192.168.2.10.

To access the switch through a Telnet session, you must first set the IP address for the Master unit, and set the default gateway if you are managing the switch from a different IP subnet. For example,

```
SC31020(config)#interface vlan 1
SC31020(config-if)#ip address 192.168.2.1 255.255.255.0
SC31020(config-if)#exit
SC31020(config)#ip default-gateway 192.168.1.254
SC31020(config)#
```

If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

After you configure the switch with an IP address, you can open a Telnet session by performing these steps:

1. From the remote host, enter the Telnet command and the IP address or host name of the device you want to access.

2. At the prompt, enter the user name and system password. The CLI will display the "Vty-*n*#" prompt for the administrator to show that you are using privileged access mode (i.e., Privileged Exec), or "Vty-*n*>" for the guest to show that you are using normal access mode (i.e., Normal Exec), where *n* indicates the number of the current Telnet session.

3. Enter the necessary commands to complete your desired tasks.

4. When finished, exit the session with the "quit" or "exit" command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:

  CLI session with the SC310 is opened.
  To end the CLI session, enter [Exit].

Vty-0#
```

Note: You can open up to eight sessions to the device via Telnet or SSH.

Entering Commands

Keywords and Arguments

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command "show interfaces status ethernet 1/5," **show interfaces** and **status** are keywords, **ethernet** is an argument that specifies the interface type, and **1/5** specifies the unit/port.

You can enter commands as follows:

- To enter a simple command, enter the command keyword.

- To enter multiple commands, enter each command in the required order. For example, to enable Privileged Exec command mode, and display the startup configuration, enter the following commands. The default password "super" is used to change from Normal Exec to Privileged Exec mode:

```
SC31020>enable
Password:
SC31020#show startup-config
```

- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
SC31020(config)#username admin password 0 jamesbond
```

Minimum Abbreviation

The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command "configure" can be entered as **con**. If an entry is ambiguous, the system will prompt for further input.

Command Completion

If you terminate input with a Tab key, the CLI will print the remaining characters of a partial keyword up to the point of ambiguity. In the "logging history" example, typing **log** followed by a tab will result in printing the command up to "**logging**."

Getting Help on Commands

You can display a brief description of the help system by entering the **help** command. You can also display command syntax by using the "?" character to list keywords or parameters.

Showing Commands

If you enter a "?" at the command prompt, the system will display the first level of keywords or command groups. You can also display a list of valid keywords for a specific command. For example, the command "**show system ?**" displays a list of possible show commands:

```
SC31020#show ?
  cluster               Display cluster
  dns                   DNS information
  dot1q-tunnel          802.1Q tunnel
  sflow                 Shows the sflow information
  upgrade               Shows upgrade information
  access-group          Access groups
  access-list           Access lists
  accounting            Uses the specified accounting list
  arp                   Information of ARP cache
  authorization         Enables EXEC accounting
  bridge-ext            Bridge extension information
  cable-diagnostics     Shows the information of cable diagnostics
  calendar              Date and time information
  class-map             Displays class maps
  debug                 State of each debugging option
  dns                   DNS information
  dos-protection        Shows the system dos-protection summary information
  dot1q-tunnel          802.1Q tunnel
  dot1x                 802.1X content
  history               Shows history information
  hosts                 Host information
  interfaces            Shows interface information
  ip                    IP information
  ipv6                  IPv6 information
  lacp                  LACP statistics
  license               Show license
  line                  TTY line information
```

```
  lldp                  LLDP
  log                   Log records
  logging               Logging setting
  loopback-detection    Shows loopback detection information
  mac                   MAC access list
  mac-address-table     Configuration of the address table
  mac-vlan              MAC-based VLAN information
  management            Shows management information
  memory                Memory utilization
  network-access        Shows the entries of the secure port.
  nlm                   Show notification log
  ntp                   Network Time Protocol configuration
  policy-map            Displays policy maps
  port                  Port characteristics
  port-channel          Port channel information
  power-save            Shows the power saving information
  privilege             Shows current privilege level
  process               Device process
  protocol-vlan         Protocol-VLAN information
  public-key            Public key information
  qos                   Quality of Service
  queue                 Priority queue information
  radius-server         RADIUS server information
  reload                Shows the reload settings
  rmon                  Remote monitoring information
  rspan                 Display status of the current RSPAN configuration
  running-config        Information on the running configuration
  sflow                 Shows the sflow information
  snmp                  Simple Network Management Protocol configuration and
                        statistics
  snmp-server           Displays SNMP server configuration
  sntp                  Simple Network Time Protocol configuration
  spanning-tree         Spanning-tree configuration
  ssh                   Secure shell server connections
  startup-config        Startup system configuration
  subnet-vlan           IP subnet-based VLAN information
  system                System information
  tacacs-server         TACACS server information
  tech-support          Technical information
  time-range            Time range
  traffic-segmentation  Traffic segmentation information
  upgrade               Shows upgrade information
  users                 Information about users logged in
  version               System hardware and software versions
  vlan                  Shows virtual LAN settings
  voice                 Shows the voice VLAN information
  watchdog              Displays watchdog status
  web-auth              Shows web authentication configuration
SC31020#show
```

The command "**show interfaces ?**" will display the following information:

```
SC31020#show interfaces ?
  brief                 Shows brief interface description
  counters              Interface counters information
  history               Historical sample of interface counters information
  protocol-vlan         Protocol-VLAN information
  status                Shows interface status
  switchport            Shows interface switchport information
  transceiver           Interface of transceiver information
```

```
  transceiver-threshold  Interface of transceiver-threshold information
SC31020#
```

Show commands which display more than one page of information (e.g., **show running-config**) pause and require you to press the [Space] bar to continue displaying one more page, the [Enter] key to display one more line, or the [a] key to display the rest of the information without stopping. You can press any other key to terminate the display.

Partial Keyword Lookup

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example "**s?**" shows all the keywords starting with "s."

```
SC31020#show s?
sflow           snmp            snmp-server     sntp            spanning-tree
ssh             startup-config  system
SC31020#show s
```

Negating the Effect of Commands

For many configuration commands you can enter the prefix keyword "**no**" to cancel the effect of a command or reset the configuration to the default value. For example, the **logging** command will log system messages to a host server. To disable logging, specify the **no logging** command. This guide describes the negation effect for all applicable commands.

Using Command History

The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the **show history** command displays a longer list of recently executed commands.

Understanding Command Modes

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain switching functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark "**?**" at the prompt to display a list of the commands available for the current mode. The command classes and associated modes are displayed in the following table:

Table 1: General Command Modes

Class	Mode	
Exec	Normal Privileged	
Configuration	Global*	Access Control List Class Map DHCP IGMP Profile Interface Line Multiple Spanning Tree Policy Map Time Range VLAN Database

* You must be in Privileged Exec mode to access the Global configuration mode.
You must be in Global Configuration mode to access any of the other configuration modes.

Exec Commands

When you open a new console session on the switch with the user name and password “guest,” the system enters the Normal Exec command mode (or guest mode), displaying the “SC31020>” command prompt. Only a limited number of the commands are available in this mode. You can access all commands only from the Privileged Exec command mode (or administrator mode). To access Privilege Exec mode, open a new console session with the user name and password “admin.” The system will now display the “SC31020#” command prompt. You can also enter Privileged Exec mode from within Normal Exec mode, by entering the enable command, followed by the privileged level password “super.”

To enter Privileged Exec mode, enter the following user names and passwords:

```
Username: admin
Password: [admin login password]

  CLI session with the SC310 is opened.
  To end the CLI session, enter [Exit].

SC31020#
```

```
Username: guest
Password: [guest login password]

  CLI session with the SC310 is opened.
  To end the CLI session, enter [Exit].

Sc3010>enable
Password: [privileged level password]
SC31020#
```

Configuration Commands

Configuration commands are privileged level commands used to modify switch settings. These commands modify the running configuration only and are not saved when the switch is rebooted. To store the running configuration in non-volatile storage, use the **copy running-config startup-config** command.

The configuration commands are organized into different modes:

- Global Configuration - These commands modify the system level configuration, and include commands such as **hostname** and **snmp-server community**.
- Access Control List Configuration - These commands are used for packet filtering.
- Class Map Configuration - Creates a DiffServ class map for a specified traffic type.
- IGMP Profile - Sets a profile group and enters IGMP filter profile configuration mode.
- Interface Configuration - These commands modify the port configuration such as **speed-duplex** and **negotiation**.
- Line Configuration - These commands modify the Telnet configuration, and include command such as **parity** and **databits**.
- Multiple Spanning Tree Configuration - These commands configure settings for the selected multiple spanning tree instance.
- Policy Map Configuration - Creates a DiffServ policy map for multiple interfaces.
- Time Range - Sets a time range for use by other functions, such as Access Control Lists.
- VLAN Configuration - Includes the command to create VLAN groups.

To enter the Global Configuration mode, enter the command **configure** in Privileged Exec mode. The system prompt will change to “SC31020(config)#” which gives you access privilege to all Global Configuration commands.

```
SC31020#configure
SC31020((config)#
```

To enter the other modes, at the configuration prompt type one of the following commands. Use the **exit** or **end** command to return to the Privileged Exec mode.

For example, you can use the following commands to enter interface configuration mode, and then return to Privileged Exec mode

```
SC31020((config)#interface ethernet 1/5
.
.
.
SC31020((config-if)#exit
SC31020(config)#
```

Command Line Processing

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the "?" character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

Table 2: Keystroke Commands

Keystroke	Function
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-C	Terminates the current task and displays the command prompt.
Ctrl-E	Shifts cursor to end of command line.
Ctrl-F	Shifts cursor to the right one character.
Ctrl-K	Deletes all characters from the cursor to the end of the line.
Ctrl-L	Repeats current command line on a new line.
Ctrl-N	Enters the next command line in the history buffer.
Ctrl-P	Enters the last command.
Ctrl-R	Repeats current command line on a new line.
Ctrl-U	Deletes from the cursor to the beginning of the line.
Ctrl-W	Deletes the last word typed.
Esc-B	Moves the cursor back one word.
Esc-D	Deletes from the cursor to the end of the word.
Esc-F	Moves the cursor forward one word.
Delete key or backspace key	Erases a mistake when entering a command.

Showing Status Information

There are various “show” commands which display configuration settings or the status of specified processes. Many of these commands will not display any information unless the switch is properly configured, and in some cases the interface to which a command applies is up.

For example, if a static router port is configured, the corresponding show command will not display any information unless IGMP snooping is enabled, and the link for the static router port is up.

```
SC31020#configure
SC31020(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
SC31020(config)#end
SC31020#show ip igmp snooping mrouter
 VLAN M'cast Router Ports Type
 ---- ------------------- -------
SC31020#configure
SC31020(config)#ip igmp snooping
SC31020(config)#end
SC31020#show ip igmp snooping mrouter
 VLAN M'cast Router Ports Type
 ---- ------------------- -------
 1    Eth 1/11            Static
SC31020#
```

CLI Command Groups

The system commands can be broken down into the functional groups shown below.

Table 3: Command Group Index

Command Group	Description
General	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI
System Management	Display and setting of system information, basic modes of operation, maximum frame size, file management, telnet settings, system logs, SMTP alerts, and the system clock
Simple Network Management Protocol	Activates authentication failure traps; configures community access strings, and trap receivers
Remote Monitoring	Supports statistics, history, alarm and event groups
User Authentication	Configures user names and passwords, command privilege levels, logon access using local or remote authentication, management access through the web server, Telnet server and Secure Shell; as well as port security, IEEE 802.1X port access control, and restricted access based on specified IP addresses
General Security Measures	Segregates traffic for clients attached to common data ports; and prevents unauthorized access by configuring valid static or dynamic addresses, MAC address authentication, filtering DHCP requests and replies, and discarding invalid ARP responses

Table 3: Command Group Index (Continued)

Command Group	Description
Access Control List	Provides filtering for IPv4 frames (based on address, protocol, TCP/UDP port number or TCP control code), IPv6 frames (based on address, DSCP traffic class, or next header), or non-IP frames (based on MAC address or Ethernet type)
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs
Link Aggregation	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port
Congestion Control	Sets the input/output rate limits, traffic storm thresholds, and thresholds for broadcast and multicast storms which can be used to trigger configured rate limits or to shut down a port.
Loopback Detection	Detects general loopback conditions caused by hardware problems or faulty protocol settings
Address Table	Configures the address table for filtering specified addresses, displays current entries, clears the table, or sets the aging time
Spanning Tree	Configures Spanning Tree settings for the switch
VLANs	Configures VLAN settings, and defines port membership for VLAN groups; also enables or configures private VLANs, protocol VLANs, voice VLANs, and QinQ tunneling
Class of Service	Sets port priority for untagged frames, selects strict priority or weighted round robin, relative weight for each priority queue, also sets priority for DSCP
Quality of Service	Configures Differentiated Services
Multicast Filtering	Configures IGMP multicast filtering, query, profile, and proxy parameters; specifies ports attached to a multicast router; also configures multicast VLAN registration, and IPv6 MLD snooping
Link Layer Discovery Protocol	Configures LLDP settings to enable information discovery about neighbor devices
Domain Name Service	Configures DNS services.
Dynamic Host Configuration Protocol	Configures DHCP client and relayfunctions
IP Interface	Configures IP address for the switch interfaces; also configures ARP parameters
IP Routing	Configures static and dynamic unicast routing
Debug	Displays debugging information for all key functions
	These commands are not described in this manual. Please refer to the prompt messages included in the CLI interface.

The access mode shown in the following tables is indicated by these abbreviations:

ACL (Access Control List Configuration)
CM (Class Map Configuration)
GC (Global Configuration)
IC (Interface Configuration)
IPC (IGMP Profile Configuration)
LC (Line Configuration)
MST (Multiple Spanning Tree)
NE (Normal Exec)
PE (Privileged Exec)
PM (Policy Map Configuration)
VC (VLAN Database Configuration)

2 MTU

MTU

mtu In the interface configuration mode, use this command to set the MTU of the interface. Can be set in the range 64-10240.

Syntax

mtu [**range**]

Default Setting
1522

Command Mode
Global Configuration

Example

```
SC31020(config)# mtu 10240
```

show interfaces gigabitEthernet id mtu View the interface mtu status information.

Syntax

show interfaces gigabitEthernet [**id**] mtu

Example

```
SC31020# show interfaces GigabitEthernet 0/1 mtu
     Interface       |        MTU
---------------------+---------------------
       gi0/1         |       10240
```

3 Link-Aggregate Port Commands

Configure relevant commands

link-aggregation load-balance

Configure a traffic balancing algorithm for link-aggregation port (AGG). Use the no option for this command to set the recovery traffic balance to the default.

Syntax

link-aggregation load-balance {mac | ip-mac}

no link-aggregation load-balance

mac – The traffic is allocated according to the source MAC address of the incoming packets. In each AGG, packets from different MAC addresses are assigned to different ports. Packets from the same MAC address use the same port.

ip-mac – Traffic is allocated based on source IP and source MAC. Different source IP - source MAC traffic is forwarded through different ports, and the same source IP - source MAC is forwarded through the same link.

Default Setting
Null

Command Mode
Global Configuration

Usage
Use the show link-aggregation group command to view the traffic balancing algorithm

Example

```
SC31020(config)# link-aggregation load-balance ip
```

show link-aggregation group

Display link-aggregation settings

Example

```
SC31020(config)# show link-aggregation group
```

link-aggregation load-balance

Create a link-aggregation group.

Syntax

link-aggregation {group-number **mode {manual | lacp}}**

no link-aggregation {group-number}

group-number - The link-aggregation member port group number

manual - Use static mode

lacp - Use LACP protocol

Default Setting
The physical port does not belong to any link-aggregate port by default

Command Mode
Global Configuration

Usage
You can configure manual mode and lacp mode. No command requires no interface in the aggregation group.

Example
The following example creates a link aggregation group 1

```
SC31020(config)#link-aggregation 1 mode manual
```

Interface link-aggreation

Set a physical port as a member port of the link-aggregation port. Use the no option of the command to remove the link-aggregation Port member attribute of the port.

Syntax

link-aggregation group-number [active| passive| manual]

no link-aggregation {group-number}

group-number - The link-aggregation member port group number

Default Setting
The physical port does not belong to any link-aggregate port by default

Command Mode
Interface configuration mode

Usage
All AGG member interfaces need to be in the same VLAN.

Example

```
SC31020(config)# interface GigabitEthernet /1
SC31020(config-if-GigabitEthernet0/1)# link-aggregation 1 active
```

show link-aggregation group Display link-aggregation settings

Example

```
SC31020(config)# show link-aggregation group
```

Display relevant commands

show link-aggregation Display the status of all link aggregation groups

Syntax

show link-aggregation [group | group-number]

show link-aggregate group - Show all link aggregation groups

show link-aggregate group group-number - Displays a specific group of link aggregation

Default Setting
Null

Command Mode
Privilege mode

Usage
If you do not specify the aggregate port interface number, all the information of the aggregate port will be displayed.

Example
The following example shows information about link-aggregation 1

```
SC31020# show link-aggregation group 1
```

4 Port Mirroring Commands

Configure relevant commands

monitor session Create a SPAN session and specify the destination port (monitor port) and source port (monitored port). Use the no option of the command to delete the session or remove the source port or destination port separately.

Syntax

monitor session *session_number* {[source **interface GigabitEthernet** *port-id* [both | rx | tx]] | [destination **interface GigabitEthernet**]}

no monitor session *session_number {[source* ***interface GigabitEthernet*** *port-id [both | rx | tx]] | [destination* **interface GigabitEthernet** *port-id]}*

session_number - SPAN session number.

source interface GigabitEthernet port-id - Specify the source port. For interface-id, specify the corresponding interface number, only the physical port, not for the SVI.

destination interface GIgabitEthernet port-id - Specify the destination port. For interface-id, specify the corresponding interface number, only the physical port, not for the SVI.

both - While monitoring input and output messages.

rx - Only monitor the input message.

tx - Only monitor the output message.

Default Setting
Null

Command Mode
Global configuration mode

Command Usage
Switch port and AGG (separate port settings) can be configured as source and destination ports. The SPAN session does not affect the normal operation of the switch. SPAN sessions can be configured on a disabled port, however, SPAN does not work immediately until the destination and source port are enabled. A port can not be both a source port and a destination port. Use the show monitor command to display the operating status of the SPAN session.

Example
The following example shows how to create a SPAN session: Session 1. If the session has already been set up, First clear the configuration of the current session 1, and then set the port 0 interface to the port interface 0/1.

```
SC31020(config)# no monitor session 1
SC31020(config)# monitor session 1 source interfaces
                    GigabitEthernet 0/2 both
SC31020(config)# monitor session 1 destination interface
                    GigabitEthernet 0/1
```

Display relevant commands

show monitor Displays the status of the current SPAN configuration.

Default Setting
All SPAN sessions are displayed by default

Command Mode
Privilege mode

Example
The following example shows how to create a SPAN session: Session 1. If the session has already been set up, First clear the configuration of the current session 1, and then set the port 0 interface to the port interface 0/1.

```
SC31020# show monitor
Session 1 Configuration
Source RX Port : gi0/9
Source TX Port : gi0/9
Destination port : gi0/10
Ingress State: disabled
```

5 Port Isolation Commands

Configure relevant commands

isolate-port Configure the port isolation in port mode and delete the configuration with the no command. By default, port isolation is disabled.

Syntax

Switchport protected

no Switchport protected

Switchport protected - Turn on port isolation configuration

Default
Disabled

Command Mode
Port configuration mode

Usage
After the port isolation function is enabled, the port and port, port, and link aggregation

group (AGG) can not be accessed from each other.

Example
The following is the isolation between port 0/1 and port 0/2.

```
SC31020(config)# interface GigabitEthernet 0/1
SC31020(config)# interface GigabitEthernet 0/2

SC31020(config-if-GigabitEthernet0/2)# switchport protected
SC31020(config-if-GigabitEthernet0/1)# switchport protected
```

show interfaces GigabitEthernet 0/1 protected View the current port isolation information

Display relevant commands

show isolate-port Displays the current port isolation configuration.

Syntax

show interfaces port-id **protected**

Default

Null

Command Mode

Privilege mode

Example

```
SC31020#show isolate-port
```

show interfaces port-id protected View the current port isolation information

6 Port Speed Limit

Configure relevant commands

rate-limit In port mode, enable / disable the port input / output rate.

Syntax

rate-limit {input | output}

no rate-limit {input | output}

rate-limit {input | output} - Open the port speed limit function, limiting the input and output speed.

no rate-limit {input | output} - Close the port speed limit function, limiting the input and output speed.

Default
Turn off port speed limit function

Command Mode
Interface configuration mode

Usage
After the port speed limit is enabled, the upstream and downstream rates of the ports are controlled.

Example
The following is the configuration of port 0/1 configuration port uplink rate limit.

```
SC31020(config-if-GigabitEthernet0/1)# rate-limit input 10000
```

show rate-limit View the current rate configuration information of the port.

Display relevant commands

show rate-limit & show traffic-shap

Displays the current port rate limit configuration.

Syntax

show rate-limit

Show rate-limit interfaces {port-id}

show rate-limit - Display the upstream rate limit configuration information for all the ports

show rate-limit interface {port-id} - Display the upstream rate limit configuration information of a current port

Default
Null

Command Mode
Privilege mode

Usage
Display the upstream rate limit configuration information for all the ports.

Example

```
SC31020# show rate-limit interfaces GigabitEthernet 0/1
Interface           |Ingress             |Egress
                    |kbps                |kbps
--------------------+--------------------+--------------------
gi0/1               |IGR-UNLIMIT         |10000
```

show rate-limit interface port-list

View the current port rate configuration information.

7 Storm control

Configure relevant commands

storm-control Enable or disable storm control in port mode: Use the storm-control command to enable storm control, Use the no command to turn off storm control.

Syntax

storm-control {[broadcast | unknown-multicast | unknown-unicast] kbps}

no storm-control

broadcast - Broadcast packets

Unknown-multicast - Unknown Multicast packets

Unknown-unicast - Unknown unicast packets

kbps - Rate unit

Default
Turn off storm control

Command Mode
Interface configuration mode

Usage
After the storm control function is enabled, you can set the rate at which the packets received on the corresponding port (the rate of the received packets (broadcast, unknown multicast, unknown unicast).

Example
The following is the port 0/1 open storm control configuration.

```
SC31020(config-if-GigabitEthernet0/1)#storm-control broadcast kbps 1024
SC31020(config-if-GigabitEthernet0/1)#storm-control Unknown-multicas kbps
  1024
SC31020(config-if-GigabitEthernet0/1)#storm-controlUnknown-unicastkbps1024
```

show storm-control Display storm control information.

show interface The storm control information is displayed in the interface attribute.

Display relevant commands

show storm-control

Syntax

show storm-control

show storm-control - Display storm control information

show interface - The storm control information is displayed in the interface attribute

Default
Null

Command Mode
Privilege mode

Usage
View storm control configuration information.

Example

```
SC31020(config-if-GigabitEthernet0/1)#storm-control broadcast kbps 1024
SC31020# show storm-control

Interface    | Broadcast  |  Unkown-Multicast | Unknown-Unicast |  Action
             |   kbps     |       kbps        |      kbps       |
-------------+------------+-------------------+-----------------+----------
gi0/1           Disabled         Disabled          Disabled        Drop
gi0/2             1024           Disabled          Disabled        Drop
gi0/3           Disabled         Disabled          Disabled        Drop
gi0/4           Disabled         Disabled          Disabled        Drop
gi0/5           Disabled         Disabled          Disabled        Drop
gi0/6           Disabled         Disabled          Disabled        Drop
gi0/7           Disabled         Disabled          Disabled        Drop
gi0/8           Disabled         Disabled          Disabled        Drop
gi0/9           Disabled         Disabled          Disabled        Drop
gi0/10          Disabled         Disabled          Disabled        Drop
```

8 Port Security

Configure relevant commands

Port-security After you enable Port-security, configure the limit mac number of the port. Close Port-security.

Syntax

port-security [address-limit] {Number of limitation**} action {[**discard|forward|shutdown**]}**

no port-security

number of limitation - Limit the number of macs, in the range of 1-256.

discard | forward | shutdown - Action to be taken when limitation is reached.

Default
Enable the port security function on the global switch, the port is turned off by default.

Command Mode
Port configuration mode

Usage
Open port security, when the port to learn the number of mac in the end limit, the message was discarded.

Example
The following example is configured gig0 / 1 maximum mac learning number is 200, over the message is discarded.

```
SC31020(config-if-GigabitEthernet0/1)# port-security address-limit 200 action
  discard
```

no port-security Turn off port security.

Display relevant commands

Port-security Displays information about port security.

Syntax

Show port-security interface {port-id}

Show port-security interface {port-id} - Display the port security configuration information of the specified port

discard | forward | shutdown - Action to be taken when limitation is reached.

Default
Null

Command Mode
Privilege mode

Example
Display the port security configuration information for gig1:

```
SC31020# show port-security interfaces GigabitEthernet 0/1

Port      |    Security      |   CurrentAddr   |      Action
----------+------------------+-----------------+------------------
gi0/1     |  Enabled(200)    |       13        |      Discard
```

Show port-security View the port security global status.

9 NTP/SNTP Commands

NTP Configure relevant commands

server Configure the NTP/SNTP server IP address

Syntax

{[ntp|sntp]} server{server-ip}

server-ip - server IP address

discard | forward | shutdown - Action to be taken when limitation is reached.

Default
default server ip 216.229.0.179

Command Mode
Global configuration mode

Usage
Use this command to configure the NTP/SNTP server IP address

Example

```
SC31020(config)# ntp server 192.168.100.150
SC31020(config)# sntp server 192.168.100.159
```

show ntp Display NTP configuration information.

show sntp Display SNTP configuration information.

Show ntp/sntp status

show ntp/sntp status Display ntp/sntp function status, server address, port number.

Syntax

show {[ntp|sntp]}

show ntp - Display NTP configuration information

show sntp - Display SNTP configuration information

Default
Null

Command Mode
Privilege mode

Usage
Display ntp/sntp function status, server address, port number

Example
Display NTP configuration information

```
SC31020# show ntp
NTP is Enabled
NTP Server address: 192.168.100.150
NTP Server port: 123
```

Display SNTP configuration information

```
SC31020# show sntp
SNTP is Enabled
SNTP Server address: 192.168.100.159
SNTP Server port: 123
```

10 EEE

eee Open the EEE function, the switch will automatically turn off part of the idle circuit, effectively reduce power consumption, energy saving.

Syntax

eee interfaces GigabitEthernet {port-id}

eee - Turn on all port eee functions

eee interfaces GigabitEthernet {port-id} - Open the eee function for the specified port

Default
Turn off the eee function

Command Mode
Global configuration mode

Usage
Effectively reduce the switch power consumption, energy saving.

Example
Turn on all port eee functions:

```
SC31020(config)# eee
```

Open the eee function for the specified port:

```
SC31020(config)# eee interfaces GigabitEthernet 0/1
```

show eee View the configuration information for the EEE function.

11 DDOS Protection

Configuration DDOS protection

Turn on DDOS protection

Open the ddos protection function, you can defend against ddos attacks.

Syntax

Dos{[land-deny | smurf-deny | nullscan-deny | xma-deny | synfin-deny | syn-sportl1024-deny | pod-deny]}

land-deny - Source IP equals to destination IP

smurf-deny - Smurf Attacks messages

nullscan-deny - Null scan attack

xma-deny - Xmascan:sequence number is zero and the FIN, URG and PSH bits are set

synfin-deny - SYN and FIN bits set in the packet

syn-sportl1024-deny - SYN packets with sport less than 1024

pod-deny - Ping of death attacks

Default
Turn off the DDOS protection function.

Command Mode
Global configuration mode

Usage
Prevent the ddos attack.

Example
Turn on land-deny attack protection:

```
SC31020(config)# dos land-deny
```

Turn off DDOS protection

Turn off the ddos protection function.

Syntax

no dos {attack-name}

no dos {attack-name} - Turn off a specific attack on the ddos protection

Default
Null

Command Mode
Global configuration mode

Usage
Turn off the defense against a specified DDOS attack.

Example
Turn off land-deny attack protection:

```
SC31020(config)# no dos land-deny
```

Show DDOS protection

View the configuration information for DOS protection.

Syntax

Show dos

Default
Null

Command Mode
Privilege Mode

Usage
View the DDOS protection.

Example
View the configuration information for DOS protection:

```
SC31020# show dos
             Type                    |        State (Length)
-------------------------------------+-------------------------------------
DMAC equal to SMAC                   |           disabled
Land (DIP = SIP)                     |           enabled
UDP Blat (DPORT = SPORT)             |           disabled
TCP Blat (DPORT = SPORT)             |           disabled
POD (Ping of Death)                  |           disabled
IPv6 Min Fragment Size               |      disabled (1240 Bytes)
ICMP Fragment Packets                |           disabled
```

```
IPv4 Ping Max Packet Size            |      disabled (512 Bytes)
IPv6 Ping Max Packet Size            |      disabled (512 Bytes)
Smurf Attack                         |   disabled (Netmask Length: 0)
TCP Min Header Length                |      disabled (20 Bytes)
TCP Syn (SPORT < 1024)               |           disabled
Null Scan Attack                     |           disabled
X-Mas Scan Attack                    |           disabled
TCP SYN-FIN Attack                   |           disabled
TCP SYN-RST Attack                   |           disabled
TCP Fragment (Offset = 1)            |           disabled
```

12 CPU Guard

Configuration CPU Guard

cpu-protect Configuring each type of packet bandwidth can suppress high-speed attack packets in the network.

Syntax

cpu-protect {[**cpu**]}{**bandwidth**}pps_vaule

cpu-protect {[**sub-interface**]}{[Message_type]}**pps** pps_vaule

cpu bandwidth - Set cpu bandwidth(pps)

Sub_interface - Set the type of cpu protected packets

cpu bandwidth pps_vaule - Set the total bandwidth of the cpu, in the range of 64-4000

message_type - The message types include: manage, protocol, route

[Message_type] pps pps_vaule - Set the bandwidth of each type of packet, in the range of 1 to 4000

Default
Cpu Port Bandwidth 1000pps

Cpu Protect Manage Bandwidth 500pps

Cpu Protect Route Bandwidth 200pps

Cpu Protect Protocol Bandwidth 500pps

Command Mode
Global configuration mode

Usage
To Configure each type of message bandwidth can inhibit high rate of attack packets in network.

Example
Set the total bandwidth of the cpu:

```
SC31020(config)# cpu-protect cpu bandwidth 4000
```

Set the bandwidth of manage packets:

```
SC31020(config)# cpu-protect sub-interface manage pps 600
```

Show CPU Guard

show cpu-protect View the configuration information for CPU Guard.

Syntax

show cpu-protect

show cpu-protect cpu

show cpu-protect sub-interface {[manage | protocol | route]}

show cpu-protect - View the configuration information for CPU Guard

show cpu-protect cpu - View the configuration information for CPU bandwidth

show cpu-protect sub-interface - View the bandwidth of each type of packet

Default
Null

Command Mode
Privilege mode

Usage
View the CPU Guard information

Example
View the configuration information for CPU Guard:

```
SC31020# show cpu-protect
```

View the configuration information for CPU bandwidth:

```
SC31020# show cpu-protect cpu
```

View the bandwidth of each type of packet:

```
SC31020# show cpu-protect sub-interface manage
```

13 Dual Configuration

Backup the Configuration File

copy backup-config Configuring each type of packet bandwidth can suppress high-speed attack packets in the network.

Syntax

copy {[running-config | startup-config]}**backup-config**

running-config - Backup the current configuration file to backup-config

startup-config - Backup the startup-config file to backup-config

Default
Null

Command Mode
Privilege mode

Usage
Backup the configuration file.

Example
Backup the running-config file:

```
SC31020# copy running-config backup-config
```

Backup the startup-config file:

```
SC31020# copy startup-config backup-config
```

Restore the Configuration File

copy backup-config Configuring each type of packet bandwidth can suppress high-speed attack packets in the network.

Syntax

copy backup-config {[running-config | startup-config]}

running-config - restore the current configuration file from backup-config

startup-config - restore the startup-config file from backup-config

Default
Null

Command Mode
Privilege mode

Usage
Restore the configuration file.

Example
Restore the running-config file:

```
SC31020# copy backup-config running-config
```

Restore the startup-config file:

```
SC31020# copy backup-config startup-config
```

14 RMON

RMON Event

rmon event

Syntax

rmon event<1-65535>[log][trap COMMUNITY][description DESCRIPTION][owner NAME]

<1-65535> - Specify event index to create or modify

log- Specify to show syslog

trap COMMUNITY - Specify SNMP community to show SNMP trap

description DESCRIPTION - Specify description of event

owner NAME - Specify owner of event

Default
Null

Command Mode
Global Configuration mode

Usage
Use the rmon event command to add or modify a RMON event entry. Use the no form of this command to delete. You can verity settings by the show rmon event command.

Example
The example shows how to add RMON event entry with log and trap action and modify it action to log only:

```
SC31020(config)# rmon event 1 log trap public description test owner admin
SC31020# show rmon event 1
Rmon Event Index       : 1
Rmon Event Type        : Log and Trap
Rmon Event Community   : public
Rmon Event Description : test
Rmon Event Last Sent   :
Rmon Event Owner       : admin
SC31020(config)# rmon event 1 log description test owner admin
SC31020# show rmon event 1
Rmon Event Index       : 1
Rmon Event Type        : Log
Rmon Event Community   :
```

```
Rmon Event Description : test
Rmon Event Last Sent   :
Rmon Event Owner       : admin
```

RMON Alarm

rmon alarm Syntax

rmon alarm<1-65535>**interface** {port-id}{[broadcast-pkts|collision|crc-align-errors|drop-events|fragments|jabbers

|multicast-pkts|octets|oversize-pkts|pkts|pkts1024to1518octets|pkts128to255octets|pkts256to511octets|pkts512to1023octets|ptks64octets|pkts65to127octets|undersize-pkts]}<1-2147483647>{[absolute|delta]}**ring**<0-2147483647><1-65535>**falling**<0-2147483647><1-65535>**startup**{[falling|rising|rising-falling]}[owner Name]

no rmon alarm<1-65535>[owner NAME]

<1-65535> - Specify event index to create or modify.

port-id - Specify the interface to sample.

(variable) - Specify a mib object to sample.

<1-2147483647> - Specify the time in seconds that the alarm monitors the MIB variable.

(absolute|delta) - Specify absolute to compare sample counter absolutely.

<0-2147483647> - Specify a number which the alarm trigger rising event.

<1-65535> - Specify event index when the rising threshold exceeds.

<0-2147483647> - Specify a number which the alarm trigger falling event.

<1-65535> - Specify event index when the falling threshold exceeds.

falling|rising|rising-falling - Specify only to how rising or falling startup event. Or show either rising or falling startup event.

owner Name - Specify owner of alarm.

Default
Null

Command Mode
Global Configuration mode

Usage

Use the rmon alarm command to add or modify a RMON alarm entry. Before add alarm entry, at least one event entry must be added. Use the no form of this command to delete. You can verity settings by the show rmon alarm command.

Example

The example shows how to add RMON alarm entry that sample interface 1 packets delta count every 300 seconds.Trigger event index 1 if over than rising threshold 10000, trigger Event index 2 if lower than falling threshold.

```
 SC31020(config)# rmon event 1 log
SC31020(config)# rmon event 2 log
SC31020(config)# rmon alarm 1 interface GigabitEthernet 0/1 pkts 300 delta
  rising 1000 1 falling  100 1 startup rising-falling owner admin
SC31020# show rmon alarm 1
Rmon Alarm Index              : 1
Rmon Alarm Sample Interval    : 300
Rmon Alarm Sample Interface   : gi0/1
Rmon Alarm Sample Variable    : Pkts
Rmon Alarm Sample Type        : delta
Rmon Alarm Type               : Rising or Falling
Rmon Alarm Rising Threshold   : 1000
Rmon Alarm Rising Event       : 1
Rmon Alarm Falling Threshold : 100
Rmon Alarm Falling Event      : 1
Rmon Alarm Owner              : admin

SC31020(config)# rmon event 1 log trap public description test owner admin
SC31020# show rmon event 1
Rmon Event Index       : 1
Rmon Event Type        : Log and Trap
Rmon Event Community   : public
Rmon Event Description : test
Rmon Event Last Sent   :
```

RMON History

rmon history

Syntax

rmon history <1-65535>**interface** {port-id}[buckets<1-50>][interval<1-3600>][owner NAME]

no rmon history <1-65535>

<1-65535> - Specify event index to create or modify

port-id - Specify the interface to sample

buckets<1-50> - Specify the maximum number of buckets.

interval<1-3600> - Specify time interval for each sample

owner NAME - Specify owner of history

Default
Null

Command Mode
Global Configuration mode

Usage
Use the rmon history command to add or modify a RMON history entry. Use the no form of this command to delete. You can verity settings by the show rmon history command.

Example
The example shows how to add RMON history entry that monitor interface gig0/1 every 60 seconds and then modify it to monitor every 30 seconds.

```
SC31020(config)# rmon history 1 interface GigabitEthernet 0/1 interval 60
  owner admin
SC31020# show rmon history 1
Rmon History Index       : 1
Rmon Collection Interface: gi0/1
Rmon History Bucket      : 50
Rmon history Interval    : 60
Rmon History Owner       : admin

SC31020(config)# rmon history 1 interface GigabitEthernet 0/1 interval 30
  owner admin
SC31020# show rmon history 1
Rmon History Index       : 1
Rmon Collection Interface: gi0/1
Rmon History Bucket      : 50
Rmon history Interval    : 30
Rmon History Owner       : admin
```

Clear RMON Interface Statistics

clear rmon interface statistcs

Syntax

clear rmon interface {port-id} **statistics**

port-id - Specify the interface to clear

Default
Null

Command Mode
Privilege mode

Usage
Use the clear rmon interface statistics command to clear RMON etherStat Statistics those are recorded on interface.You can verity results by the show rmon interface statistics command.You can verity results by the **show rmon interface statistics** command.

Example
The example shows how to clear RMON etherStat Statistics on interface gig0/1.

```
SC31020# clear rmon interfaces GigabitEthernet 0/1 statistics
SC31020# show rmon interfaces GigabitEthernet 0/1 statistics
==== Port gi0/1 ==============================
etherStatsDropEvents       : 0
etherStatsOctets          : 0
etherStatsPkts           : 0
etherStatsBroadcastPkts          : 0
Example       etherStatsMulticastPkts    : 0
etherStatsCRCAlignErrors     : 0
etherStatsUnderSizePkts     : 0
etherStatsOverSizePkts      : 0
etherStatsFragments        : 0
etherStatsJabbers         : 0
etherStatsCollisions       : 0
etherStatsPkts64Octets      : 0
etherStatsPkts65to127Octets   : 0
etherStatsPkts128to255Octets  : 0
etherStatsPkts256to511Octets  : 0
etherStatsPkts512to1023Octets  : 0
etherStatsPkts1024to1518Octets   : 0
```

Show RMON Interface Statistics

show rmon interface statistcs

Syntax

show rmon interface {port-id} **statistics**

port-id - Specify the interface to show

Default
Null

Command Mode
Privilege mode

Usage
Use the show rmon interface statistics command to show RMON etherStat Statistics of interface You can verity results by the **show rmon interface statistics** command.

Example
The example shows how to show RMON etherStat Statistics on interface gig0/1.

```
SC31020# show rmon interfaces GigabitEthernet 0/1 statistics
==== Port gi0/1 ==============================
etherStatsDropEvents       : 0
etherStatsOctets         : 12313
etherStatsPkts           : 120
etherStatsBroadcastPkts     : 32
etherStatsMulticastPkts     : 85
etherStatsCRCAlignErrors    : 0
etherStatsUnderSizePkts     : 0
etherStatsOverSizePkts      : 0
etherStatsFragments         : 0
etherStatsJabbers           : 0
etherStatsCollisions        : 0
etherStatsPkts64Octets      : 11
etherStatsPkts65to127Octets   : 86
etherStatsPkts128to255Octets  : 23
etherStatsPkts256to511Octets  : 0
etherStatsPkts512to1023Octets  : 0
etherStatsPkts1024to1518Octets   : 0
```

Show RMON Event

show rmon event

Syntax

show rmon event [<1-65535>|all]

<1-65535> - Specify event index to show

all - Show all existing events

Default
Null

Command Mode
Privilege mode

Usage
Use the **show rmon event** command to show existed RMON event entry.

Example
The example shows how to show RMON event entry:

```
SC31020(config)#rmon event 1 log trap public description test owner admin
SC31020(config)# exit         //Returns the privilege mode
SC31020# show rmon event 1
Rmon Event Index       : 1
Rmon Event Type        : Log and Trap
Rmon Event Community   : public
Rmon Event Description : test
Rmon Event Last Sent   :
Rmon Event Owner       : admin
```

Show RMON Alarm

show rmon alarm

Syntax

show rmon alarm [<1-65535>|all]

<1-65535> - Specify alarm index to show

all - Show all existing alarms

Default
Null

Command Mode
Privilege mode

Usage
Use the **show rmon alarm** command to show existed RMON alarm entry.

Example
The example shows how to show RMON alarm entry:

```
SC31020(config)# SC31020(config)# rmon alarm 1 interface GigabitEthernet 0/1
  broadcast-pkts 300 delta rising 10000 1 falling 100 1 startup rising-falling
  owner admin
SC31020(config)# exit         //Returns the privilege mode
SC31020# show rmon alarm 1
Rmon Alarm Index             : 1
Rmon Alarm Sample Interval   : 300
Rmon Alarm Sample Interface  : gi0/1
Rmon Alarm Sample Variable   : BroadcastPkts
Rmon Alarm Sample Type       : delta
Rmon Alarm Type              : Rising or Falling
Rmon Alarm Rising Threshold  : 10000
Rmon Alarm Rising Event      : 1
Rmon Alarm Falling Threshold : 100
Rmon Alarm Falling Event     : 1
Rmon Alarm Owner             : admin
```

Show RMON History

show rmon history

Syntax

show rmon history [<1-65535>|all]

<1-65535> - Specify history index to show

all - Show all existing history

Default
Null

Command Mode
Privilege mode

Usage
Use the **show rmon history** command to show existed RMON history entry.

Example
The example shows how to show RMON history entry:

```
SC31020(config)# rmon history 1 interface GigabitEthernet 0/1 interval
30 owner admin
SC31020(config)# exit
SC31020# show rmon history 1
Rmon History Index       : 1
Rmon Collection Interface: gi0/1
Rmon History Bucket      : 50
Rmon history Interval    : 30
Rmon History Owner       : admin
```

15 ARP Inspection

ARP Inspection

arp inspection

Syntax

arp-inspection

no arp-inspection

Default
arp inspection is disabled

Command Mode
Global Configuration mode

Usage
Use the arp-inspection command to enable Dynamic Arp Inspection function. Use the no form of this command to disable.

Example
The example shows how to enable Dynamic Arp Inspection on VLAN 1. You can verify settings by the following show arp-inspection command.

```
SC31020(config)# arp-inspection
SC31020# show arp-inspection
Dynamic ARP Inspection     : enabled
Enable on Vlans            : 1-4094
```

ARP Inspection Rate Limit

arp inspection rate-limit

Syntax

arp-inspection rate-limit<1-50>

no arp-inspection rate-limit

<1-50> - Set 1 to 50 PPS of DHCP packet rate limitation

Default
default is unlimited of ARP packet

Command Mode
Interface Configuration mode

Usage
Use the arp-inspection rate-limit command to set rate limitation on interface. The switch drop ARP packets after receives more than configured rate of packets per second.use the no form of this command to return to default settings.

Example
The example shows how to set rate limit to 30 pps on interface gig0/1.You can verify settings by the following show arp-inspection interface command.

```
SC31020(config)# interface GigabitEthernet 0/1
SC31020(config-if-GigabitEthernet0/1)# arp-inspection rate-limit 30
SC31020(config-if-GigabitEthernet0/1)# end   //Returns the privilege mode
SC31020# show arp-inspection interfaces GigabitEthernet 0/1

Interfaces|Trust State|Rate(pps)|SMAC Check|DMAC Check|IP Check/Allow Zero|
----------+-----------+---------+----------|----------+-------------------+
  gi0/1   | Untrusted |    30   | disabled | disabled | disabled/disabled
```

ARP Inspection Trust

arp inspection trust

Syntax

arp-inspection trust

no arp-inspection trust

Default
ARP inspection trust is disabled

Command Mode
Interface Configuration mode

Usage
Use the arp-inspection trust command to set trusted interface.The switch does not check ARP packets that are received on the trusted interface; it simply forwards It. Use the no arp-inspection trust form of this command to set untrusted interface.

Example
The example shows how to set interface gig0/1 to trust.You can verify settings by the following show arp-inspection interface command.

```
SC31020(config)# interface GigabitEthernet 0/1
SC31020(config-if-GigabitEthernet0/1)# arp-inspection trust
SC31020(config-if-GigabitEthernet0/1)# do show arp-inspection interfaces
GigabitEthernet 0/1

Interfaces|Trust State|Rate(pps)|SMAC Check|DMAC Check|IP Check/Allow Zero|
----------+-----------+---------+----------|----------+-------------------+
  gi0/1   |  Trusted  |   None  | disabled | disabled | disabled/disabled
```

ARP Inspection Validate

arp inspection validate

Syntax

arp-inspection validate{[src-mac|dst-mac|ip[allow-zeros]]}

no arp-inspection validate{[src-mac|dst-mac|ip[allow-zeros]]}

src-mac - The”src-mac”drop ARP requests and reply packets that arp-sender-mac and ethernet-source-mac is not Match.

dst-mac - The”dst-mac”drops ARP reply packets that arp-target-mac and ethernet-dest-mac is not match.

ip - The”ip”drop ARP request and reply packets that Sender-ip is invalid such as broadcast, multicast, all zero IP address and drop ARP reply packets that Target-ip is invalid.

allow-zeros - The”allow-zeros”means won’t drop all zero IP address.

Default
Default is disabled of all validation

Command Mode
Interface Configuration mode

Usage
Use the arp-inspection validate command to enable validate function on interface. Use the no arp-inspection validate form of this command to disable validation.

Example
The example shows how to set interface gi1 to validate “src-mac”, “dst-mac” and “ip allow zeros”. You can verify settings by the following show ip arp inspection interface command.

```
SC31020(config-if-GigabitEthernet0/1)# arp-inspection validate src-mac
SC31020(config-if-GigabitEthernet0/1)# arp-inspection validate dst-mac
SC31020(config-if-GigabitEthernet0/1)# arp-inspection validate ip allow-zeros
SC31020(config-if-GigabitEthernet0/1)# do show arp-inspection interfaces
GigabitEthernet 0/1

Interfaces|Trust State|Rate(pps)|SMAC Check|DMAC Check|IP Check/Allow Zero|
----------+-----------+---------+----------|----------+-------------------+
  gi0/1   | Untrusted |   None  | enabled  | enabled  |  enabled/enabled
```

Clear ARP Inspection Statistics

clear arp inspection interfaces statistics

Syntax

clear arp-inspection interfaces {port-id} statistics

port-id - Specifies ports to clear statistics

Default
Null

Command Mode
Privilege mode

Usage
Use the clear arp-inspection interfaces {port-id} statistics command to clear statistics that are recorded on interface.

Example
The example shows how to clear statistics on interiface gig0/1t.You can verify settings by the following show arp-inspection interface statistics command.

```
SC31020# clear arp-inspection interfaces GigabitEthernet 0/1 statistics
SC31020# show arp-inspection interfaces GigabitEthernet 0/1 statistics

Port|Forward|Source MAC Failures|Dest MAC Failures|SIP Validation Failures|
DIP Validation Failures|IP-MAC Mismatch Failures
----+-------+-------------------+-----------------+-----------------------+-
  ----------------------+------------------------
gi0/1|  0   |           0        |        0        |            0          |
           0          |            0
```

Show ARP Inspection

clear arp inspection interfaces statistics

Syntax

show arp-inspection interfaces

Default

Null

Command Mode

Privilege mode

Usage

Use the show arp-inspection command to show settings of ARP Inspection.

Example

The example shows how to show settings of arp inspection:

```
SC31020# show arp-inspection
Dynamic ARP Inspection     : enabled
Enable on Vlans            : 1-4094
```

Show ARP Inspection Interface

show arp inspection interfaces

Syntax

show arp-inspection interfaces {port-id}

show arp-inspection interfaces {port-id}statistics

Default

Null

Command Mode

Privilege mode

Usage

Use the show arp-inspection interfaces command to show settings or statistics of interface.

Example

The example shows how to show settings of interface gig0/1:

```
SC31020# show arp-inspection interfaces GigabitEthernet 0/1

Interfaces|Trust State|Rate(pps)|SMAC Check|DMAC Check|IP Check/Allow Zero|
----------+-----------+---------+----------|----------+-------------------+
  gi0/1   | Untrusted |   None  | disabled | disabled | disabled/disabled

SC31020# show arp-inspection interfaces GigabitEthernet 0/1 statistics

Port|Forward|Source MAC Failures|Dest MAC Failures|SIP Validation Failures|
DIP Validation Failures|IP-MAC Mismatch Failures
----+-------+------------------+-----------------+-----------------------+-
  ----------------------+------------------------
gi0/1|  0   |           0        |        0        |            0          |
            0          |            0
```

16 Flow Control Commands

Flow Control Configuration Command

flowcontrol Turn on port flow control

Syntax

flowcontrol {[on|off]}

on - Turn on flow control

off - Turn off flow control

Default
Turn off flow control.

Command Mode
Interface configuration mode

Usage
Use this command to enable or disable port flow control.

Example
The example shows how to enable Dynamic Arp Inspection on VLAN 1. You can verify settings by the following show arp-inspection command.

```
SC31020(config-if-GigabitEthernet0/1)# flowcontrol on
```

show interfaces View interface status information

Syntax

show interfaces {port-id}

17 VLAN Commands

Configure Commands

VLAN description Configure the name of the VLAN.Use this command's no option to revert the setting to a default value.

Syntax

description vlan-name

no description

vlan-nameThe name of the vlan

Default
VLAN default name is: VLAN?VLAN ID,eg: VLAN 2 default name”VLAN0002”

Command Mode
VLAN Configuration mode

Usage
Use show vlan to view the configure of vlan.

Example

```
SC31020(config)# vlan 3
SC31020(config-vlan)# description nihao
```

show vlan Display VLAN member ports and other information.

Syntax

show vlan

vlan-id Use command vlan vlan-id to inter configuration mode. Use the no option of the command to remove the existing VLAN.

Syntax

vlan vlan-id

no vlan vlan-id

vlan - VLAN ID number(1-4094). Notice: The default VLAN, VLAN 1, cannot be deleted

Default
vlan1

Command Mode
Global Configuration mode

Usage
If the input VLAN vlan-id does not exist, the system requirement creates VLAN and enters the vlan. Existence goes into VLAN.

Example

```
SC31020(config)# vlan 5
SC31020(config)# no vlan 5
```

show vlan Display VLAN member ports and other information.

Syntax

show vlan

Switch Mode

switch mode Using this command specifies a two - layer interface (switch port) mode, which can be specified as access /trunk/hybrid port. Use the switch mode access option to revert the schema of the interface to default values.

Syntax

switch mode [access | trunk | hybrid]

access - Configure a switch port mode is access

trunk - Configure a switch port mode is trunk

hybrid - Configure a switch port mode is hybrid

Default
The switch port default mode is access

Command Mode
Interface Configuration mode

Usage
If a switch port mode is access this port can only be a member of a VLAN. Use command **switch access vlan** specifies which VLAN is the member of the interface. If a switch port mode trunk or hybrid and this port can be a member of multiple VLANs this port Which VLAN the interface can belong to is determined by the licensing VLAN list of the interface, trunk port or hybrid port are all VLAN members in the list of license VLAN. Use **switch {trunk | hybrid}** command to define the licensing VLAN list of interfaces.

Example
Configure the port1 mode is trunk:

```
SC31020(config)# interface GigabitEthernet 0/1
SC31020(config-if-GigabitEthernet0/1)# switch mode trunk
```

show vlan Display VLAN member ports and other information.

Syntax

show vlan

Management VLAN

management vlan Use command management-vlan vlan vlan-id to inter configuration mode. Use the no option of the command to remove the create management-vlan.

Syntax

Management-vlan vlan vlan-id

no management-vlan

vlan-id - VLAN ID number(1-4094)

Default
management-vlan vlan 1

Command Mode
Global Configuration mode

Usage
If the input VLAN vlan-id does not exist, the system requirement creates VLAN and enters the vlan. Existence goes into VLAN.

Example

```
SC31020(config)# management-vlan vlan 4
SC31020(config)# no management-vlan
```

show vlan Display VLAN member ports and other information.

Syntax

show vlan

Configure Different Types of VLAN

switch access vlan In port mode, configure the access attribute of the port.

Syntax

switch access vlan vlan-id

vlan-id - Port to join VLAN's ID

Default
Port default mode is access. Default VLAN is VLAN 1.

Command Mode
Interface Configuration mode

Usage
Enter a VLAN ID. If the input is an VLAN ID that is not created the device will indicate that the VLAN does not exist. If the input is already existing VLAN ID, the VLAN member port is increased.

Example
Configure port 1 belong to vlan 2:

```
SC31020(config)# interface GigabitEthernet 0/1
SC31020(config-if-GigabitEthernet0/1)# switch access vlan 2
```

show vlan Display VLAN member ports and other information.

Syntax

show vlan

switch trunk allowed vlan

Specify a native VLAN for a trunk port and a list of permissions to configure this Trunk port VLAN. Use the no option of this command to restore the trunk property of the interface to the default value.

Syntax

switch trunk allowed vlan vlan-id

no switch trunk allowed vlan

allowed vlan vlan-list - Configure the permission VLAN list for this Trunk port. The parameter vlan-list can be either a VLAN or a series of VLAN, beginning with a small VLAN ID and ending with a large VLAN ID, with the (-) symbolic connection in the middle. Such as: 10-20. Segments can be separated by symbols, such as: 1-10,20-25,30,33. The meaning of all is that the permission VLAN list contains all supported VLAN; the add indicates that the specified VLAN list is added to the license VLAN list; the remove indicates that the specified VLAN list is removed from the license VLAN list.

Default
Port default mode is access. Default VLAN is VLAN 1.

Command Mode
Interface Configuration mode

Usage
Enter a VLAN ID.If the input is an VLAN ID that is not created the device will indicate that the VLAN does not exist. If the input is already existing VLAN ID, the VLAN member port is increased.

Example
Configure port 1 belong to vlan 3:

```
SC31020(config)# interface GigabitEthernet 0/1
SC31020(config-if-GigabitEthernet0/1)# switch trunk allowed vlan 3
```

show vlan

Display VLAN member ports and other information.

Syntax

show vlan

switch trunk native vlan

Specify a native VLAN for a trunk port and a list of permissions to configure this Trunk port VLAN. Use the no option of this command to restore the trunk property of the interface to the default value.

Syntax

switch trunk native vlan vlan-id

no switch trunk native vlan

native vlan - Trunk port message received, if the message with VLAN mark, then put this message to the corresponding VLAN tag, if the message with no VLAN mark, then the message is forwarded to the port of native VLAN.

Default
Default VLAN is VLAN 1.

Command Mode
Interface Configuration mode

Usage
To configure the Trunk native VLAN of a port, this port must be the trunk property.

Example
Configure gig0/1 belong to native vlan3:

```
SC31020(config)# interface gig 0/1
SC31020(config-if-GigabitEthernet0/1)# switch trunk native vlan 3
```

show vlan Display VLAN member ports and other information.

Syntax

show vlan

switch hybrid native vlan Specify a native VLAN for a hybrid port. Use the no option of this command to restore the Hybrid property of the interface to the default value.

Syntax

switch hybrid native vlan vlan-id

no switch hybrid native vlan

no - Restore Hybrid default VLAN

Default
Default native vlan is vlan 1

Command Mode
Interface Configuration mode

Usage
To configure the Hybrid native VLAN of a port, this port must be the Hybrid property.

Example

```
SC31020(config)# interface GigabitEthernet 0/1
SC31020(config-if-GigabitEthernet0/1)# switch hybrid native vlan 3
```

show vlan Display VLAN member ports and other information.

Syntax

show vlan

Display Relevant Commands

show vlan Display VLAN member ports and other information.

Syntax

show vlan [id vlan-id]

vlan-idThe number of VLAN ID

Default
Show all information by default

Command Mode
Privileged mode

Usage
To return to privileged mode, enter the end command, or type the Ctrl+Z combination key. To return to global configuration mode, enter the exit command.

Example

```
SC31020# show vlan 3

VID   |    VLAN Name    |   Untagged Ports   |  Tagged Ports    |   Type
------+-----------------+--------------------+------------------+---------
3     |    VLAN0003     |        gi0/1       |      ---         |  Static
```

show vlan Display VLAN member ports and other information.

Syntax

show vlan

18 Voice LAN

Configure Commands

voice-lan First create a VLAN, and voice VLAN to specify a VLAN has been created to enable the voice VLAN ID. Use the “no” command to close voice VLAN .Voice VLAN is disable by default.

Syntax

voice-vlan vlan id

voice-vlan

no voice-vlan

voice-vlan vlan id - The number of voice-vlan id. Notice: The voice vlan ID can not be same as surveillance vlan ID

Default
Null

Command Mode
Global Configuration mode

Usage
Use show voice-vlan to view the configure of voice-vlan.

Example

```
SC31020(config)# voice-vlan vlan 2
SC31020(config)# voice-vlan
```

show voice-vlan View global configuration information for voice VLAN.

Syntax

show voice-vlan

voice-vlan mode Using this command specifies a two - layer interface (switch port) mode, which can be specified as autotag/autountag/manual for switch port. Use the voice-vlan mode autoTag option to revert the schema of the interface to default values. Notice:Ports can not configure voice-vlan on the access port!

Syntax

Voice-vlan mode [autoTag | autounTag | manual]

autoTag - The voice VLAN mode for configuring ports is autoTag

autounTag - The voice VLAN mode for configuring ports is autounTag

manual - The voice VLAN mode for configuring ports is manual

Default
The voice-vlan default mode is autoTag.

Command Mode
Interface Configuration mode

Usage
If the port set voice VLAN mode is autoTag, the port is automatically joined with voice VLAN, with tag. If the mode is autountag, the port is automatically added to the voice VLAN without tag. Note: when adding the voice VLAN mode to manually join the port, you need to forward the port to the voice VLAN in advance.

Example
Configure port 1 to join voice VLAN as autotag

```
SC31020(config)# interface GigabitEthernet 0/1
SC31020(config-if-GigabitEthernet0/1)# voice-vlan  mode autoTag
```

show voice-vlan View global configuration information for voice VLAN.

Syntax

show voice-vlan

voice-vlan oui-table In global configuration mode, set OUI-table and note that the MAC address cannot be multicast and broadcast addresses. Mask cannot enter zero before F.

Syntax

voice-vlan oui-table A:B:C:D:E:F mask

voice-vlan oui-table - Match the filter's source MAC address for the incoming message

Default
The voice-vlan oui-table defaults to 8 rules.

Command Mode
Global Configuration mode

Usage
In global settings, oui-table adds the port to the voice VLAN when the port's source MAC address matches the address in the oui list

Example
Configure voice VLAN OUI

```
SC31020(config)# voice-vlan oui-table 02:00:12:32:56:89 mask
  FF:FF:FF:FF:FF:00
```

show voice-vlan interfaces GigabitEthernet 0/1

Display configuration of voice-vlan oui-table information

Syntax

show voice-vlan interfaces GigabitEthernet 0/1

voice VLAN aging-time and cos

In global configuration mode, set voice VLAN aging-time (1-65535)and cos (0-7).

Syntax

voice-vlan aging-time X(1-65535)

voice-vlan cos X(0-7) remark

Aging-time - Specifies the aging time of the port in voice VLAN

cos - Specify the voice VLAN Class Of Service

Default
The default aging-time is 720 minutes.
The default cos value is 5.

Command Mode
Global Configuration mode

Usage
The aging time and the cos value refer to the survival time and the priority of the voice message after the port is added to the voice VLAN.

Example
Configure voice VLAN aging-time is 30 minutes and cos value is 7

```
SC31020(config)# voice-vlan aging-time 30
SC31020(config)# voice-vlan cos 7 remark
```

show voice-vlan Display configuration of voice-vlan aging-time and cos information.

Syntax

show voice-vlan

Display Relevant Commands

show voice VLAN Display VLAN member ports and other information.

Syntax

Show vlan id

Show voice-vlan device

Vlan-id - The number of voice VLAN ID

Voice-vlan device - The ports in voice VLAN

Default
Show voice-vlan global information by default.
Show the ports in voice vlan by default

Command Mode
Privileged mode

Usage
To return to privileged mode, enter the end command, or type the Ctrl+Z combination key. To return to global configuration mode, enter the exit command.

Example

```
SC31020# show voice-vlan device

Interface  |    MAC Address    |        start-time
-----------+-------------------+--------------------------
gi0/1      |    00E0.BB00.0000 |    2020-01-01 00:24:03
```

```
SC31020# show vlan 2
VID  |   VLAN Name  |  Untagged Ports  |  Tagged Ports  |  Type
-----+--------------+------------------+----------------+---------
  2  |   VLAN0002   |        ---       |      gi0/1     | Static
```

show vlan Display configuration of voice-vlan information.

Syntax

show vlan vlan-id

show voice-vlan device Display the information of ports join voice-vlan.

Syntax

show voice-vlan device

19 Surveillance VLAN

Configure Commands

surveillance-vlan

First create a VLAN, and surveillance VLAN to specify a VLAN has been created to enable the surveillance VLAN ID. Use the “no” command to close surveillance VLAN surveillance VLAN is disable by default.

Syntax

surveillance-vlan vlan id

surveillance-vlan

no surveillance-vlan

surveillance-vlan vlan id - The number of surveillance-vlan id. Notice: The surveillance vlan ID can not be same as voice vlan ID

Default
Null

Command Mode
Global Configuration mode

Usage
Use show surveillance-vlan to view the configure of surveillance-vlan.

Example

```
SC31020(config)# surveillance-vlan vlan 3
SC31020(config)# surveillance-vlan
```

show surveillance-vlan

View global configuration information for surveillance VLAN.

Syntax

show surveillance-vlan

surveillance-vlan mode

Using this command specifies a two - layer interface (switch port)mode, which can be specified as auto/manual for switch port. Use the surveillance-vlan

mode auto option to revert the schema of the interface to default values.Ports can not configure surveillance-vlan on the access port!

Syntax

surveillance-vlan mode [auto| manual]

auto - The surveillance VLAN mode for configuring ports is autoTag

manual - The surveillance VLAN mode for configuring ports is manual

Default
The surveillance-vlan default mode is auto.

Command Mode
Interface Configuration mode

Usage
If the port set surveillance VLAN mode is auto, the port is automatically joined with surveillance VLAN,.Note: when adding the surveillance VLAN mode to manually join the port, you need to forward the port to the surveillance VLAN in advance.

Example
Configure port 1 to join surveillance VLAN as auto:

```
SC31020(config)# interface GigabitEthernet 0/1
SC31020(config-if-GigabitEthernet0/1)# surveillance-vlan  mode auto
```

show surveillance-vlan interfaces GigabitEthernet 0/1

View configuration information for voice VLAN

Syntax

show surveillance-vlan interfaces GigabitEthernet 0/1

surveillance-vlan oui-table

In global configuration mode, set OUI-table and note that the MAC address cannot be multicast and broadcast addresses. Mask cannot enter zero before F.

Syntax

surveillance-vlan oui-table A:B:C:D:E:F

mask A:B:C:D:E:F

surveillance-vlan oui-table - Match the filter's source MAC address for the incoming message

Default
Null

Command Mode
Global Configuration mode

Usage
In global settings, oui-table adds the port to the surveillance VLAN when the port's source MAC address matches the address in the oui list.

Example
Configure voice VLAN OUI:

```
SC31020(config)# surveillance-vlan oui-table 04:10:12:32:56:89 mask
  FF:FF:FF:FF:FF:00 componentType video_encoder
```

show surveillance-vlan

Display configuration of surveillance-vlan oui-table information.

Syntax

show surveillance-vlan

surveillance VLAN aging-time and cos

In global configuration mode, set surveillance VLAN aging-time (1-65535) and cos (0-7).

Syntax

surveillance-vlan aging-time X(1-65535)

surveillance-vlan cos X(0-7) remark

Aging-time - Specifies the aging time of the port in surveillance VLAN

cos - Specify the surveillance VLAN Class Of Service

Default
The default aging-time is 720 minutes.
The default cos value is 5

Command Mode
Global Configuration mode

Usage
The aging time and the cos value refer to the survival time and the priority of the surveillance message after the port is added to the voice VLAN

Example
Configure surveillance VLAN aging-time is 20 minutes and cos value is 7

```
SC31020(config)# surveillance-vlan aging-time 20
SC31020(config)# surveillance-vlan cos 7 remark
```

show surveillance-vlan

Display configuration of surveillance-vlan aging-time and cos information

Syntax

show surveillance-vlan

Display Relevant Commands

show surveillance VLAN

Display VLAN member ports and other information.

Syntax

Show vlan id

Show surveillance-vlan device

Vlan-id - The number of surveillance VLAN ID

surveillance-vlan device - The ports in surveillance VLAN

Default
Show surveillance-vlan global information by default.
Show the ports in surveillance vlan by default

Command Mode
Privileged mode

Usage
To return to privileged mode, enter the end command, or type the Ctrl+Z combination key. To return to global configuration mode, enter the exit command.

Example

```
SC31020# show surveillance-vlan device
Interface  |  Component Type  |  Description  |  MAC Address  |  start-time
-----------+------------------|---------------|---------------+------------
gi0/1      |Other IP Surveillance Device|     |0410.1232.5689 | 2020-01-01
  17:31:03
```

```
SC31020# show vlan 3

VID  |  VLAN Name  |   Untagged Ports   |   Tagged Ports   |  Type
-----+-------------+--------------------+------------------+---------
  3  |  VLAN0003   |         ---        |       gi0/1      |  Static
```

show vlan Display configuration of surveillance-vlan information.

Syntax

show vlan vlan-id

show surveillance-vlan device Display the information of ports join surveillance-vlan

Syntax

Show surveillance-vlan device

20 DHCP Snooping

Configure Commands

dhcp-snooping Enable DHCP-Snooping,If a port is a non trusted port, then the port discards the service message (DHCP_OFFER, DHCP_ACK, DHCP_NCK). If a port is a trusted port, then the port can forward the service message normally.

Syntax

dhcp-snooping

no dhcp-snooping

dhcp-snooping - Enable dhcp-snooping

no dhcp-snooping - Disable dhcp-snooping

Default
Disable

Command Mode
Global Configuration mode

Usage
In the global configuration mode, after opening the DHCP-snooping function, you can effectively prevent illegal servers from being established.

Example

```
SC31020(config)# dhcp-snooping
```

show dhcp-snooping Displays the current configuration.

Syntax

show dhcp-snooping

dhcp-snooping trust Open the DHCP-Snooping trust function, if a port is a non trusted port, then the port service message received will be discarded if a port to port the port trust can normal forwarding service Message.

Syntax

dhcp-snooping trust

no dhcp-snooping trust

dhcp-snooping trust - Configure the port is dhcp-snooping trust

no dhcp-snooping trust - Configure the port is dhcp-snooping untrust

Default
Untrust

Command Mode
Interface Configuration mode

Usage
In port mode, when the port is opened, the port can forward the service message. If this port is a non trusted port, then the port cannot forward the service message.

Example

```
SC31020(config-if-GigabitEthernet0/2)# dhcp-snooping trust
```

show dhcp-snooping Displays the current configuration.

Syntax

show dhcp-snooping

dhcp-snooping vlan Enable DHCP snooping information 82 for VLAN

Syntax

dhcp-snooping vlan

dhcp snooping vlan - Enable the dhcp snooping vlan

Default
Enable

Command Mode
Global Configuration mode

Usage
There be DHCP snooping information 82 for VLANs enabled

Example

```
SC31020(config)# dhcp-snooping vlan 1-4094
```

show dhcp-snooping Display DHCP snooping information

Syntax

show dhcp-snooping

dhcp-snooping option Enable DHCP snooping option 82

Syntax

dhcp-snooping option

Default
Disable

Command Mode
Interface Configuration mode

Usage
There be DHCP snooping information 82 enabled.

Example

```
SC31020(config-if-GigabitEthernet0/1)# dhcp-snooping option
```

show dhcp-snooping Display dhcp snooping information

Syntax

show dhcp-snooping

dhcp-snooping option remote-id Enable DHCP snooping option 82

Syntax

dhcp-snooping option remote-id

STRING - ID string (1~63)

Default
DUT's mac address

Command Mode
Global Configuration mode

Usage
A "remote ID" containing the switch's information as a trusted identifier for the remote high-speed modem.

Example

```
SC31020(config)# dhcp-snooping option remote-id 192.168.100.145
```

show dhcp-snooping Display dhcp snooping information

Syntax

show dhcp-snooping

dhcp-snooping option circuit-id configure DHCP snooping information 82 of circuit-ID.

Syntax

dhcp-snooping option circuit-id

STRING - ID string (1~63)

Default
Null

Command Mode
Interface Configuration mode

Usage
It indicates that the received DHCP request message is from the link identifier.

Example

```
SC31020(config-if-GigabitEthernet0/1)# dhcp-snooping option circuit-id
  192.168.100.145
```

show dhcp-snooping interfaces GigabitEthernet 0/x

Display DHCP snooping of cid information

Syntax

show dhcp-snooping interfaces GigabitEthernet 0/x

dhcp-snooping option action

Configure global DHCP snooping policy

Syntax

dhcp-snooping option action (drop| keep | replace)

drop - Drop packets with option82

keep - Keep original option82

replace - Replace option82 content by switch setting

Default
The global DHCP relay policy shall be drop.

Command Mode
Global Configuration mode

Usage
DHCP snooping information 82 policy.

Example

```
SC31020(config-if-GigabitEthernet0/1)# dhcp-snooping option action drop
```

show dhcp-snooping interfaces GigabitEthernet 0/x

Display DHCP snooping information

Syntax

show dhcp-snooping interfaces GigabitEthernet 0/x

Configure Commands

show dhcp-snooping Displays the current DHCP-Snooping open, shutdown, and configuration information.

Syntax

show DHCP-Snooping

Show DHCP-Snooping interface gigabitEthernet 0/x

show dhcp-snooping - Displays the current DHCP-Snooping configuration information

show dhcp-snooping interfacegigabitEthernet 0/x - Displays the current DHCP-Snooping configuration on port or Aggregateport(1-8)

Default
Null

Command Mode
Privileged mode

Usage
View the current DHCP-snooping information.

Example

```
SC31020# show dhcp-snooping

DHCP Snooping : enabled
Enable on following Vlans : 1-4094
circuit-id default format : vlan-port
remote-id : 00:e0:4c:00:00:00 (Switch Mac in Byte Order)

SC31020# show dhcp-snooping interfaces GigabitEthernet 0/1

Interfaces | Trust State | Rate (pps) | hwaddr Check | Insert Option82 |
-----------+-------------+------------+--------------+-----------------+
gi0/1      |  Untrusted  |     None   |   disabled   |     disabled    |
```

show dhcp-snooping Displays the current DHCP-Snooping configuration information.

Syntax

show dhcp-snooping

show dhcp-snooping interfacegigabitEthernet 0/x

Displays the current DHCP-Snooping configuration on port or Aggregateport(1-8)

Syntax

show dhcp-snooping

21 Loopback Detection

Configure Commands

loopback-detection

Configure loop detection, activate this function, and when loop appears on the network, the loop port is directly link-down or issued a warning.

Syntax

Loopback-detection [enable | ctp-interval | resume-interval | snmp-trap]

enable - enable loop detection function defaults is disable

ctp-interval - ctp sending interval(1-32767)

resume-interval - Port automatic recovery time interval(0,60-1000000) default '60',set '0' means no auto-resume

snmp-trap - Decide whether to send an alarm message. You need to start the SNMP function and SNMP trap first

Default
Null

Command Mode
Global Configuration mode

Usage
In the global mode, configuration loopback-detection

Example
Configure the loopback-detection enable, ctp-interval, resume-interval, resume-interval, snmp-trap.

```
SC31020(config)# loopback-detection enable
SC31020(config)# loopback-detection ctp-interval 1
SC31020(config)# loopback-detection resume-interval 60
SC31020(config)# loopback-detection snmp-trap
```

show loopback-detection

View the current loop detection status and configuration information.

Syntax

show loopback-detection

Display Relevant Commands

show loopback-detection Use the following command to see loop detection information.

Syntax

show loopback-detection

Default
Null

Command Mode
Privileged mode

Usage
Check loop-detection port configuration and status

Example
Check loop-detection port configuration and status.

```
SC31020# show loopback-detection

Loopback detection configuration
Loopback detection : enabled
CTP tx interval : 10
Port resume interval : 60
Loopback detection trap: enabled
Interfaces |   State | Result |
-----------+---------+--------+
gi0/1      | enabled | NORMAL |
gi0/2      | enabled | NORMAL |
gi0/3      | enabled | NORMAL |
gi0/4      | enabled | NORMAL |
gi0/5      | enabled | NORMAL |
gi0/6      | enabled | LOOP-SHUTDOWN |
gi0/7      | enabled | NORMAL |
gi0/8      | enabled | NORMAL |
gi0/9      | enabled | NORMAL |
gi0/10     | enabled | NORMAL |
agg1       | enabled | LOOP-SHUTDOWN
```

show loopback-detection View the current port loop detection status and configuration information.

Syntax

show loopback-detection

22 Spanning-tree

Configure Commands

spanning-tree enable

Enable spanning-tree function, that is to avoid the loop, enable spanning tree function switch will block loop port according to the port role.

Syntax

spanning-tree enable

no spanning-tree enable

enable - Enable spanning-tree

no - Disable spanning-tree

Default
Disabled

Command Mode
Global Configuration mode

Usage
In the global mode, configuration spanning-tree.

Example
Configuring the spanning tree to turn on and off.

```
SC31020(config)# spanning-tree enable
SC31020(config)# no spanning-tree enable
```

show spanning-tree

View the current spanning tree status and configuration information.

Syntax

show spanning-tree

spanning-tree mode

Configure spanning-tree mode, there are three versions: stp, rstp, mstp

Syntax

spanning-tree mode [rstp|stp|mstp]

stp - Running the stp protocol

rstp - Running the rstp protocol

mstp - Running the mstp protocol

Default
rstp

Command Mode
Set the spanning tree protocol version of the switch running in global mode

Usage
In the global mode, configuration spanning-tree.

Example
Set the protocol version of the switch running to RSTP

```
SC31020(config)# spanning-tree mode rstp
```

show spanning-tree View the current spanning tree status and configuration information.

Syntax

show spanning-tree

spanning-tree forward-time Configure spanning-tree forward-time, default 15s.

Syntax

spanning-tree forward-time [4-30s]

forward-time - Forwarding delay, the time interval in which a port switches from one state to another.

Default
15

Command Mode
Global Configuration mode

Usage
Configuring forwarding delay in global mode.

Example
Configuring spanning-tree forwarding delay.

```
SC31020(config)# spanning-tree forward-time 17
```

show spanning-tree

View the current spanning tree status and configuration information.

Syntax

show spanning-tree

spanning-tree hello-time

Configure the spanning tree to send BPDU messages to neighboring devices at intervals, that is, the transmission frequency of BPDU.

Syntax

spanning-tree hello-time [1-10s]

Default
2

Command Mode
Global Configuration mode

Usage
Set the transmit frequency of the BPDU in the switch in global mode.

Example
Configuring the spanning tree BPDU transmission interval:

```
SC31020(config)# spanning-tree hello-time 5
```

show spanning-tree

View the current spanning tree status and configuration information.

Syntax

show spanning-tree

spanning-tree max-age

Configure port BPDU aging time. Exchange the opportunity to maintain a timer aging, every time after receipt of BPDU from the new timing, when participating in compute a spanning tree port (root port and port blocking) in a

max-age BPDU message is not received after a timeout, the switch will recalculate the topology.

Syntax

spanning-tree max-age [6-40s]

Default
20

Command Mode
Global Configuration mode

Usage
Set the BPDU timeout time of the switch in global mode.

Example
Set the BPDU timeout of the switch to 30 seconds:

```
SC31020(config)# spanning-tree max-age 30
```

show spanning-tree View the current spanning tree status and configuration information.

Syntax

show spanning-tree

spanning-tree max-hops The maximum BPDU hops of the switch-port, BPDU, is reduced by 1 per passing device. If the switch receives a hops value of 0, the BPDU message will be discarded, and the switch will control the spanning tree size by that value.

Syntax

spanning-tree max-hops [1-40]

Default
20

Command Mode
Global Configuration mode

Usage
Sets the maximum hops count of the switch BPDU in global mode.

Example
Set the BPDU maximum hops count to 30 times:

```
SC31020(config)# spanning-tree max-hops 30
```

show spanning-tree View the current spanning tree status and configuration information.

Syntax

show spanning-tree

spanning-tree pathcost metod By default, the port automatically calculates path consumption based on port rate and specifies the criteria used when calculating path consumption. There are two calculation criteria: **dot1D-1998** and **dot1T-2001**.

Syntax

spanning-tree pathcost method [dot1D-1998 | dot1T-2001]

dot1D-1998 - Using the dot1D-1998 port path consumption calculation criteria

dot1T-2001 - Using the dot1T-2001 port path consumption calculation criteria

Default
dot1T-2001

Command Mode
Global Configuration mode

Usage
In global mode, set the calculation method of switch port path consumption value.

Example
Configure the port consumption value is calculated as dot1D-1998:

```
SC31020(config)# spanning-tree pathcost method dot1D-1998
```

show spanning-tree View the current spanning tree status and configuration information.

Syntax

show spanning-tree

spanning-tree priority

The bridge priority setting spanning-tree, select one of the highest priority switches as the root bridge.

Syntax

spanning-tree priority [0-61440]

priority [0-61440]Configure the bridge priority of the switch, range 0-61440, and must be a multiple of 4096, default 32768

Default

32768

Command Mode

Global Configuration mode

Usage

Set switch bridge priority in global mode.

Example

Set the switch bridge priority to 4096:

```
SC31020(config)# spanning-tree priority 4096
```

show spanning-tree

View the current spanning tree status and configuration information.

Syntax

show spanning-tree

spanning-tree mst configure

Configure the mstp parameters.

Syntax

spanning-tree mst configuration [cr | instance | name | revision | no]}

spanning-tree mst instance (0-15) priority (0-61440)

spanning-tree mst configure - Enter the MSTP configuration mode Note that "cr" means no arguments are entered

Instance (1-15) vlan (1-4094) - Configure the mapping relationship between the MSTP instance and the VLAN

name - Configuration Bridge name (Max.32 characters)

revision - Mstp revision level (0-65535)

No instance x - Delete the exit instance

No name - Delete the instance name

No revision - Delete the revision

Spanning-tree mst instance (1-15) priority(0-61440) - Configure the mstp instance priority,it must multiples of 4096

Default
Null

Command Mode
Global Configuration mode

Usage
Set mstp information,if create a same as other devices region,you should be ensure that the MSTP version, name, instance mapping relationship of the 2 devices are the same.

Example
Set the switch mst instance is 5, name is nihao, revision is 33 and configure the instance 5 priority is 4096:

```
SC31020(config)# spanning-tree mst configuration
SC31020(config-mst)# instance 5 vlan 5
SC31020(config-mst)# name nihao
SC31020(config-mst)# revision 33
SC31020(config)# spanning-tree mst instance 5 priority 4096
```

show spanning-tree mst configuration

View the current spanning-tree mstp status and configuration information.

Syntax

show spanning-tree mst configuration

spanning-tree enable

[no] Enable spanning-tree on switch-port

Syntax

spanning-tree [enable]

no spanning-tree enable

enable - Enabled port spanning tree function, the default all ports open the spanning tree function

Default
Null

Command Mode
Port Configuration mode

Usage
Enter the port configuration mode and open / close the spanning tree function of the port.

Example
Open and close the spanning tree function of GigabitEthernet0/1:

```
SC31020(config-if-GigabitEthernet0/1)# spanning-tree enable
SC31020(config-if-GigabitEthernet0/1)# no spanning-tree enable
```

show spanning-tree interface gigabitEthernet 0/1

Display the spanning tree status and configuration information of GigabitEthernet0/1.

Syntax

show spanning-tree interface gigabitEthernet 0/1

spanning-tree bpdu

Configuring ports to handle BPDU.

Syntax

spanning-tree bpdu [filter|guard]

filter - Configuration port neither receives nor sends BPDU messages

guard - Do not receive BPDU messages

Default
Null

Command Mode
Port Configuration mode

Usage
Enter the port configuration mode and set the port's BPDU processing mode.

Example
The BPDU setting GigabitEthernet0/1 is handled as guard:

```
SC31020(config-if-GigabitEthernet0/1)# spanning-tree bpdu guard
```

show spanning-tree interface gigabitEthernet 0/1

Display the spanning tree status and configuration information of GigabitEthernet0/1.

Syntax

show spanning-tree interface gigabitEthernet 0/1

spanning-tree cost

Configure the port external path cost, and the switch sends BPDU to the downstream switch, which adds the cast value of the transmit port to the cast field of the BPDU.

Syntax

spanning-tree cost [1-200000000]

cost [1-200000000] - The value of external path cost

Default
19

Command Mode
Port Configuration mode

Usage
Enter the port configuration mode and set the cost value of the port.

Example
Set the cost value of GigabitEthernet0/1 to 2000:

```
SC31020(config-if-GigabitEthernet0/1)# spanning-tree cost 2000
```

show spanning-tree interface gigabitEthernet 0/1

Display the spanning tree status and configuration information of GigabitEthernet0/1.

Syntax

show spanning-tree interface gigabitEthernet 0/1

spanning-tree guard

Set port protection function

Syntax

spanning-tree guard [loop | none | root]

loop - Set the loop to avoid the port configured with this command. The BPDU continues to remain blocked and the loop is avoided

root - Ports that enable this function do not re - select the root bridge after receiving a higher priority BPDU

none - Turn off the guard function

Default
None

Command Mode
Port Configuration mode

Usage
Enter the port configuration mode and set the port protection function.

Example
Set the loop guard on GigabitEthernet0/1:

```
SC31020(config-if-GigabitEthernet0/1)# spanning-tree guard loop
```

show spanning-tree interface gigabitEthernet 0/1

Display the spanning tree status and configuration information of GigabitEthernet0/1.

Syntax

show spanning-tree interface gigabitEthernet 0/1

spanning-tree link-type

Sets the link type of the port. By default, the switch automatically selects the link type based on the duplex mode of the port, the full duplex port is point-to-point, and the half duplex port is shared.

Syntax

spanning-tree link-type [point-to-point | shared]

point-to-point - Set the link type is point-to-point

shared - Set the link type is shared

Default
The switch automatically selects the link type, the full duplex port is point-to-point, and the half duplex port is shared.

Command Mode
Port Configuration mode

Usage
Enter the port configuration mode and set the spanning-tree link-type.

Example
Set the link type of GigabitEthernet0/1 to shared:

```
SC31020(config-if-GigabitEthernet0/1)# spanning-tree link-type shared
```

show spanning-tree interface gigabitEthernet 0/1

Display the spanning tree status and configuration information of GigabitEthernet0/1.

Syntax

show spanning-tree interface gigabitEthernet 0/1

spanning-tree portfast edgeport

Some port is directly connected with PC, and the port is not possible loop, so these ports do not need to participate in the spanning tree operations, configured as edge port port linkup directly to the forwarding state, will not experience learn, listen.

Syntax

spanning-tree portfast [edgeport | network]

edgeport - Sets the edge-port for specified port

network - Sets the network port for specified port

Default
Network port

Command Mode
Port Configuration mode

Usage
Enter the port configuration mode and set the port mode is edgeport.

Example
Set GigabitEthernet0/1 for the edgeport:

```
SC31020(config-if-GigabitEthernet0/1)# spanning-tree portfast edgeport
```

show spanning-tree interface gigabitEthernet 0/1

Display the spanning tree status and configuration information of GigabitEthernet0/1.

Syntax

show spanning-tree interface gigabitEthernet 0/1

spanning-tree port-priority

Configure the bridge priority of the port. If the user wants to specify a port as the root port, the bridge priority of the port can be increased.

Syntax

spanning-tree port-priority [0-240]

port-priority [0-240] - Sets the bridge priority of the port, with a range of 0-240 and must be a multiple of 16, default 128

Default
128

Command Mode
Port Configuration mode

Usage
Enter the port configuration mode and set the bridge priority of the port.

Example
Set the priority of GigabitEthernet0/1 to 112:

```
SC31020(config-if-GigabitEthernet0/1)# spanning-tree port-priority 112
```

show spanning-tree interface gigabitEthernet 0/1

Display the spanning tree status and configuration information of GigabitEthernet0/1.

Syntax

show spanning-tree interface gigabitEthernet 0/1

spanning-tree bpdu

BPDU packets are filtered or flood when stp is disabled on ports.

Syntax

spanning-tree bpdu [filtering | flooding]

filtering - bpdu packets are filtered when stp is disabled on ports

flooding - bpdu packets are flooded to all ports with stp disabled and flooding mode

Default
BPDU flooding

Command Mode
Global Configuration mode

Usage
In global mode, configure the way BPDU messages are handled.

Example
When the spanning tree is closed, set the BPDU packet to filtering:

```
SC31020(config)# spanning-tree bpdu filtering
```

show spanning-tree Display the spanning tree status and configuration information.

Syntax

show spanning-tree

spanning-tree trap Spanning tree trap information.

Syntax

spanning-tree trap [new-root| topology-change]

new-root - New root trap

topology-change - Topology change trap

Default
Null

Command Mode
Global Configuration mode

Usage
In global mode, configure the spanning-tree trap information.

Example
Enable the spanning-tree trap of new-root:

```
SC31020(config)# spanning-tree trap new-root
```

show spanning-tree trap new-root Display the spanning tree trap new-root status and configuration information.

Syntax

show spanning-tree trap new-root

Display Relevant Commands

show spanning-tree Displays the current spanning tree status and configuration information.

Syntax

Spanning-tree [cr | interface gigabitEthernet 0/x | link-aggregation]

Interface gigabitEthernet 0/x - Display the current port spanning tree status and configuration information Note that "cr" means no arguments are entered

Default
Null

Command Mode
Privileged mode

Usage
In privileged mode, view the spanning tree status. Show global status without parameters.

Example
The following commands, from top to bottom, are to display the global state information of the spanning tree, display the spanning tree status information of the Gi 0/1.

```
SC31020# show spanning-tree
SC31020# show spanning-tree interfaces GigabitEthernet 0/1
```

show spanning-tree View the current spanning tree status and configuration information.

Syntax

show spanning-tree

show spanning-tree interface gigabitEthernet 0/1 Display the spanning tree status and configuration information of GigabitEthernet0/1.

Syntax

show spanning-tree interface gigabitEthernet 0/1

23 DHCP v4server

Configure Commands

DHCP v4server Configure the DHCP server parameter, then open DHCP sever, and the downstream device gets IP from the switch.

Syntax

ip dhcpserver pool

ip dhcpserver mask

ip dhcpserver gate-way

ip address

ip dhcp server

dhcp-snooping

ip dhcpserver pool - Configure the v4 server pool

ip dhcpserver mask - Configure the v4 server mask

ip dhcpserver gate-way - Configure the v4 server gate-way

ip address - The IP address of the device must be in the same network segment as the address pool of the sever

ip dhcp server - Enable the ip dhcp server function.use "no" command, you can disable the function

dhcp-snooping - Enable the dhcp-snooping

Default
Disabled

Command Mode
Global Configuration mode

Usage
In the global configuration mode, The first parameter configuration server, to enable IPv4 server, Lower establishment access to switch in the IP address pool.

Example

```
SC31020(config)# ip dhcpserver pool 192.168.6.100-192.168.6.200
  pt1:192.168.6.100, pt2:192.168.6.200
SC31020(config)# ip dhcpserver mask 255.255.255.0
SC31020(config)# ip dhcpserver gate-way 192.168.6.1
SC31020(config)# ip address 192.168.6.1
SC31020(config)# ip dhcp server
SC31020(config)# dhcp-snooping
```

show ip dhcp server Displays the ip dhcp server configuration

Syntax

show ip dhcp server

Display Relevant Commands

show ip dhcp server Configure the DHCP server parameter, then open DHCP sever, and the downstream device gets IP from the switch.

Syntax

show ip dhcp server

show ip dhcp server - Display the configure of ip dhcp server

Default
Null

Command Mode
Privileged mode

Usage
View the ip dhcp server information.

Example

```
Show ip dhcp server
```

show ip dhcp server Displays the ip dhcp server configuration

Syntax

show ip dhcp server

24 IPv4 Client

Configure Commands

ipv4 client Configure the ipv4 client parameter, the switch can get IP from DHCP server.

Syntax

ip dhcp

no ip dhcp

ip dhcp - Enbale ip dhcp client

no ip dhcp - Disable ip dhcp client

Default
Disabled

Command Mode
Global Configuration mode

Usage
In the global configure mode, enable the ip dhcp, the switch can get ip from DHCP server.

Example
Configuring the spanning tree to turn on and off.

```
SC31020(config)# ip dhcp
SC31020# show ip dhcp
DHCP Status : enabled
```

show ip dhcp Displays the ip dhcp client configuration.

Syntax

show ip dhcp

Display Relevant Commands

show ip DHCP Enable the ip DHCP, the switch can get IP from DHCP server.

Syntax

Show ip dhcp

Show ip

show ip dhcp - Display the configure of ip dhcp

Show ip - Display the switch get ip from the dhcp server

Default
Null

Command Mode
Privileged mode

Usage
View the ip dhcp information.

Example

```
SC31020# show ip
Example Example Example IP Address: 192.168.0.143
Subnet Netmask: 255.255.255.0
Default Gateway: 192.168.0.177
SC31020# show ip dhcp
DHCP Status : enabled
```

show ip dhcp Displays the ip dhcp information.

Syntax

show ip dhcp

show ip Displays the switch get ip from the dhcp server.

Syntax

show ip

25 IPv6 Client

Configure Commands

ipv6 client Configure the ipv6 client parameter, the switch can get IP from DHCP server.

Syntax

Ipv6 dhcp

no ipv6 dhcp

ipv6 autoconfiguration

no ipv6 autoconfiguration

Ipv6 dhcp - Enbale ipv6 dhcp client

no ipv6 dhcp - Disable ipv6 dhcp client

autoconfiguration - Enable Ipv6 auto-configuration

No ipv6 autoconfiguration - Disable Ipv6 auto-configuration

Default
Disabled

Command Mode
Global Configuration mode

Usage
In the global configure mode, enable the ipv6 dhcp, the switch can get ipv6 from ipv6 DHCP server.

Example

```
SC31020(config)# ipv6 dhcp
SC31020(config)# ipv6 autoconfiguration
```

show ipv6 dhcp Displays the ipv6 dhcp client configuration.

Syntax

show ipv6 dhcp

show ipv6 Display the switch get ipv6 from the ipv6 dhcp server.

Syntax

show ipv6

Configure Commands

show ipv6 DHCP Enable the ipv6 DHCP, the switch can get IP from DHCP server.

Syntax

Show ip dhcp

Show ipv6

Default
Null

Command Mode
Privileged mode

Usage
View the ip dhcp information

Example

```
SC31020# show ipv6 dhcp
DHCPv6 Status : enabled
SC31020# show ipv6
IPv6 DHCP Configuration     : Enabled
IPv6 DHCP DUID              : 00:01:00:01:00:00:00:5a:00:e0:4c:00:00:00
IPv6 Auto Configuration     : Enabled
IPv6 Link Local Address     : fe80::2e0:4cff:fe00:0/64
IPv6 static Address         :
IPv6 static Gateway Address :
IPv6 in use Address         : fd00::2e0:4cff:fe00:0/64
IPv6 in use Address         : fe80::2e0:4cff:fe00:0/64
```

show ipv6 dhcp Displays the ipv6 dhcp client configuration.

Syntax

show ipv6 dhcp

show ipv6 Display the switch get ipv6 from the ipv6 dhcp server.

Syntax

show ipv6

26 IGMP Snooping

Configure Commands

ip igmp snooping

Enable igmp snooping in global configuration mode ,and Add "no" to the command will disable igmp snooping.

Syntax

ip igmp snooping

no ip igmp snooping

Default
Enabled

Command Mode
Global Configuration mode

Usage
Use command ip igmp snooping to enable igmp snooping function. Use the no form of this command to disable. You can verify settings by the show ip igmp snooping command.

Example
Configuring the spanning tree to turn on and off.

```
SC31020(config)# ip igmp snooping
SC31020(config)# no ip igmp snooping
```

show ip igmp snooping

Verify settings of igmp snooping

Syntax

show ip igmp snooping

ip igmp snooping version

Set igmp snooping version in global configuration mode.

Syntax

ip igmp snooping version (2/3)

(2/3) - IGMP version 2 or version 3 mode

Default
3

Command Mode
Global Configuration mode

Usage
Use the ip igmp snooping version command to change IGMP support version. You can verify settings by the show ip igmp snooping command.

Example
The following example specifies that set ip igmp snooping version 2:

```
Switch(config)#ip igmp snooping version 2
```

show ip igmp snooping

Verify settings of igmp snooping

Syntax

show ip igmp snooping

ip igmp snooping vlan

Enable igmp snooping of specific vlan,please input ip igmp snooping vlan vlan-list in Global configuration mode.and Add "no" to the command will disable the igmp snooping function of the vlan.

Syntax

ip igmp snooping vlan VLAN-LIST

VLAN-LIST - Specifies VLAN ID list to set

Default
Default is disable for all VLANs

Command Mode
Global Configuration mode

Usage
Disable will clear all ip igmp snooping dynamic group and dynamic router port and make all static ip igmp invalid of this vlan.Will not learn dynamic group and router port by igmp message any more.
Use the **ip igmp snooping vlan** command to enable IGMP on VLAN. Use the

no form of this command to disable.
You can verify settings by the **show ip igmp snooping vlan** command.

Example
The following example specifies that set ip igmp snooping vlan test:

```
SC31020(config)# ip igmp snooping vlan 2
```

Show ip igmp snooping vlan

Verify settings of igmp snooping.

Syntax

Show ip igmp snooping vlan

ip igmp snooping fast-leave

Enable igmp snooping fast-leave function. If there is only one member of the group, and device receive leave report from the member, the group will leave immediately.

Syntax

ip igmp snooping fast-leave

Default
Disabled

Command Mode
Global Configuration mode

Usage
Use the **ip igmp snooping fast-leave enable** command to enable fast-leave function.
Use the **no** form of this command to disable.
You can verify settings by the **show ip igmp snooping vlan** command.

Example
The following example specifies the set ip igmp snooping fast-leave test:

```
SC31020(config)# ip igmp snooping fast-leave
```

Show ip igmp snooping vlan

Verify settings of igmp snooping.

Syntax

Show ip igmp snooping vlan

ip igmp snooping suppression

Enable igmp snooping of suppression function, router port will just forward one report packet when received many the same group join packet.and the function is invalid in igmp snooping v3.

Syntax

ip igmp snooping suppression

Default
Disabled

Command Mode
Global Configuration mode

Usage
Use the ip igmp snooping suppression command to enable suppression function.
Use the no form of this command to disable.
You can verify settings by the show ip igmp snooping vlan command.

Example
The following example specifies that set ip igmp snooping suppression test:

```
SC31020(config)# ip igmp snooping suppression
```

Show ip igmp snooping vlan

Verify settings of igmp snooping.

Syntax

Show ip igmp snooping vlan

ip igmp snooping unknown-multicast action

Set the action when received unknown-multicast.

Syntax

ip igmp snooping unknown-multicast action (drop | flood | router-port)

(drop|flood|router-port) - Drop/flood in vlan or forward to router port of unknown multicast packet

Default
Drop

Command Mode
Global Configuration mode

Usage
When igmp and mld snooping disable, it can't set action router port.
When disable igmp snooping & mld snooping,it set unknown multicast action flood.
When action is router-port to flood or drop ,it will delete the unknown multicast group entry.
Use the **ip igmp snooping unknown-multicast action** command to change action.
You can verify settings by the **show ip igmp snooping vlan** command.

Example
The following example specifies the set ip igmp unknown-multicast test:

```
SC31020(config)# ip igmp snooping unknown-multicast action drop
```

Show ip igmp snooping vlan

Verify settings of igmp snooping.

Syntax

Show ip igmp snooping vlan

ip igmp snooping vlan mrouter

Add static router port for vlan.

Syntax

ip igmp snooping vlan VLAN-LIST mrouter interfaces GigabitEthernet|Aggregateport IF_PORTS

No ip igmp snooping vlan VLAN-LIST mrouter interfaces GigabitEthernet|Aggregateport IF_PORTS

VLAN-LIST - Specifies VLAN ID list to set

IF-PORTS - Specifies a port list to set or remove

Default
None static router ports by default.

Command Mode
Global Configuration mode

Usage
Use the **ip igmp snooping vlan mrouter** command to add static router port. All query packets will forward to this port.

Use the **no** form of this command to delete static router port. You can verify settings by the **show ip igmp snooping vlan** command.

Example
The following example specifies that set ip igmp snooping static router port test:

```
SC31020(config)# ip igmp snooping vlan 2 mrouter interfaces GigabitEthernet
  0/5
```

Show ip igmp snooping vlan

Verify settings of igmp snooping.

Syntax

Show ip igmp snooping vlan

ip igmp snooping vlan mrouter learn

Enable learning router port by routing protocol packets such as PIM/PIMv2, DVMRP, MOSPF. Use the no form of this command to disable.

Syntax

ip igmp snooping vlan VLAN-LIST mrouter learn pim-dvmrp

No ip igmp snooping vlan VLAN-LIST mrouter learn pim-dvmrp

VLAN-LIST - Specifies VLAN ID list to set

IF-PORTS - Specifies a port list to set or remove

Default
Enabled

Command Mode
Global Configuration mode

Usage
Use the ip igmp snooping vlan mrouter learn pim-dvmrp command to Enable learning router port by routing protocol packets such as PIM/PIMv2, DVMRP, MOSPF.
Use the no form of this command to disable.
You can verify settings by the show ip igmp snooping vlan command.

Example
The following example specifies that Enable learning router port test:

```
SC31020(config)# ip igmp snooping vlan 2 mrouter learn pim-dvmrp
```

Show ip igmp snooping vlan

Verify settings of igmp snooping.

Syntax

Show ip igmp snooping vlan

ip igmp snooping vlan static

Add a static group.

Syntax

ip igmp snooping vlan *VLAN-LIST* **static** *group-address* **interfaces GigabitEthernet|Aggregateport IF_PORTS**

no ip igmp snooping vlan *VLAN-LIST* **static** *group-address* **interfaces GigabitEthernet|Aggregateport IF_PORTS**

Ip-addr - Specifies multicast group ipv4 address

IF-PORTS - Specifies a port list to set or remove

Default
Enabled

Command Mode
Global Configuration mode

Usage
Use the **ip igmp snooping vlan static** command to add a static group. The static group will not learn other dynamic ports.If the dynamic group exist ,then the static group will overlap the dynamic group.The static group set to valid unless igmp snooping vlan enable.
Use the **no** form of this command to delete static group.If remove the last member of static group,the static group will be delete.
You can verify settings by the **show ip igmp snooping group** command.

Example
The following example specifies that set ip igmp snooping static group test:

```
SC31020(config)# ip igmp snooping vlan 2 static 239.1.1.1 interfaces
  GigabitEthernet 0/6
```

Show ip igmp snooping group

Verify the static group

Syntax

Show ip igmp snooping group

ip igmp snooping vlan querier

Enable querier for vlan and adding "no" to the command will disable querier function.

Syntax

ip igmp snooping vlan *VLAN-LIST* **querier**

no ip igmp snooping vlan *VLAN-LIST* **querier**

VLAN-LIST - Specifies VLAN ID list to set

Default
Disabled

Command Mode
Global Configuration mode

Usage
When enable ip igmp vlan querier, there will process router select, the select successful will send general and specific query.
Use the **ip igmp snooping vlan querier** command to add querier.
Use the no form of this command to delete querier.
You can verify settings by the **show ip igmp snooping querier** command.

Example
The following example specifies that enable vlan querier test:

```
SC31020(config)# ip igmp snooping vlan 2 querier
```

Show ip igmp snooping querier

Verify the querier information.

Syntax

Show ip igmp snooping querier

ip igmp snooping vlan querier version

Set igmp snooping querier version in global configuration mode.

Syntax

ip igmp snooping vlan *VLAN-LIST* **querier version** (2|3)

VLAN-LINST - Specifies VLAN ID list to set

(2|3) - Query version 2 or 3

Default
2

Command Mode
Global Configuration mode

Usage
Use the **ip igmp snooping vlan querier version** command to set querier version.
You can verify settings by the **show ip igmp snooping querier** command.

Example
The following example specifies that set ip igmp snooping querier version test:

```
SC31020(config)# ip igmp snooping vlan 2 querier version 3
```

Show ip igmp snooping querier

Verify the querier information.

Syntax

Show ip igmp snooping querier

ip igmp snooping vlan querier last-member-query-count

Set igmp snooping querier last-member-query-count.

Syntax

ip igmp snooping vlan *VLAN-LIST* **querier last-member-query-count** *<1-7>*

no ip igmp snooping vlan *VLAN-LIST* **querier last-member-query-count**

VLAN-LINST - Specifies VLAN ID list to set

last-member-query-count <1-7> - Specifies last member query count to set

Default
2

Command Mode
Global Configuration mode

Usage
Use the **ip igmp snooping vlan querier last-member-query-count** command to change how many query packets will send.
Use the **no** form of this command to restore to default.
You can verify settings by the **show ip igmp snooping vlan** command.

Example
The following example specifies that set ip igmp snooping querier last-member-query-count test:

```
SC31020(config)# ip igmp snooping vlan 2 querier last-member-query-count 5
```

Show ip igmp snooping vlan

Verify the querier information.

Syntax

Show ip igmp snooping vlan

ip igmp snooping vlan querier last-member-query-interval

Set igmp snooping querier last-member-query-interval.

Syntax

ip igmp snooping vlan *VLAN-LIST* q**uerier last-member-query-interval** *<1-25>*

no ip igmp snooping vlan *VLAN-LIST* **querier last-member-query-interval**

VLAN-LIST - Specifies VLAN ID list to set

last-member-query-interval <1-25> - Specifies last member query interval to set

Default
1

Command Mode
Global Configuration mode

Usage
Use the **ip igmp snooping vlan querier last-member-query-interval** command to set interval between each query packet.
Use the **no** form of this command to restore to default.
You can verify settings by the **show ip igmp snooping vlan** command.

Example
The following example specifies that set ip igmp snooping querier last-member-query-interval test:

```
SC31020(config)# ip igmp snooping vlan 2 querier last-member-query-interval
  10
```

Show ip igmp snooping vlan

Verify the querier information.

Syntax

Show ip igmp snooping vlan

ip igmp snooping vlan querier max-response-time

Set igmp snooping querier max-response-time.

Syntax

ip igmp snooping vlan *VLAN-LIST* **querier max-response-time** *<5-20>*

no ip igmp snooping vlan *VLAN-LIST* **querier max-response-time**

VLAN-LIST - Specifies VLAN ID list to set

last-member-query-interval <5-20> - Specifies a response time to set

Default
10

Command Mode
Global Configuration mode

Usage
Use the **ip igmp snooping vlan querier max-response-time** command to set response-time.
Use the **no** form of this command to restore to default.
You can verify settings by the **show ip igmp snooping vlan** command.

Example
The following example specifies that set ip igmp snooping querier max-response-time test:

```
SC31020(config)# ip igmp snooping vlan 2 querier max-response-time 20
```

Show ip igmp snooping vlan

Verify the querier information.

Syntax

Show ip igmp snooping vlan

ip igmp snooping vlan querier query-interval

Set igmp snooping querier Interval between each query.

Syntax

ip igmp snooping vlan *VLAN-LIST* **querier query-interval** *<30-18000>*

no ip igmp snooping vlan *VLAN-LIST* **querier query-interval**

VLAN-LIST - Specifies VLAN ID list to set

query-interval <30-18000> - Specifies a response time to set

Default
125

Command Mode
Global Configuration mode

Usage
Use the **ip igmp snooping vlan querier query-interval** command to set Interval between each query.
Use the **no** form of this command to restore to default.
You can verify settings by the **show ip igmp snooping vlan** command.

Example
The following example specifies that set ip igmp snooping querier version test:

```
SC31020(config)# ip igmp snooping vlan 2 querier query-interval 200
```

Show ip igmp snooping vlan

Verify the querier information.

Syntax

Show ip igmp snooping vlan

ip igmp snooping vlan robustness-variable

Set igmp snooping querier robustness-variable.

Syntax

ip igmp snooping vlan *VLAN-LIST* **robustness-variable** *<1-7>*

no ip igmp snooping vlan *VLAN-LIST* **robustness-variable**

VLAN-LIST - Specifies VLAN ID list to set

robustness-variable <1-7> - Specifies a robustness value to set

Default
2

Command Mode
Global Configuration mode

Usage
Use the **ip igmp snooping vlan robustness-variable** command to times to retry.
Use the **no** form of this command to restore to default.
You can verify settings by the **show ip igmp snooping vlan** command.

Example
The following example specifies that set ip igmp snooping querier robustness-variable test:

```
SC31020(config)# ip igmp snooping vlan 1 robustness-variable 5
```

Show ip igmp snooping vlan

Verify the querier information.

Syntax

Show ip igmp snooping vlan

ip igmp profile

Add igmp profile if you want to permit or deny some groups.

Syntax

ip igmp profile *<1-128>*

no Ip igmp profile *<1-128>*

<1-128> - Specifies profile ID

Default
No profile exist by default.

Command Mode
Global Configuration mode

Usage
Use the **ip igmp profile** command to enter profile configuration.
Use the **no** form of this command to delete profile.
You can verify settings by the **show ip igmp profile** command.

Example
The following example specifies that set ip igmp snooping profile test:

```
SC31020(config)# ip igmp profile 1
```

Show ip igmp profile Verify the ip igmp profile information.

Syntax

Show ip igmp profile

profile range Configure igmp profile if you want to permit or deny some groups.

Syntax

Profile range ip *<ip-addr> [ip-addr]* **action** *(permit|deny)*

<ip-addr> - Start ipv4 multicast address

[ip-addr] - End ipv4 multicast address

(permit|deny) - Permit: allow Multicast address rang ip address learning. Deny: do not allow Multicast address rang ip address learning

Default
None

Command Mode
Igmp Profile Configuration mode

Usage
Use the **profile** command to generate IGMP profile.
You can verify settings by the **show ip igmp profile** command.

Example
The following example specifies that set ip igmp snooping profile test:

```
SC31020(config)#  ip igmp profile 1
SC31020(config)# profile range ip 225.1.1.1 225.1.2.1 action permit
```

Show ip igmp profile Verify the ip igmp profile information.

Syntax

Show ip igmp profile

ip igmp filter Use ip igmp filter command to bind a profile for port.

Syntax

ip igmp filter *<1-128>*

no Ip igmp filter

<1-128> - Specifies profile ID

Default
None

Command Mode
Port Configuration mode

Usage
Use the **ip igmp filter** command to bind a profile for port. When the port bind a profile then the port learning group will update, if the group is not match the profile rule it will remove the port from the group. Static group is excluded.
Use the **no** form of this command to delete profile.
You can verify settings by the **show running-config** command.

Example
The following example specifies that set ip igmp filter test:

```
SC31020(config)# interface GigabitEthernet 0/1
SC31020(config-if-GigabitEthernet0/1)# ip igmp filter 1
```

Show running-config Verify the ip igmp profile information.

Syntax

Show running-config

Commands related to display and monitoring

clear ip igmp snooping statistics Clear igmp snooping statistics.

Syntax

clear ip igmp snooping statistics

None - Clear all igmp packets statistics

Default
Null

Command Mode
Privileged EXEC.

Usage
This command will clear all of the igmp packets statistics.
You can verify settings by the **show ip igmp snooping statistics** command.

Example
The following example specifies that show ip igmp snooping statistics test:

```
SC31020(config)# ip igmp snooping
SC31020#clear  ip igmp snooping statistics
SC31020#show ip igmp snooping statistics
SC31020#show ip igmp snooping statistics

Packet Statistics
Total RX                          :  0
Valid RX                          :  0
Invalid RX                        :  0
Other RX                          :  0
Leave RX                          :  0
Report RX                         :  0
General Query RX                  :  0
Special Group Query RX            :  0
Special Group & Source Query RX   :  0
Leave TX                          :  0
Report TX                         :  0
General Query TX                  :  0
Special Group Query TX            :  0
Special Group & Source Query TX   :  0
```

Show ip igmp snooping statistics

Verify igmp snooping statistics information.

Syntax

show ip igmp snooping statistics

clear ip igmp snooping groups

clear igmp snooping groups.

Syntax

clear ip igmp snooping groups *[(dynamic|static)]*

None - Clear ip igmp groups include dynamic and static

(dynamic|static) - Ip igmp group is dynamic and static

Default
Null

Command Mode
Privileged EXEC.

Usage
This command will clear the igmp groups for dynamic or static or all of type. You can verify settings by the **show ip igmp snooping groups** command.

Example
The following example specifies that show ip igmp snooping groups test:

```
SC31020(config)# ip igmp snooping
SC31020#clear ip igmp snooping groups
SC31020#show ip igmp snooping groups

VLAN | Group IP Address |  Type  | Life(Sec) | Port
-----+------------------+--------+-----------+------
Total Number of Entry = 0
```

Show ip igmp snooping groups

Verify igmp snooping groups information.

Syntax

show ip igmp snooping groups

show ip igmp snooping

View igmp snooping global information.

Syntax

show ip igmp snooping

Default
None

Command Mode
Privileged EXEC.

Usage
This command will display ip igmp snooping global info.

Example
The following example specifies that show ip igmp snooping test:

```
SC31020#show ip igmp snooping
IGMP Snooping state : Enable
```

```
IGMP Snooping Version : v3
IGMP Fast-Leave : Disable
IGMP Report Suppression : Disable
IGMP Forward Method : mac
IGMP Unknown IP Multicast Action : Drop
IGMP Multicast router learning mode : pim-dvmrp

               vlan 1
             -------------
IGMP Snooping state : enabled
IGMP Fast-Leave : disabled
IGMP Multicast router learning mode : pim-dvmrp
IGMP VLAN querier : disabled
```

Show ip igmp snooping

Verify igmp snooping information.

Syntax

show ip igmp snooping

show ip igmp snooping vlan

View igmp snooping vlan information.

Syntax

show ip igmp snooping vlan *[VLAN-LIST]*

None - Show all ip igmp snooping vlan info

[VLAN-LIST] - Show specifies vlan ip igmp snooping info

Default
None

Command Mode
Privileged EXEC.

Usage
This command will display ip igmp snooping vlan info.

Example
The following example specifies that show ip igmp snooping vlan test:

```
SC31020#show ip igmp snooping vlan
IGMP Snooping global state  : enabled
IGMP Global IGMPv2 fast-leave : disabled
IGMP Global multicast router learning mode : pim-dvmrp

                  vlan 1
                -------------
IGMP Snooping state : enabled
IGMP Fast-Leave : disabled
IGMP Multicast router learning mode : pim-dvmrp
```

```
IGMP VLAN querier : disabled
```

Show ip igmp snooping vlan

Verify settings of igmp snooping vlan.

Syntax

show ip igmp snooping vlan

show ip igmp snooping forward-all

Display igmp snooping forward-all info.

Syntax

show ip igmp snooping forward-all [**vlan***VLAN-LIST*]

None - Show all ip igmp snooping vlan forward-all info

[VLAN-LIST] - Show specifies vlan ip igmp snooping forward-all info

Default
Null

Command Mode
Privileged EXEC.

Usage
This command will display ip igmp snooping forward-all info.

Example
The following example specifies that show ip igmp snooping forward-all test:

```
SC31020#show ip igmp snooping forward-all
IGMP Snooping VLAN           : 1
IGMP Snooping static port    : None
IGMP Snooping forbidden port : None
```

Show ip igmp snooping forward-all

Verify settings of igmp snooping forward-all.

Syntax

Show ip igmp snooping forward-all

show ip igmp snooping groups

Display igmp snooping groups info.

Syntax

show ip igmp snooping groups [counters | dynamic | static]

None - Show all ip igmp groups include dynamic and static info

Counters - Show dynamic and static groups counters

(dynamic|static) - Show dynamic or static igmp groups

Default
None

Command Mode
Privileged EXEC.

Usage
This command will display ip igmp snooping groups for dynamic or static or all of type.

Example
The following example specifies that show ip igmp snooping groups test:

```
SC31020#show ip igmp snooping groups

VLAN | Group IP Address |  Type   | Life(Sec) | Port
-----+------------------+--------+-----------+-------
1    |        239.1.1.1 |  Static|     --    | gi0/3
1    |  239.255.255.250 | Dynamic|    253    | gi0/1

Total Number of Entry = 2
```

Show ip igmp snooping groups

Verify igmp snooping groups information.

Syntax

Show ip igmp snooping groups

show ip igmp snooping mrouter

Display igmp snooping mrouter information.

Syntax

show ip igmp snooping mrouter [*counters* | *dynamic* | *static*]

None - Show all ip igmp groups include dynamic and static info

Counters - Show dynamic and static groups counters

(dynamic|static) - Show dynamic or static igmp groups

Default
Null

Command Mode
Privileged EXEC.

Usage
This command will display ip igmp snooping mrouter for dynamic or static or all of type.

Example
The following example specifies that show ip igmp snooping mrouter test:

```
SC31020#show ip igmp snooping mrouter

VID  |  Port   |   type  | Expiry Time(Sec)
-----+---------+---------+-----------------
1    |  gi0/8  |  Static |      ---

Total Entry 1
```

Show ip igmp snooping mrouter

verify igmp snooping mrouter information.

Syntax

Show ip igmp snooping mrouter

show ip igmp snooping querier

Display igmp snooping querier info.

Syntax

show ip igmp snooping querier

Default
Null

Command Mode
Privileged EXEC.

Usage
This command will display all of the static vlan ip igmp mrouter info.

Example
The following example specifies that show ip igmp snooping querier test:

```
SC31020#show ip igmp snooping querier

VID  |    State    |    Status   |  Version   |  Querier IP
-----+-------------+-------------+------------+--------------------
1    |  Disabled   | Non-Querier |   No       |    ------
```

```
Total Entry 1
```

Show ip igmp snooping querier

Verify igmp snooping querier information.

Syntax

show ip igmp snooping querier

27 MLD Snooping

Command Related to Configuration

ipv6 mld snooping

Enable mld snooping in global configuration mode ,and Add "no" to the command will disable mld snooping.

Syntax

ipv6 mld snooping

no ipv6 mld snooping

Default
Enabled

Command Mode
Global Configuration mode

Usage
Use command **ipv6 mld snooping** to enable igmp snooping function.
Use the **no** form of this command to disable.Disable will clear all ipv6 mld snooping dynamic groups and dynamic router port, and make the static ipv6 mld group invalid.No more dynamic group and router port by mld message will be learned.
You can verify settings by the **show ipv6 mld snooping** command.

Example

```
SC31020(config)# ipv6 mld snooping
SC31020(config)# no ipv6 mld snooping
```

show ipv6 mld snooping

Verify settings of ipv6 mld snooping.

Syntax

show ipv6 mld snooping

ipv6 mld snooping version

Set mld snooping version in global configuration mode.

Syntax

ipv6 mld snooping version *(1|2)*

(1|2) - MLD version 1 or version 2 mode

Default
1

Command Mode
Global Configuration mode

Usage
Use the **ipv6 mld snooping version** command to change MLD support version. Version 2 packet won't be processed if choose version 1.
You can verify settings by the **show ipv6 mld snooping** command.

Example
The following example specifies that set ipv6 mld snooping version 2:

```
Switch(config)#ipv6 mld snooping version 2
```

show ipv6 mld snooping

Verify settings of ipv6 mld snooping.

Syntax

show ipv6 mld snooping

ipv6 mld snooping vlan

Enable mld snooping of specific vlan, please input ipv6 mld snooping vlan vlan-list in Global configuration mode.and Add "no" to the command will disable the mld snooping function of the vlan.

Syntax

ipv6 mld snooping vlan *VLAN-LIST*

VLAN-LIST - Specifies VLAN ID list to set

Default
Disabled for all VLANs.

Command Mode
Global Configuration mode

Usage
Disable will clear all ipv6 mld snooping dynamic group and dynamic router port and make all static ipv6 mld invalid of this vlan.Will not learn dynamic group and router port by mld message any more.
Use the **ipv6 mld snooping vlan** command to enable mld on VLAN.
Use the **no** form of this command to disable.
You can verify settings by the **show ipv6 mld snooping vlan** command.

Example
The following example specifies tha set ipv6 mld snooping vlan test:

```
SC31020(config)# ipv6 mld snooping vlan 2
```

show ipv6 mld snooping vlan

Verify settings of mld snooping.

Syntax

show ipv6 mld snooping vlan

ipv6 mld snooping vlan immediate-leave

Enable mld snooping vlan immediate-leave function, If there is only one member of the group, and device receive leave packet from the member, the group will leave immediately.

Syntax

ipv6 mld snooping vlan immediate-leave

VLAN-LIST - Specifies VLAN ID list to set

Default
Disabled

Command Mode
Global Configuration mode

Usage
Use the **ipv6 mld snooping vlan immediate-leave** command to enable vlan immediate-leave function. Group will remove port immediately when receive leave packet.
Use the **no** form of this command to disable.
You can verify settings by the **show ipv6 mld snooping vlan** command.

Example
The following example specifies tha set ipv6 mld snooping vlan immediate-leave test:

```
SC31020(config)# ipv6 mld snooping vlan 1 immediate-leave
```

show ipv6 mld snooping vlan

Verify settings of mld snooping.

Syntax

show ipv6 mld snooping vlan

ipv6 mld snooping report-suppression

Enable mld snooping of report-suppression function, router port will just forward one report packet when received many the same group join packet.and the function is invalid in mld snooping v2.

Syntax

ipv6 mld snooping report-suppression

no ipv6 mld snooping report-suppression

Default
Enable

Command Mode
Global Configuration mode

Usage
Use the **ipv6 mld snooping report-suppression** command to enable report-suppression function.
Use the **no** form of this command to disable. Disable report-supression will forward all received reports to the vlan router ports.
You can verify settings by the **show ipv6 mld snooping** command.

Example
The following example specifies that disable ipv6 mld snooping report-suppression test:

```
SC31020(config)# no ipv6 mld snooping report-suppression
```

show ipv6 mld snooping

Verify settings of mld snooping.

Syntax

show ipv6 mld snooping

ipv6 mld snooping unknown-multicast action

Set the action when received unknown-multicast.

Syntax

ipv6 mld snooping unknown-multicast action (*drop* | *flood* | *router-port*)

(drop|flood|router-port) - Drop/flood in vlan or forward to router port of unknown multicast packet

Default
Flood

Command Mode
Global Configuration mode

Usage
When mld and mld snooping disable, it can't set action router port.
When disable mld snooping & mld snooping, it set unknown multicast action flood.
When action is router-port to flood or drop, it will delete the unknown multicast group entry.
Use the **ipv6 mld snooping unknown-multicast action** command to change action.
You can verify settings by the **show ipv6 mld snooping** command.

Example
The following example specifies the set ipv6 mld unknown-multicast vlan test:

```
SC31020(config)# ipv6 mld snooping unknown-multicast action drop
```

show ipv6 mld snooping vlan

Verify settings of mld snooping.

Syntax

show ipv6 mld snooping vlan

ipv6 mld snooping vlan static-router-port

Add static router port for vlan.

Syntax

ipv6 mld snooping vlan *VLAN-LIST* **static-router-port GigabitEthernet|Aggregateport IF_PORTS**

No ipv6 mld snooping vlan *VLAN-LIST* **static-router-port GigabitEthernet|Aggregateport IF_PORTS**

VLAN-LIST - Specifies VLAN ID list to set

IF-PORTS - Specifies a port list to set or remove

Default
None static router ports by default.

Command Mode
Global Configuration mode

Usage
Use the **ipv6 mld snooping vlan static-router-port** command to add static router port. All query packets will forward to this port.
Use the **no** form of this command to delete static router port.
You can verify settings by the **show ipv6 mld snooping router** command.

Example
The following example specifies that set ipv6 mld snooping static router port test:

```
SC31020(config)# ipv6 mld snooping vlan 2 static-router-port GigabitEthernet
  0/5
```

show ipv6 mld snooping router

Verify the ipv6 mld snooping router Information.

Syntax

show ipv6 mld snooping router

ipv6 mld snooping vlan router learn

Enable learning router port by routing protocol packets such as PIM/PIMv2, DVMRP, MOSPF. Use the no form of this command to disable.

Syntax

ipv6 mld snooping vlan *VLAN-LIST* **mrouter learn pim-dvmrp**

No ipv6 mld snooping vlan *VLAN-LIST* **mrouter learn pim-dvmrp**

VLAN-LIST - Specifies VLAN ID list to set

IF-PORTS - Specifies a port list to set or remove

Default
Enabled

Command Mode
Global Configuration mode

Usage
Use the **ipv6 mld snooping vlan mrouter learn pim-dvmrp** command to Enable learning router port by routing protocol packets such as PIM/PIMv2, DVMRP, MOSPF.
Use the **no** form of this command to disable.
You can verify settings by the **show ipv6 mld snooping vlan** command.

Example
The following example specifies that Enable learning router port test:

```
SC31020(config)# ipv6 mld snooping vlan 2 mrouter learn pim-dvmrp
```

show ipv6 mld snooping vlan

Verify the ipv6 mld snooping Information.

Syntax

show ipv6 mld snooping vlan

ipv6 mld snooping vlan static-group

Add a static group

Syntax

ipv6 mld snooping vlan *VLAN-LIST* **static-group** *group-address* **interfaces GigabitEthernet|Aggregateport IF_PORTS**

no ipv6 mld snooping vlan *VLAN-LIST* **static-group** *group-address* **interfaces GigabitEthernet|Aggregateport IF_PORTS**

Ip-addr - Specifies multicast group ipv6 address

IF-PORTS - Specifies a port list to set or remove

Default
No static group by default.

Command Mode
Global Configuration mode

Usage
Use the **ipv6 mld snooping vlan static-group** command to add a static group. The static group will not learn other dynamic ports. If the dynamic group exists then the static group will overlap the dynamic group.The static group set to valid unless mld snooping vlan enable.
Use the **no** form of this command to delete static group.If remove the last

member of static group, the static group will be delete.
You can verify settings by **the show ipv6 mld snooping groups** command.

Example
The following example specifies that set ipv6 mld snooping static group test:

```
SC31020(config)# ipv6 mld snooping vlan 1 static-group ff08::9 interfaces
  Aggregateport 0/6
```

show ipv6 mld snooping groups

Verify static group.

Syntax

show ipv6 mld snooping groups

Commands related to display and monitoring

clear ipv6 mld snooping statistics

Clear ipv6 mld statistics.

Syntax

clear ipv6 mld snooping statistics

None - Clear all igmp packets statistics

Default
None

Command Mode
Privileged EXEC.

Usage
This command will clear all of the ipv6 mld packets statistics.
You can verify settings by the **show ipv6 mld snooping statistics** command.

Example
The following example specifies that show ipv6 mld snooping statistics test:

```
SC31020#clear ipv6 mld snooping statistics
SC31020#show ipv6 mld snooping
Snooping                          : Enabled
Report Suppression                : Enabled
Operation Version                 : v1
Forward Method                    : mac
Unknown IPv6 Multicast Action     : Flood
```

```
Packet Statistics
Total RX                          :  0
Valid RX                          :  0
Invalid RX                        :  0
Other RX                          :  0
Leave RX                          :  0
Report RX                         :  0
General Query RX                  :  0
Specail Group Query RX            :  0
Specail Group & Source Query RX   :  0
Leave TX                          :  0
Report TX                         :  0
General Query TX                  :  0
Specail Group Query TX            :  0
Specail Group & Source Query TX   :  0
```

show ipv6 mld snooping Verify ipv6 mld statistics info.

Syntax

show ipv6 mld snooping

clear ipv6 mld snooping groups Clear mld snooping groups.

Syntax

clear ipv6 mld snooping groups *[(dynamic | static)]*

None - Clear ipv6 mld groups include dynamic and static

(dynamic | static) - Ipv6 mld group is dynamic and static

Default
None

Command Mode
Privileged EXEC.

Usage
This command will clear the mld groups for dynamic or static or all of type. You can verify settings by the **show ipv6 mld snooping groups** command.

Example
The following example specifies that show ipv6 mld snooping groups test:

```
SC31020#clear  ipv6 mld snooping groups
SC31020#show ipv6 mld snooping groups
VLAN  | Group IP Address |  Type  | Life(Sec) | Port
------+------------------+--------+-----------+---------
Total Number of Entry = 0
```

show ipv6 mld snooping groups

Verify mld snooping groups information

Syntax

Show ipv6 mld snooping groups

show ipv6 mld snooping

View mld snooping global information.

Syntax

show ipv6 mld snooping

Default
None

Command Mode
Privileged EXEC.

Usage
This command will display ipv6 mld snooping global info.

Example
The following example specifies that show ipv6 mld snooping test:

```
SC31020#show ipv6 mld snooping
MLD Snooping Status

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

Snooping                         : Enabled
Report Suppression               : Enabled
Forward Method                   : mac
Unknown IPv6 Multicast Action    : Flood

Packet Statistics
Total RX                          :  121
Valid RX                          :  121
Invalid RX                        :  0
Other RX                          :  0
Leave RX                          :  0
Report RX                         :  121
General Query RX                  :  0
Special Group Query RX            :  0
Special Group & Source Query RX   :  0
Leave TX                          :  0
Report TX                         :  0
General Query TX                  :  0
Special Group Query TX            :  0
Special Group & Source Query TX   :  0

Total Number of Entry = 0
```

show ipv6 mld snooping Verify settings of mld snooping.

Syntax

Show ipv6 mld snooping

show ipv6 mld snooping vlan View mld snooping vlan info.

Syntax

show ipv6 mld snooping vlan *[VLAN-LIST]*

None - Show all mld snooping vlan info

[VLAN-LIST] - Shows specific vlan mld snooping info

Default
Null

Command Mode
Privileged EXEC.

Usage
This command will display ipv6 mld snooping vlan info.

Example
The following example specifies that show ipv6 mld snooping vlan test:

```
SC31020#show ipv6 mld snooping vlan 1
MLD Snooping is globaly enabled
MLD Snooping VLAN 1 admin : enabled
MLD Snooping oper mode : enabled
MLD Snooping robustness: admin 2 oper 2
MLD Snooping query interval: admin 125 sec oper 125 sec
MLD Snooping query max response : admin 10 sec oper  10 sec
MLD Snooping last member query counter: admin 2  oper 2
MLD Snooping last member query interval: admin 1 sec  oper 1 sec
MLD Snooping immediate leave: enabled
MLD Snooping automatic learning of multicast router ports: enabled
```

show ipv6 mld snooping vlan Verify settings of mld snooping vlan.

Syntax

Show ipv6 mld snooping vlan

show ipv6 mld snooping forward-all Display mld snooping forward-all info.

Syntax

show ipv6 mld snooping forward-all [vlan*VLAN-LIST*]

None - Show all ipv6 mld snooping vlan forward-all info

[VLAN-LIST] - Show specific vlan ipv6 mld snooping forward-all info

Default
Show all vlan ipv6 mld forward all info.

Command Mode
Privileged EXEC.

Usage
This command will display ipv6 mld snooping forward-all info.

Example
The following example specifies that show ipv6 mld snooping forward-all test:

```
SC31020#show ipv6 mld snooping forward-all

MLD Snooping VLAN           : 1
MLD Snooping static port    : None
MLD Snooping forbidden port : None

MLD Snooping VLAN           : 2
MLD Snooping static port    : None
MLD Snooping forbidden port : None

MLD Snooping VLAN           : 3
MLD Snooping static port    : None
MLD Snooping forbidden port : None
```

Show ipv6 mld snooping forward-all

Verify settings of mld snooping forward-all.

Syntax

Show ipv6 mld snooping forward-all

show ipv6 mld snooping groups

Display mld snooping groups info.

Syntax

show ipv6 mld snooping groups [*counters* | *dynamic* | *static*]

None - Show all ipv6 mld groups include dynamic and static info

Counters - Show dynamic and static groups counters

(dynamic | static) - Show dynamic or static igmp groups

Default
None.

Command Mode
Privileged EXEC.

Usage
This command will display ipv6 mld snooping groups for dynamic or static or all of type.

Example
The following example specifies that show ipv6 mld snooping groups test:

```
SC31020#show ipv6 mld snooping groups

VLAN |            Group IP Address          |  Type   | Life(Sec) | Port
-----+---------------------------------------+---------+-----------+--------
1 |           ff02::c                       | Dynamic |    259    | gi0/1
1 |           ff02::fb                      | Dynamic |    259    | gi0/1
1 |           ff02::1:3                     | Dynamic |    260    | gi0/1
1 |           ff02::1:ff0d:3c99            | Dynamic |    259    | gi0/1
1 |           ff02::1:ffc5:6583            | Dynamic |    259    | gi0/1

Total Number of Entry = 5
```

Show ipv6 mld snooping groups

Verify mld snooping groups info.

Syntax

Show ipv6 mld snooping groups

show ipv6 mld snooping router

Display mld snooping router info.

Syntax

show ipv6 mld snooping router [*counters*| *dynamic* | *static*]

None - Show all ipv6 mld router include dynamic and static info

(dynamic | static) - Show dynamic or static mld router

Default
None.

Command Mode
Privileged EXEC.

Usage
This command will display ipv6 mld snooping router for dynamic or static or all of type.

Example

The following example specifies that show ipv6 mld snooping router test:

```
SC31020#show ipv6 mld snooping router

Dynamic Router Table
VID   |  Port   | Expiry Time(Sec)
------+---------+-----------------


Total Entry 0


Static Router Table
VID   | Port Mask
------+------------------------
1 | gi0/5


Total Entry 1


Forbidden Router Table
VID   | Port Mask
------+------------------------


 Total Entry 0
```

Show ipv6 mld snooping router

Verify mld snooping router info.

Syntax

Show ipv6 mld snooping router

28 Path Detection

Configure Commands

ping Detect host is reachable or not.include ipv4 address, ipv6 address and domain name.

Syntax

ping *[HOSTNAME]*

[HOSTNAME] - Host name info

Default
None

Command Mode
Privileged EXEC.

Usage
This command will detect host is reachable or not.

Example
The following example specifies that ping test:

```
SC31020#ping fe80::1104:72ba:d80d:3c99

PING fe80::1104:72ba:d80d:3c99 (fe80::1104:72ba:d80d:3c99): 56 data bytes
64 bytes from fe80::1104:72ba:d80d:3c99: icmp6_seq=0 ttl=64 time=10.0 ms
64 bytes from fe80::1104:72ba:d80d:3c99: icmp6_seq=1 ttl=64 time=0.0 ms
64 bytes from fe80::1104:72ba:d80d:3c99: icmp6_seq=2 ttl=64 time=0.0 ms
64 bytes from fe80::1104:72ba:d80d:3c99: icmp6_seq=3 ttl=64 time=0.0 ms
```

ping Adding the host name after the command will check the host is reachable or not.

Syntax

ping *[HOSTNAME]*

traceroute Trace route to network hosts.and record the routing information to the host,include ipv4 address, ipv6 address and domain name.

Syntax

traceroute *[HOSTNAME]*

[HOSTNAME] - Host name info

Default
None

Command Mode
Privileged EXEC.

Usage
This command will record the routing information to the host.

Example
The following example specifies that traceroute test:

```
SC31020#traceroute www.baidu.com
```

traceroute Adding the host name after the command will display the routing information to the host

Syntax

traceroute *[HOSTNAME]*

29 Access Control List

Configure Commands

standard ip access-list Configure the standard ip access-list .By a series of match rules, we can filter network data.

Syntax

ip access-list standard ***{****ACL-name****}***

no ip access-list standard ***{****ACL-name****}***

ACL-name - The name of the ACL (0-9)

Default
None

Command Mode
Configuration mode

Usage
Configuration access control list.

Example

```
ip access-list standard 0
```

show access-list Display access control list information.

Syntax

show access-list

extended ip access-list Configure the extended ip access-list. By a series of match rules, we can filter network data.

Syntax

ip access-list extended {ACL-name**}**

no ip access-list extended {ACL-name**}**

ACL-name - The name of the ACL (10-19)

Default
None

Command Mode
Configuration mode

Usage
Configuration access control list.

Example

```
ip access-list extended 10
```

show access-list Display access control list information.

Syntax

show access-list

ACE configuration Under the ip access-list, config the specific rules.

Syntax

ip access-list {standard|extended} {0-9|10-19**} [**0-9 | deny | end | exit | help | no | permit**]**

0-9 - Config ace number, optional. Default value is 0.

deny - Deny assignable data type, parameter has [any | host | sip]

end - Quit

exit - Back to Previous Level

no - Delete the rules

permit - Permit assignable data type, parameter has [any | host | sip]

Default
Null

Command Mode
ACL Configuration mode

Usage
Configuration ACE.

Example

```
ip access-list standard 0
permit any

ip access-list extended 10
permit ip any any
```

show access-list Display access control list information.

Syntax

show access-list

standard ip access-list deny|permit Under the standard ip access-list, config the deny or permit rules.

Syntax

ip access-list standard {0-9**}[**ace_id**] {deny | permit}** {any | host | sip}

ip access-list standard {0-9**} no {**ace_id**}**

any - any source IP address

host - host IP address

sip - assignable source IP address and mask

ace_id - ACE number (0-9)

Default
Null

Command Mode
ACL Configuration mode

Usage
Configuration ACE.

Example

```
ip access-list standard 0
permit any
```

show access-list Display access control list information.

Syntax

show access-list

extended ip access-list deny|permit

Under the standard ip access-list, config the deny or permit rules.

Syntax

ip access-list extended {10-19} [ace_id] {deny | permit} {ip | tcp | udp} {any | host | sip} [eq] {any | host | dip} [eq]

ip access-list extended {10-19} **no** {ace_id}

ip | tcp | udp - protocol type

any - any source IP address

host - host IP address

sip - assignable source IP address and mask

dip - assignable dest IP address and mask

eq - TCP/UDP port filtering

ace_id - ACE number(0-9)

Default
Null

Command Mode
ACL Configuration mode

Usage
Configuration ACE.

Example

```
ip access-list extended 10
permit ip any any
```

show access-list

Display access control list information.

Syntax

show access-list

ip access-list commit

Use this command, will be AC L Apply to the interface. We can filter rx data.

Syntax

interface GigabitEthernet {port_id}

ip access-list {ACL-name} **commit**

interface GigabitEthernet {port_id}

no ip access-list {ACL-name} **commit**

port_id - Interface ID

ACL-name The name of the ACL

Default
Null

Command Mode
Interface Configuration mode

Usage
Apply the ACL.

Example

```
interface GigabitEthernet 0/1
ip access-list 0 commit
```

standard ipv6 access-list Configure the standard ipv6 access-list. By a series of match rules, we can filter network ipv6 data.

Syntax

ipv6 access-list standard *{ACL-name}*

no ipv6 access-list standard *{ACL-name}*

ACL-name - The name of the ACL (26-35)

Default
Null

Command Mode
Configuration mode

Usage
Configuration access control list.

Example

```
ipv6 access-list standard 26
```

show access-list Display access control list information.

Syntax

show access-list

extended ipv6 access-list

Configure the extended ipv6 access-list. By a series of match rules, we can filter network ipv6 data.

Syntax

ipv6 access-list extended *{ACL-name}*

no ipv6 access-list extended *{ACL-name}*

ACL-name - The name of the ACL (36-45)

Default
Null

Command Mode
Configuration mode

Usage
Configuration access control list.

Example

```
ipv6 access-list standard 36
```

show access-list

Display access control list information.

Syntax

show access-list

ipv6 ACE configuration

Under the ipv6 access-list, config the specific rules.

Syntax

ipv6 access-list {standard | extended} {26-35|36-45} [0-9 | deny | end | exit | help | no | permit]

0-9 - Config ace number, optional. Default value is 0.

deny - Deny assignable data type, parameter has [any | host | sip]

end - Quit

exit - Back to Previous Level

no - Delete the rules

permit - Permit assignable data type, parameter has [any | host | sip]

Default
Null

Command Mode
ipv6 ACL configuration mode

Usage
Configuration ACE

Example

```
ipv6 access-list standard 26
permit any

ipv6 access-list extended 36
permit ip any any
```

show access-list Display access control list information.

Syntax

show access-list

standard ipv6 access-list deny|permit Under the standard ip access-list, config the deny or permit rules.

Syntax

ipv6 access-list standard {26-35} [ace_id] {deny | permit} [any | host | sip]

ipv6 access-list standard {26-35} **no** {ace_id}

any - any source IP address

host - host IP address

sip - assignable source IP address and mask

ace_id - ACE number(0-9)

Default
Null

Command Mode
ACL configuration mode

Usage
Configuration ACE

Example

```
ipv6 access-list standard 26
permit any
```

show access-list Display access control list information.

Syntax

show access-list

extended ipv6 access-list deny|permit Under the extended ip access-list, config the deny or permit rules.

Syntax

ip access-list extended {36-45} [ace_id] {deny | permit} {ip | tcp |udp} {any | host | sip} [eq] {any | host | dip} [eq]

ip access-list extended {36-45} **no** {ace_id}

ip | tcp | udp - protocol type

any - any source IP address

host - host IP address

sip - assignable source IP address and mask

dip - assignable dest IP address and mask

eq - TCP/UDP port filtering

ace_id - ACE number(0-9)

Default
Null

Command Mode
ACL configuration mode

Usage
Configuration ACE

Example

```
ipv6 access-list standard 36
permit ip any any
```

show access-list Display access control list information.

Syntax

show access-list

ipv6 access-list commit

Use this command, Will be ipv6 ACL Apply to the interface. We can filter rx data.

Syntax

interface GigabitEthernet {port_id}

ipv6 access-list {ACL-name} **commit**

interface GigabitEthernet {port_id}

no ipv6 access-list {ACL-name} **commit**

port_id - Interface ID

ACL-name - The name of the ACL

Default
Null

Command Mode
Interface Configuration mode

Usage
Apply the ACL

Example

```
interface GigabitEthernet 0/1
ipv6 access-list 26 commit
```

mac access-list extended

Configure the MAC access-list. By a series of match rules, we can filter network data.

Syntax

mac access-list extended {ACL-name}

no mac access-list extended {ACL-name}

ACL-name - The name of the ACL (20-25)

Default
Null

Command Mode
Configuration mode

Usage
Configuration access control list

Example

```
mac access-list extended 20
```

show access-list Display access control list information.

Syntax

show access-list

mac ACE configuration Under the mac access-list, config the specific rules.

Syntax

mac access-list extended {20-25} [0-9 | deny | end | exit | help | no | permit]

0-9 - Config ace number, optional. Default value is 0.

deny - Deny assignable data type, parameter has [any | host | sip]

end - Quit

exit - Back to Previous Level

no - Delete the rules

permit - Permit assignable data type ?parameter has [any | host | sip]

Default
Null

Command Mode
ACL Configuration mode

Usage
Configuration ACE

Example

```
mac access-list extended 20
permit any
```

show access-list Display access control list information.

Syntax

show access-list

mac access-list deny|permit Under the extended mac access-list, config the deny or permit rules.

Syntax

mac access-list extended {20-25} [ace_id] {deny | permit} {any | host} {any | host} [ethtype]

mac access-list extended {20-25} **no** {ace_id}

any - any source/dest mac address

host - host mac address

ethtype - ethernet frame type

ace_id - ACE number(0-9)

Default
Null

Command Mode
ACL Configuration mode

Usage
Configuration ACE

Example

```
ip access-list extended 10
permit ip any any
```

show access-list Display access control list information.

Syntax

show access-list

mac access-list commit Use this command, Will be mac ACL Apply to the interface. We can filter rx data.

Syntax

interface GigabitEthernet {port_id}

mac access-list {ACL-name} **commit**

interface GigabitEthernet {port_id}

no mac access-list {ACL-name} **commit**

port_id - Interface ID

ACL-name - The name of the ACL

Default
Null

Command Mode
Interface Configuration mode

Usage
Apply the ACL

Example

```
interface GigabitEthernet 0/1
mac access-list 20 commit
```

Display Commands

show access-list Show access-list information.

Syntax

show access-list

Default
Null

Command Mode
Privileged mode

Usage
Display access control list information.

Example

```
show access-list

mac access-list extended 20
0 permit any any

ip access-list standard 0
0 permit any

ip access-list extended 10
0 permit ip any any
```

```
ipv6 access-list standard 26
0 permit any

ipv6 access-list extended 36
```

30 802.1X

Note: If you want this function to take effect, please configure the 802.1X server of RADIUS first.

Configure Commands

authentication dot1x

global switches, If you want to use this function, you must config this command.

Syntax

authentication dot1x

no authentication dot1x

Default
Null

Command Mode
Configuration mode

Usage
Configuration 802.1X

Example

```
authentication dot1x
```

show authentication

Display 802.1x information.

Syntax

show authentication

authentication dot1x

Under the interface, we use this command open port's 802.1X function.

Syntax

interface GigabitEthernet {port_id} **authentication dot1x**

interface GigabitEthernet {port_id} **no authentication dot1x**

port_id - Interface ID

Default
Null

Command Mode
Interface Configuration mode

Usage
Configuration 802.1X

Example

```
interface GigabitEthernet 0/3
authentication dot1x
```

show authentication interface GigabitEthernet

Display 802.1x port information.

Syntax

show authentication interface GigabitEthernet port_id

authentication port-control

Under the interface,we use this command config 802.1X port-control mode.

Syntax

interface GigabitEthernet {port_id} **authentication port-control** {auto | force-auth | force-unauth}

interface GigabitEthernet {port_id} **no authentication port-control**

port_id - Interface ID

auto - auto mode

force-auth - force-auth mode

force-unauth - force-unauth mode

Default
Null

Command Mode
Interface Configuration mode

Usage
Configuration 802.1X port-control mode.

Example

```
interface GigabitEthernet 0/3
 authentication port-control auto
```

show authentication interface GigabitEthernet

Display 802.1x port information.

Syntax

show authentication interface GigabitEthernet port_id

authentication host-mode

Under the interface, we use this command config 802.1X host-mode.

Syntax

interface GigabitEthernet {port_id} **authentication host-mode** {single-host | multi-host | multi-auth}

interface GigabitEthernet {port_id} **no authentication host-mode**

port_id - Interface ID

single-host - Single Host Mode

multi-host - Multiple Host Mode

multi-auth - Multiple Authentication Mode

Default
Multi-auth

Command Mode
Interface Configuration mode

Usage
Configuration 802.1X port-control mode.

Example

```
interface GigabitEthernet 0/3
 authentication host-mode multi-host
```

show authentication interface GigabitEthernet

Display 802.1x port information.

Syntax

show authentication interface GigabitEthernet port_id

Display Commands

show authentication Show 802.1X information.

Syntax

show authentication {interfaces GigabitEthernet port_id**}**

port_id - Interface ID

Default

Null

Command Mode

Privileged mode

Usage

Display 802.1X information.

Example

```
Show authentication interface GigabitEthernet0/3

Interface Configurations

Interface GigabitEthernet0/3

Admin Control          : force-unauth
Host Mode              : multi-host
Type dot1x State       : enabled
Type mac State         : disabled
Type web State         : disabled
Type Order             : dot1x
MAC/WEB Method Order   : radius
Guest VLAN             : disabled
Reauthentication       : disabled
Max Hosts              : 256
VLAN Assign Mode       : static

Common Timers
Reauthenticate Period: 3600
Inactive Timeout     : 60
Quiet Period         : 60

802.1x Parameters
EAP Max Request      : 2
EAP TX Period        : 30
Supplicant Timeout   : 30
Server Timeout       : 30

Web-auth Parameters
Login Attempt        : 3
```

31 AAA

Configure Commands

radius host Configure all the parameters that switch connect to the radius server.

Syntax

radius host {host_name} [auth-port] {port_id} [key] {key} [priority] {pri_value} [retransmit] {retransmit_times} [timeout] {timeout_vlaue} [type] {auth_type}

no radius host {ip_addr}

host_name - radius sever ip address or domain name

port_id - TCP/UDP port number, default is 1812.(0-65535)

key - Radius server key

pri_value - Priority vlaue,(1-65534)

retransmit_times - The number of retransmit, default is 3.(1-10)

timeout_vlaue - Timeout value in seconds to wait for server to reply.(1-30)

auth_type - Usage type.[802.1x|login|all]

Default
port_id:1812
retransmit_times:3

Command Mode
Configuration mode

Usage
Configuration radius.

Example

```
radius host 192.168.100.1 auth-port 1812 key public priority 1 retransmit 1
  timeout 1 type all
```

show radius Display radius information.

Syntax

show radius

tacacs host Configure all the parameters that switch connect to the tacacs server.

Syntax

tacacs host {host_name} [port] {port_id} [key] {key} [priority] {pri_value} [timeout] {timeout_vlaue}

no tacacs host {ip_addr}

host_name - Tacacs sever ip address or domain name

port_id - TCP/UDP port number,default is 49.(0-65535)

key - Tacacs server key

pri_value - priority vlaue,(1-65534)

timeout_value - Timeout value in seconds to wait for server to reply.(1-30)

Default
port_id:49

Command Mode
Configuration mode

Usage
Configuration tacacs.

Example

```
tacacs host 192.168.100.1 port 49 key public priority 1 timeout 30
```

show tacacs Display tacacs information.

Syntax

show tacacs

aaa authentication enable Configure enable authentication method.

Syntax

aaa authentication {enable} {list_name} {auth_method_list}

no aaa authentication {enable} {list_name}

list_name - Auth Method List Name

auth_method_list - Enable Authentication Method List. [radius |tacacs+ | enable]

Default
port_id:49

Command Mode
Configuration mode

Usage
Configure enable authentication method.

Example

```
aaa authentication enable Xn enable tacacs+ radius
```

show aaa authentication enable lists

Display enable authentication information.

Syntax

show aaa authentication enable lists

aaa authentication login

Configure login authentication method. Login include telnet and SSH.

Syntax

aaa authentication {login} {list_name} {auth_method_list}

no aaa authentication {login} {list_name}

list_name - Auth Method List Name

auth_method_list - Login Authentication Method List. [radius |tacacs+ | enable]

Default
Null

Command Mode
Configuration mode

Usage
Configure login authentication method.

Example

```
aaa authentication login Xn local radius tacacs+
```

show aaa authentication login lists

Display login authentication information.

Syntax

show aaa authentication login lists

line telnet

If you want to login by telnet and need AAA authentication, you must config this command.

Syntax

line telnet login authentication {Login_auth_list_name}

enable authentication {enable_auth_list_name}

line telnet

no login authentication

no enable authentication

Login_auth_list_name - Login auth Method List Name

enable_auth_list_name - Enable auth Method List Name

Default
Null

Command Mode
Configuration mode

Usage
Configure telnet authentication method.

Example

```
line telnet
login authentication Xn
enable authentication Xn
```

show line lists

Display telnet authentication information.

Syntax

show line lists

line ssh

If you want to login by ssh and need AAA authentication, you must config this command.

Syntax

line ssh

login authentication {Login_auth_list_name}

enable authentication {enable_auth_list_name}

line ssh

no login authentication

no enable authentication

Login_auth_list_name - Login auth Method List Name

enable_auth_list_name - Enable auth Method List Name

Default
Null

Command Mode
Configuration mode

Usage
Configure ssh authentication method.

Example

```
line ssh
login authentication Xn
enable authentication Xn
```

show line lists Display ssh authentication information.

Syntax

show line lists

Display Commands

show radius Show radius information.

Syntax

show radius

Default
Null

Command Mode
Privileged mode

Usage
Display radius information.

Example
Show radius:

```
Prio |   IP Address    | Auth-Port| Retries| Timeout|    Type    |   Key
-----+-----------------+----------+--------+--------+------------+--------
 1   |  192.168.100.1 |   1812    |   1   |    1   |    All     | public
```

show tacacs Show tacacs information.

Syntax

show tacacs

Default
Null

Command Mode
Privileged mode

Usage
Display tacacs information.

Example

```
Prio | Timeout |     IP Address     |  Port  |   Key
-----+---------+--------------------+--------+----------
1    |   30    |   192.168.100.1    |   49   |  public
```

show aaa authentication enable list Show aaa authentication information.

Syntax

show aaa authentication enable list

Default
Null

Command Mode
Privileged mode

Usage
Display aaa authentication information.

Example

```
show aaa authentication enable list


Enable List Name      Authentication Method List
------------------| -------------------------------
default           |   enable
Xn                |   enable tacacs+ radius
```

sshow aaa authentication login list

Show aaa authentication information.

Syntax

show aaa authentication login list

Default
Null

Command Mode
Privileged mode

Usage
Display aaa authentication information.

Example

```
show aaa authentication login lists

Login List Name      Authentication Method List
------------------| -------------------------------
default           |   local
  Xn              |   enable radius tacacs+
```

32 SSH

Configure Commands

ip ssh Enable ssh function.

Syntax

ip ssh [all | v1 | v2]

no ip ssh [all | v1| v2]

[all|v1|v2]ssh version number

Default
Null

Command Mode
Configuration mode

Usage
Configuration radius.

Example

```
ip ssh
```

33 SSL

Configure Commands

ssl Generate ssl digital certificate.

Syntax

ssl

Default
Null

Command Mode
Privileged mode

Usage
Generate new certificate

Example

```
ssl
```

ssl replace Make the new ssl digital certificate work.

Syntax

ssl replace

Default
Null

Command Mode
Privileged mode

Usage
Make the new ssl digital certificate work.

Example

```
ssl replace
```

34 QoS

Configure Commands

qos trust Config qos classify mode.

Syntax

qos trust {classify_mode}

no qos trust

classify_mode - Qos Classify mode: [cos | dscp]

Default
Null

Command Mode
Configuration mode

Usage
Config qos classify mode

Example

```
qos queue trust dscp
```

show qos Display qos information.

Syntax

show qos

qos queue schedule Config qos schedule algorithm.

Syntax

qos queue schedule {schedule_mode}

schedule_mode - Qos schedule mode: [sp | wrr | hybird]

Default
Null

Command Mode
Configuration mode

Usage
Config qos schedule algorithm.

Example

```
qos queue schedule wrr
```

show qos queueing Display qos queue information.

Syntax

show qos queueing

qos map cos-queue Config qos queue mapping relationship.

Syntax

qos map cos-queue {cos_value} **to** {queue_num}

cos_value - Cos value

queue_num - Queue number (1-8)

Default
Null

Command Mode
Configuration mode

Usage
Config qos queue mapping relationship

Example

```
qos map cos-queue 1 to 1
```

show qos map cos-queue Display qos map information.

Syntax

show qos map cos-queue

qos map dscp-queue Config qos queue mapping relationship.

Syntax

qos map dscp-queue {dscp_value} **to** {queue_num}

dscp_value - DSCP value

queue_num - Queue number (1-8)

Default
Null

Command Mode
Configuration mode

Usage
Config qos queue mapping relationship.

Example

```
qos map dscp-queue 1 to 8
```

show qos map dscp-queue Display qos queue map information.

Syntax

show qos map dscp-queue

qos map weight When you use WRR mode, you need config every queues weight value.you must use this command.

Syntax

qos map weight {weight_values}

weight_values - weight_values (1-127)

Default
Null

Command Mode
Configuration mode

Usage
Config qos queue weight.

Example

```
qos queue weight 1 1 1 50 50 50 100 100
```

show qos map queueing Display qos queue information.

Syntax

show qos map queueing

qos queue strict-priority-num When you use hybird mode, you need config SP schedule queue's number.you must use this command.

Syntax

qos queue strict-priority-num {SP_num}

weight_values - weight_values (1-127)

Default
Null

Command Mode
Configuration mode

Usage
Config qos queue weight.

Example

```
qos queue weight 1 1 1 50 50 50 100 100
```

Display Commands

show qos Show qos information.

Syntax

show qos

Default
Null

Command Mode
Privileged mode

Usage
Display qos information.

Example

```
show qos
QoS Mode: enable
Basic trust: cos
```

show qos queueing Show qos queue information.

Syntax

show qos queueing

Default
Null

Command Mode
Privileged mode

Usage
Display qos queueing information.

Example

```
show qos queueing
queue Schedule Alg: hybrid
qid-weights    Ef - Priority
1 -   1         dis - N/A
2 -   2         dis - N/A
3 -   3         dis - N/A
4 -   4         dis - N/A
5 -   5         dis - N/A
6 -   6         dis - N/A
7 -   10        dis - N/A
8 -   N/A       ena - 8
```

show qos map cos-queue Show qos queue information.

Syntax

show qos map cos-queue

Default
Null

Command Mode
Privileged mode

Usage
Display qos map information.

Example
Show qos map cos-queue

```
CoS to Queue mappings
COS      0  1  2  3  4  5  6  7
--------------------------------
Queue    2  1  1  2  3  3  4  4
```

show qos map dscp-queue

Show qos queue information.

Syntax

show qos map dscp-queue

Default
Null

Command Mode
Privileged mode

Usage
Display qos map information.

Example
Show qos map dscp-queue

```
DSCP to Queue mappings

d1: d2  0  1  2  3  4  5  6  7  8  9
---------------------------------------
0:      8  8  8  8  8  8  2  2  2  2
1:      2  2  2  2  2  2  2  2  2  2
2:      2  2  2  2  2  2  2  2  2  2
3:      2  2  2  2  2  2  2  2  2  2
4:      2  2  2  2  2  2  2  2  2  2
5:      2  2  2  2  2  2  2  2  2  2
6:      2  2  2  2
```

35 PoE Commands

Configure Commands

poe enable Enable the power supply capability of the POE port.

Syntax

poe enable

no poe enable

poe enable - Enable POE power supply function, the default is on

no poe enable - Turn off POE power supply

Default
Enabled

Command Mode
Interface Configuration mode

Usage
Use this command to enable/disable the remote power supply capability of the port.

Example

```
SC31020(config-if-GigabitEthernet0/1)# poe enable
SC31020(config-if-GigabitEthernet0/1)# no poe enable
```

show poe interfaces configuration View the configuration information of current interface POE.

Syntax

show poe interfaces configuration

poe mode Configure the power management mode of the POE system.

Syntax

poe mode auto

poe mode energy-saving

poe mode static

auto - Set the power management mode to automatic mode, which is the default mode for POE devices

energy-saving - Set the power management mode to energy saving mode, which is an optional mode for POE devices

static - Set the power management mode to static mode, which is an optional mode for POE devices

Default
Energy saving

Command Mode
Global Configuration mode

Usage
Execute the following command to set the system power management mode.

Example

```
SC31020(config)# poe mode auto
SC31020(config)# poe mode energy-saving
SC31020(config)# poe mode static
```

show poe powersupply

View the poe system configuration information.

Syntax

show poe powersupply

poe max-power

Set the system maximum power.

Syntax

poe max-power

no poe max-power

int - Maximum power in the range <6, 11, 20, 32, 35 W>

Default
35 W

Command Mode
Interface Configuration mode

Usage
Use this command to configure the maximum power of the port.

Example

```
SC31020(config)# interface GigabitEthernet 0/1
SC31020(config-if-GigabitEthernet0/1)# poe max-power 20
```

show poe interfaces configuration

View the poe interface configuration information.

Syntax

show poe interfaces configuration

poe alloc-power

Set the system allocation power.

Syntax

poe alloc-power

no poe alloc-power

int - Allocation power in the range <6, 11, 20, 32, 35 W>

Default
35 W

Command Mode
Interface Configuration mode

Usage
Use this command to configure the allocation power of the port in static mode.

Example

```
SC31020(config)# interface GigabitEthernet 0/1
SC31020(config-if-GigabitEthernet0/1)# poe alloc-power 20
```

show poe interfaces configuration

View the poe interface configuration information.

Syntax

show poe interfaces configuration

poe timer enable

Enable the POE timer.

Syntax

poe timer enable

no poe timer enable

poe timer enable - Enable POE timer

no poe timer enable - Disable POE timer

Default
POE timer disabled

Command Mode
Global Configuration mode

Usage
Use this command to enable / disable the remote power supply capability of the port.

Example

```
SC31020(config)# poe timer enable
SC31020(config)# no poe timer enable
```

show poe timer View the configuration information of current interface POE timer.

Syntax

show poe timer

poe timer configuration Set the poe timer mode.

Syntax

Set the poe timer mode

absolute - Set poe power to the absolute time

periodic - Set the poe power cycle time

Default
Null

Command Mode
Interface Configuration mode

Usage
Use the command to set the poe power supply time.

Example

```
SC31020(config)# poe timer enable
SC31020(config)# interface GigabitEthernet 0/5
SC31020(config-if-GigabitEthernet0/5)# poe timer periodic everyday 8:30 to
  19:30 mon to wed
SC31020(config-if-GigabitEthernet0/5)# poe timer absolute start 08:30 jul 25
  2017 stop 18:30 sep 30 2017
```

show poe timer View the configuration information of current interface POE timer information.

Syntax

show poe timer

Display Relevant Commands

show poe interface View the POE configuration and status information for the specified port.

Syntax

show poe interface gigabitEthernet port-id

port-id - Allocation power in the range <6, 11, 20, 32, 35 W>

Default
Null

Command Mode
Privileged Configuration mode

Usage
Execute this command to view the POE status of the specified port.

Example

```
SC31020# show poe interfaces GigabitEthernet 0/1

Interface               : gi0/1
Pd Description          :
Power control           : Normal
Power status            : Detecting
Max power               : 35 W
Allocate power          : 35 W
Current power           : 0 W
Average power           : 0 W
Peak power              : 0 W
Voltage                 : 52.908 V
Current                 : 0 mA
```

```
PD class                : NoPd
Trouble cause           : None
Trouble Recover Mode    : auto
Power management        : Energy-saving
SC31020#
```

show poe interfaces View the PoE status or configuration of all ports.

Syntax

show poe interfaces status

show poe interfaces configuration

Default
Null

Command Mode
Privileged Configuration mode

Usage
Execute this command to view the POE status or configuration of all ports.

Example

```
SC31020# show poe interfaces status

Interface  Power    Power    Curr   Avg    Peak   Curr    Trouble PD    Port
           Control  Status   Power  Power  Power  Current  Cause  Class Voltage
-------------------------------------------------------------------------------
gi0/1      Normal   Detecting 0W    0W     0W     0mA       0     N/A    0V
gi0/2      Normal   Detecting 0W    0W     0W     0mA       0     N/A    0V
gi0/3      Normal   Detecting 0W    0W     0W     0mA       0     N/A    0V
gi0/4      Normal   Detecting 0W    0W     0W     0mA       0     N/A    0V
gi0/5      Normal   Detecting 0W    0W     0W     0mA       0     N/A    0V
gi0/6      Normal   Detecting 0W    0W     0W     0mA       0     N/A    0V
gi0/7      Normal   Detecting 0W    0W     0W     0mA       0     N/A    0V
gi0/8      Normal   Detecting 0W    0W     0W     0mA       0     N/A    0V
SC31020#
```

show poe powersupply View the current power state of the POE system.

Syntax

show poe powersupply

Default
Null

Command Mode
Privileged Configuration mode

Usage
Execute this command to view the power supply status of the current POE system.

Example

```
SC31020# show poe powersupply
Powering Port List           :
Power Management Method      : Energy-saving
Poe interruptible power      : Disable
System Total Power           : 70 W
Power Consumption            : 0 W
Available power              : 70 W [100%]
```

show poe timer View the poe timer.

Syntax

show poe timer

Default
Null

Command Mode
Privileged Configuration mode

Usage
Execute this command to view the current poe timer information.

Example

```
SC31020# show poe timer
PORT      | Timer mode |   Start timer |   Stop timer
----------+------------+---------------+--------------
    1     |   Periodic |  Wednesday 8:0| Friday 23:0
```

36 SNMP Commands

SNMP Configuration Commands

snmp enable Enable the SNMP agent.

Syntax

Snmp enable

snmp enable - Enable the SNMP agent, the default is off

Default
Close the SNMP agent.

Command Mode
Global Configuration mode

Usage
Use this command to configure and enable the SNMP agent, Ipv6 snmp is enabled at the same time.

Example

```
SC31020(config)# snmp enable
```

show snmp View the current SNMP status.

Syntax

show snmp

no snmp enable Close the SNMP agent.

Syntax

no snmp enable

snmp enable - Enable the SNMP agent, the default is off

Default
Close the SNMP agent.

Command Mode
Global Configuration mode

Usage
Use this command to configure and shut down the SNMP agent.

Example

```
SC31020(config)# no snmp enable
```

show snmp View the current SNMP status.

Syntax

show snmp

snmp enable traps To enable SNMP to actively send trap messages to the NMS to report some urgent and important events, run the global configuration command snmp-server enable traps. The no form of this command disables SNMP from the NMS Send the Trap message pro-actively.

Syntax

snmp-server enable traps

no snmp-server enable traps

snmp-server - enable trapsOpen the trap function

no snmp-server - enable trapsClose the trap function

Default
Disable

Command Mode
Global Configuration mode

Usage
The command must be used in conjunction with the global configuration command snmp-server host to send trap messages.

Example

```
SC31020(config)# snmp-server enable traps
SC31020(config)# no snmp-server enable traps
```

show snmp View the current SNMP status.

Syntax

show snmp

snmp-server community To specify the access characters for the SNMP community, perform the global configuration command snmp-server community.

Syntax

snmp-server community *Community name* **[ro | rw| view]**

community name - Community name

Default
Null

Command Mode
Global Configuration mode

Usage
This command is used with the global configuration command snmp-server enable traps to send trap messages to the NMS.

Example

```
SC31020(config)# snmp-server community test rw
```

show snmp community View Community Information.

Syntax

show snmp community

snmp-server host To specify the SNMP host (NMS) that sends trap messages, execute the global configuration command snmp-server host.The no form of the command deletes the specified SNMP host.

Syntax

snmp-server host {host-addr **[traps]** [version {1 | 2c |2} community name}

no snmp-server host community name

host-addr - Receive the Trap host IP address

community name - Community name

version - SNMP supported version, this device supports v1, V2c, v3

Default
There is no default SNMP host.

Command Mode
Global Configuration mode

Usage
This command is used with the global configuration command snmp-server enable traps to send trap messages to the NMS.

Example

```
SC31020(config)# snmp-server host 192.168.100.149 traps
version 1 test

SC31020(config)# no snmp-server host 192.168.100.149 traps
version 1 test
```

show snmp host View the host information of the receiving trap configured by the user.

Syntax

show snmp host

snmp trap auth In the device can be based on the interface configuration whether to send the interface LinkTrap, when the function is turned on, if the authentication fails, SNMP will issue authTrap, otherwise not made. Use the no option for this command SNMP will not issue authTrap.

Syntax

snmp trap auth

no snmp trap auth

Default
The function opens, and if the interface auth fails, SNMP will issue authTrap.

Command Mode
Global Configuration mode

Usage
When the function is turned on, if auth fails to change, SNMP will be issued AuthTrap.

Example

```
SC31020(config)# snmp trap auth
SC31020(config)# no snmp trap auth
```

show snmp trap View the snmp trap configuration.

Syntax

show snmp trap

snmp trap link-status In the device can be based on the interface configuration whether to send the interface LinkTrap, when the function is turned on, if the interface Link status changes, SNMP will send LinkTrap, otherwise not made. Use the no option for this command SNMP will not send LinkTrap.

Syntax

snmp trap linkUp

snmp trap linkDown

Default
This function is enabled. If the link status changes, SNMP will send LinkTrap.

Command Mode
Global Configuration mode

Usage
For the interface (Ethernet interface, Ap interface, SVI interface), the command configures whether to send the interface LinkTrap, when the function is turned on, if the interface changes Link state, SNMP will be issued LinkTrap.

Example

```
SC31020(config)# snmp trap linkUp
SC31020(config)# snmp trap linkDown
```

show snmp trap View the snmp trap configuration.

Syntax

show snmp trap

snmp trap restart For warm-start and cold-start, open the trap function, after the success of the restart will send the relevant trap message.

Syntax

snmp trap cold-start

snmp trap warm-start

Default
This function is enabled.If the switch reboots or restarts, the trap message is sent after a successful reboot.

Command Mode
Global Configuration mode

Usage
For warm-start and cold-start, open the trap function, after the success of the restart will send the relevant trap message.

Example

```
SC31020(config)# snmp trap cold-start
SC31020(config)# snmp trap warm-start
```

show snmp trap View the snmp trap configuration.

Syntax

show snmp trap

snmp trap stp When this function is enabled, when the topology changes or a new root bridge is created, the trap information of stp is sent and no trap information is sent.

Syntax

snmp trap stp

no snmp trap stp

Default
This function default is disabled.If he topology changes or a new root bridge is created, the trap information of stp is sent and no trap information is sent.

Command Mode
Global Configuration mode

Usage
When the topology changes or a new root bridge is created, the trap information of stp is sent and no trap information is sent.

Example

```
SC31020(config)# snmp trap stp
SC31020(config)# no snmp trap stp
```

show snmp trap View the snmp trap configuration.

Syntax

show snmp trap

SNMP Display Relevant Commands

show snmp-status Displays the current SNMP on state.

Syntax

show snmp

Command Mode
Privilege Configuration mode

Example

```
SC31020# show snmp
SNMP is enabled.
```

show snmp trap Displays the current SNMP trap status.

Syntax

show snmp trap

Command Mode
Privilege Configuration mode

Example

```
SC31020# show snmp trap
SNMP global trap  : Enable
SNMP auth failed trap  : Enable
SNMP linkUp trap   : Enable
SNMP linkDown trap   : Enable
SNMP cold-start trap   : Enable
SNMP warm-start trap   : Enable
SNMP stp trap   : Enable
```

show snmp community

Displays the current SNMP community status.

Syntax

show snmp community

Command Mode
Privilege Configuration mode

Example

```
SC31020# show snmp community
Community Name       Group Name       View                Access
-------------------- ---------------- ------------------- ------------
private                   -             all                 rw
public                    -             all                 ro
```

show snmp host

Displays the host that receives the trap information.

Syntax

show snmp host

Command Mode
Privilege Configuration mode

Example

```
SC31020# show snmp host
Server            Community/User Name   Notification Version    Notification
  Type    UDP Port
Retries     Timeout
--------------------------------------------------------------------------------
  ----------------------------------------
192.168.100.139   test               v1                   trap
  162         --           --
Total Entries: 1
```

37 LLDP Settings

SNMP Configuration Commands

lldp enable

LLDP is a Layer 2 protocol that allows network devices to advertise their own device identities and performance on the local subnet.

Syntax

lldp

no lldp

Default
Disable

Command Mode
Global Configuration mode

Usage
Use “lldp” command to enable LLDP RX/TX ability. The LLDP enable status is displayed b y “show lldp” command. Use the no form of this command to disable the LLDP.

Example

```
SC31020(config)# lldp
SC31020(config)# no lldp
```

show lldp

Display lldp information.

Syntax

show lldp

lldp rx

When the port works in Rx mode, the device only receives non-sending neighbor devices to send LLDP packets.

Syntax

lldp rx

no lldp rx

Default
Disable

Command Mode
Interface Configuration mode

Usage
Use “lldp rx” command to enable LLDP PDU RX ability. The configuration is displayed b y “show lldp” command.

Example

```
SC31020(config-if-GigabitEthernet0/1)# lldp rx
SC31020(config-if-GigabitEthernet0/1)# no lldp rx
```

show lldp Display lldp information.

Syntax

show lldp

lldp tx-interval Declare local capacity to send the message.

Syntax

lldp tx-interval <5-32767>

no lldp tx-interval

<5-32767> - Specify the lldp pdu tx interval in unit of second

Default
Default tx-interval is 30s

Command Mode
Global Configuration mode

Usage
Use “lldp tx-interval” command to enable LLDP TX interval.it should be noticed that both”lldp tx-interval” and “lldp tx-delay” affects the lldp pdu tx time, the large value of the two configuration decides the TX interval, the configuration is displayed by “show lldp” command.

Example

```
SC31020(config)# lldp tx-interval 10
SC31020(config)# no lldp tx-interval
```

show lldp Display lldp information.

Syntax

show lldp

lldp reinit-delay LLDP module re-initialization delay.

Syntax

lldp reinit-delay <1-10>

no lldp reinit-delay

<1-10> - Specify th e LLDP re-initial delay time in unit of second

Default
Default reinit-delay is 2s

Command Mode
Global Configuration mode

Usage
Use “lldp reinit-delay” command to configure LLDP reinit-delay. The delay avoids LLDP generate too many pdu if the port up and down frequently. The delay starts to count when the port links down. The port would not generate lldp pdu until the delay counts to zero. The configuration is displayed by “show lldp” command. Use the no form of this command to disable the LLDP.

Example

```
SC31020(config)# lldp reinit-delay 5
SC31020(config)# no lldp reinit-delay
```

show lldp Display lldp information.

Syntax

show lldp

lldp holdtime-multiplier The message time is multiples.

Syntax

lldp holdtime-multiplier <2-10>

no holdtime-multiplier

<2-10> - Specify the LLDP hold time multiplier

Default
Lldp holdtime-multiplier 4

Command Mode
Global Configuration mode

Usage
Use “lldp holdtime-multiplier” command to con figure the LLDP PDU holdmultiplier that decides time-to-live (TTL) value sent in LLDP advertisements: TTL = (tx-interval * holdtime-multiplier). The configuration could be shown by “show lldp” command.

Example

```
SC31020(config)# lldp holdtime-multiplier 3
SC31020(config)# no lldp holdtime-multiplier
```

show lldp Display lldp information.

Syntax

show lldp

lldp lldpdu LLDPPDUs are LLDP payloads that carry messages to be sent.

Syntax

lldp lldpdu (bridging | filtering | flooding)

bridging - When lldp is globally disabled, lldp packets are briging (bridging lldp pdu to vlan number ports)

filtering - When lldp is globally disabled, lldp packets are filtered (deleted)

flooding - When lldp is globally disabled, lldp packets are flooded (forwarded to all interfaces)

Default
Default lldp pdu handling behaviour when lldp dsabled is flooding.

Command Mode
Global Configuration mode

Usage
Use “lldp lldpdu” command to configure the LLDP pdu handling behavior.When lldp is globally disabled it should be noticed that if lldp is globally enabled and per port lldp rx status is configured to disabled, the received lldp pdu would be dropped instead of taking the global disable behavior. The configuration is displayed b y “show lldp” command.

Example

```
SC31020(config)# lldp lldpdu bridging
```

show lldp Display lldp information.

Syntax

show lldp

lldp med LLDP module re-initialization delay.

Syntax

lldp med

no lldp med

Default
lldp med

Command Mode
Interface Configuration mode

Usage
Use “lldp med” to configure the LLDP MED enable status. If LLDP MED is enabled, LLDP MED capability TLV and other selected MED TLV would be attached. The configuration could be shown by “show lldp med” command. Use the no form of this command to restore the behavior to default.

Example

```
SC31020(config-if-GigabitEthernet0/1)# lldp med
SC31020(config-if-GigabitEthernet0/1)# no lldp med
```

show lldp Display lldp information.

Syntax

show lldp

lldp med fast-start-repeat-count

Configure LLDP MED fast start repeat count.

Syntax

lldp med f ast-start-repeat-count <1-10 >

no lldp med fast-start-repeat-count

<1-10> - LLDP PDU fast start TX repeat counts.

Default
Default fast start TX repeat count is 3

Command Mode
Global Configuration mode

Usage
Use “lldp lldp med f ast-start-repeat-count” command to configure the LLDP bpdu fast start tx repeat .when port links down,it will send lldp pdu immediately to notify link partner. The number of lldp pdu sends when it links up depends on fast-start-repeat-count configuration, the lldp pdu fast-start transmits in interval of one second.the fast start behavior works no matter lldp med is enabled or not attached. The configuration could be shown by “show lldp med” command. Use the no form of this command to restore the behavior to default.

Example

```
SC31020(config)# lldp med fast-start-repeat-count 3
```

show lldp med

Display lldp med information.

Syntax

show lldp med

lldp med tlv-select

Configure the tlv and no commands to add lldp packets to send tlv for lldp packets.

Syntax

lldp med tlv-select MEDTLV [MEDTLV] [MEDTLV] [MEDTLV]

no lldp med tlv-select

MEDTLV - MED optional TLV. Available optional TLVs are network-policy, location, poe-pse, inventory.

Default
network-policy TLV

Command Mode
Interface Configuration mode

Usage
Use “lldp med tlv-select” command to configure the LLDP MED TLV selection. It should be noticed that even no MED TLV is selected, MED capability TLV would be attached if LLDP MED is enable.The configuration could be shown by “show lldp med” command. Use the no form of this command to remove all selected med tlv over the dedicated ports.

Example

```
SC31020(config-if-GigabitEthernet0/1)# lldp med tlv-select network-policy
SC31020(config-if-GigabitEthernet0/1)# no lldp med tlv-s elect
```

show lldp interfaces GigabitEthernet 0/1

Display lldp information.

Syntax

show lldp interfaces GigabitEthernet 0/1

lldp tlv-select

Configure the tlv and no commands to add lldp packets to send tlv for lldp packets.

Syntax

lldp tlv-select TLV [TLV] [TLV] [TLV] [TLV] [TLV] [TLV] [TLV]

no lldp tlv-select

TLV - LLDP optional TLV, pick from: port-desc, sys-name, sys-desc, sys-cap, mac-phy, lag, max-frame-size, management-addr

Default
Default is no selected optional TLV.

Command Mode
Interface Configuration mode

Usage
Use “lldp tlv-select” command to attach selected TLV in PDU. The configuration could be shown b y “show lldp” command. Use the no form of this command to remove all selected TLV. This example selects system name, system description, system capability.

Example

```
SC31020(config-if-GigabitEthernet0/1)# lldp tlv-select sys-desc
SC31020(config-if-GigabitEthernet0/1)# no lldp tlv-select
```

show lldp interfaces GigabitEthernet 0/1

Display lldp information.

Syntax

show lldp interfaces GigabitEthernet 0/1

lldp tlv-select pvid

Configure the tlv and no commands to add lldp packets to send tlv for lldp packets.

Syntax

lldp tlv-select pvid (disable | enable)

no lldp tlv-select pvid

disable - Disable lldp 802.1pvid tlv attach state

enable - Enable lldp 802.1pvid tlv attach state

Default
Default is enabled

Command Mode
Interface Configuration mode

Usage
Use “lldp tlv-select pvid” command to configure the 802.1 PVID TLV attach enable status. The configuration could be shown by “show lldp” command.

Example

```
SC31020(config-if-GigabitEthernet0/1)# lldp tlv-select pvid enable
SC31020(config-if-GigabitEthernet0/1)# lldp tlv-select pvid disable
```

show lldp interfaces GigabitEthernet 0/1

Display lldp information.

Syntax

show lldp interfaces GigabitEthernet 0/1

lldp tlv-select vlan-name

Configure the tlv and no commands to add lldp packets to send tlv for lldp packets.

Syntax

lldp tlv-select vlan-name add (add | remove) vlan-list

no lldp tlv-select

VLAN-LIST - VLAN List (e.g. 3, 6-8): The range of VLAN ID is 2 to 4094

Default
No VLAN added

Command Mode
Interface Configuration mode

Usage
Use “lldp tlv-select vlan-name” command to add or remove VLANlist for 802.1 VLAN-NAME TLV. The configuration could be shown by “show lldp” command.

Example

```
SC31020(config-if-GigabitEthernet0/1)# lldp tlv-select vlan-name add 1
SC31020(config-if-GigabitEthernet0/1)# no lldp tlv-select
```

show lldp interfaces GigabitEthernet 0/1

Display lldp information.

Syntax

show lldp interfaces GigabitEthernet 0/1

lldp tx

When the port works in tx mode, the device only sends LLDP packets that do not accept neighbor devices to send LLDP packets.

Syntax

lldp tx

no lldp tx

Default
Disable

Command Mode
Interface Configuration mode

Usage
Use “lldp tx” command to enable LLDP PDU TX ability. The configuration is displayed b y “show lldp” command.

Example

```
SC31020(config-if-GigabitEthernet0/1)# lldp tx
SC31020(config-if-GigabitEthernet0/1)# no lldp tx
```

show lldp Display lldp information.

Syntax

show lldp

lldp tx-delay When the port works in tx mode, the device only sends LLDP packets that do not accept neighbor devices to send LLDP packets.

Syntax

lldp tx

no lldp tx

<1-8192> - Specify the lldp tx delay in unit of seconds

Default
Default tx delay is 2s

Command Mode
Global Configuration mode

Usage
Use “lldp tx-delay” command to configure the delay in seconds between successive LLDP frame transmissions. The delay starts to count in any case LLDP PDU is sent such as by LLDP PDU advertise routine, LLDP PDU content change, port link up, etc. The configuration could be shown b y “show lldp” command. Use the no form of this command to restore the delay to default value.

Example

```
SC31020(config)# lldp tx-delay 5
SC31020(config)# no lldp tx-delay
```

show lldp Display lldp information.

Syntax

show lldp

show lldp interfaces GigabitEthernet

Syntax

show lldp interfaces GigabitEthernet <1-10>

<1-10> - Gigabit Ethernet device number

Default
Null

Command Mode
Privileged Configuration mode

Usage
Display lldp information and port-related lldp information

Example

```
SC31020# show lldp interfaces GigabitEthernet 0/1
State: Enabled
Timer: 30 Seconds
Hold multiplier: 4
Reinit delay: 2 Seconds
Tx delay: 2 Seconds
LLDP packet handling: Bridging

Port     |  State | Optional TLVs  | Address
-------- + ------ + -------------- + --------
gi0/1    |Disable |                | 192.168.100.151
Port ID: gi0/1
802.3 optional TLVs:
802.1 optional TLVs
PVID: Disabled
VLANs: 1
```

show lldp local-device

Displays the current SNMP community status.

Syntax

show lldp

show lldp interfaces GigabitEthernet <1-10> local-device

<1-10> - Gigabit Ethernet device number

Default
Null

Command Mode
Privileged Configuration mode

Usage
Use “show lldp local-device” command to show the local configuration of lldp pdu.

Example

```
SC31020# show lldp interfaces GigabitEthernet 0/1
SC31020# show lldp  local-device
LLDP Local Device Information:
Chassis Type : Mac Address
Chassis ID   : 00E0.4C01.7899
System Name  : SC31020
System Description  :
System Capabilities Support : Bridge
System Capabilities Enable  : Bridge
Management Address : 192.168.100.151(IPv4)
Management Address : fe80::2e0:4cff:fe01:7899(IPv6)
```

show lldp med Displays the current SNMP community status.

Syntax

show lldp

show lldp interfaces GigabitEthernet <1-10> med

<1-10> - Gigabit Ethernet device number

Default
Null

Command Mode
Privileged Configuration mode

Usage
Use “show lldp med” command to display lldp med configuration information

Example

```
SC31020# show lldp med
Fast Start Repeat Count: 3
lldp med network-policy voice: manual
Port   | Capabilities | Network Policy | Location | Inventory | PoE PSE
------ + ------------ + -------------- + -------- + --------- + -------
gi0/1  |      No      |       No       |    No    |    No     |   N/A
gi0/2  |      No      |       Yes      |    No    |    No     |   N/A
gi0/3  |      No      |       Yes      |    No    |    No     |   N/A
gi0/4  |      No      |       Yes      |    No    |    No     |   N/A
gi0/5  |      No      |       Yes      |    No    |    No     |   N/A
gi0/6  |      No      |       Yes      |    No    |    No     |   N/A
gi0/7  |      No      |       Yes      |    No    |    No     |   N/A
gi0/8  |      No      |       Yes      |    No    |    No     |   N/A
gi0/9  |      No      |       Yes      |    No    |    No     |   N/A
gi0/10 |      No      |       Yes      |    No    |    No     |   N/A
```

show lldp neighbor

Displays the current SNMP community status.

Syntax

show lldp neighbor

Default

Null

Command Mode

Privileged Configuration mode

Usage

Use “show lldp neighbor” command to display the received neighbor lldp PDU information. When LLDP PDU is received on LLDP RX enable ports, system would store the PDU information in database until time to live of the Pdu counts down to zero.

Example

```
SC31020# show lldp neighbor
Port |   Device ID      |   Port ID    |   SysName      |  Capabilities  |  TTL
---- + ---------------- + ------------ + -------------- + -------------- + ----
gi0/4 |  00E0.4C01.7899 |        gi0/1 |                |                |   100
```

show lldp statistics

Displays the current SNMP community status.

Syntax

show lldp statistics

Default

Null

Command Mode

Privileged Configuration mode

Usage

Use “show lldp statistics” command to display the LLDP RX/TX statistics.

Example

```
SC31020# show lldp statistics
LLDP Global Statistics:
Insertions : 1
Deletions  : 0
Drops      : 0
Age Outs   : 0
| TX Frames |         RX Frames          |          RX TLVs         | RX Ageouts
       Port  |   Total    | Total | Discarded | Errors | Discarded |
  Unrecognized |    Total
```

```
--------+-----------+-------+-----------+--------+-----------+--------------
  +-----------
  gi0/1 |        12 |     0 |         0 |      0 |         0 |            0 |
  0
  gi0/2 |         0 |     0 |         0 |      0 |         0 |            0 |
  0
  gi0/3 |         0 |     0 |         0 |      0 |         0 |            0 |
  0
  gi0/4 |         3 |     3 |         0 |      0 |         0 |            0 |
  0
  gi0/5 |         0 |     0 |         0 |      0 |         0 |            0 |
  0
 gi0/6 |         0 |     0 |         0 |      0 |         0 |            0 |
  0
 gi0/7 |         0 |     0 |         0 |      0 |         0 |            0 |
  0
 gi0/8 |         0 |     0 |         0 |      0 |         0 |            0 |
  0
  gi0/9 |         0 |     0 |         0 |      0 |         0 |            0 |
  0
 gi0/10 |         0 |     0 |         0 |      0 |         0 |            0 |
  0
               |                 |   100
```

38 System Settings Commands

Basic System Settings

management-vlan Configure system management vlan.

Syntax

management-vlan vlan vlanid

vlanid - The vlanid is In the rang of <1-4094>

Default
vlan1

Command Mode
Global Configuration mode

Usage
Use this command to configure the system management vlan.

Example

```
SC31020(config)# management-vlan vlan 1
```

show management-vlan Display management vlan.

Syntax

show management-vlan

ipv6 dhcp Configure the ip DHCP.

Syntax

ipv6 dhcp

Default
Null

Command Mode
Global Configuration mode

Usage
Use this command to Configure the ip address of the switch.

Example

```
SC31020(config)# ip dhcp
```

show ip Display management ip information.

Syntax

show ip

management ip Configure system management ip.

Syntax

Ip address x.x.x.x

Ip address - The int is in the range of <0-255>

mask - The int is in the range of <0-255>

default-gateway - The int is in the range of <0-255>

Default
192.168.2.10

Command Mode
Global Configuration mode

Usage
Use this command to configure the system management ip.

Example

```
SC31020(config)# ip address 192.168.2.10 mask 255.255.255.0
SC31020(config)# ip default-gateway 192.168.2.1
```

show ip Display management ip information.

Syntax

show ip

location Configure the system location

Syntax

location

address - Set host location address

relation - Set host location relation

telephone - Set host location telephone

Default
Null

Command Mode
Global Configuration mode

Usage
Use this command to configure the system location.

Example

```
SC31020(config)# location address 11111111
SC31020(config)# location relation switch
SC31020(config)# location telephone 1234567890
```

show location Configure the ipv6 address of the switch.

Syntax

show location

ipv6 Configure the system location.

Syntax

Ipv6 address X:X::X:X

IPv6 gateway X:X::X:X

Ipv6 address - The int is In the rang of <0-255>

prefix - <0-128>

Ipv6 gateway - X:X::X:X IPv6 gateway

Default
Null

Command Mode
Global Configuration mode

Usage
Use this command to Configure the ipv6 address of the switch.

Example

```
SC31020(config)# ipv6 address 2001::5 prefix 64
SC31020(config)# ipv6 default-gateway 2001::1
```

show ipv6 Display management ipv6 information.

Syntax

show ipv6

ipv6 dhcp Configure the ipv6 DHCP.

Syntax

Ipv6 dhcp

Default
Null

Command Mode
Global Configuration mode

Usage
Use this command to Configure the ipv6 address of the switch.

Example

```
SC31020(config)# ipv6 dhcp
```

show ipv6 Display management ipv6 information.

Syntax

show ipv6

ip telnet Configure the system to telnet.

Syntax

ip telnet

Default
Null

Command Mode
Global Configuration mode

Usage
Use this command Configure the system to telnet.

Example

```
SC31020(config)# ip telnet
SC31020(config)# no ip telnet
```

Log Export Export the current configuration of the system.

Syntax

copy flash://ram.log tftp://

flash:// - Copy from flash: file system. flash://startup-config; flash://running-config; flash://backup-config; flash://ram.log

tftp:// - Copy from tftp: file system (tftp://serverip/filename)

Default
Null

Command Mode
Privileged Configuration mode

Usage
Use this command to Export the current configuration of the system.

Example

```
SC31020# copy flash://ram.log tftp://192.168.100.149/8
```

restart system System restart

Syntax

reload

Default
Null

Command Mode
Privileged Configuration mode

Usage
Use this command to restart the system.

Example

```
SC31020# reload
```

change password Change password

Syntax

username web xx **password** xx

WORD - User name

password - user password

Default
Null

Command Mode
Global Configuration mode

Usage
Use this command to change password.

Example

```
SC31020(config)# username web admin password admin
```

show username Display username information

Syntax

show username

system log Display system log

Syntax

show logging buffered

Default
Null

Command Mode
Privileged Configuration mode

Usage
Use this command to Display system log.

Example

```
SC31020# show logging buffered
Log messages in buffer
5;Jan 01 2000 00:02:22;%SYSTEM-5-INFO: Logging is enabled
5;Jan 01 2000 00:02:22;%SYSTEM-5-RESTART: System restarted - Warm
Start
5;Jan 01 2000 00:02:24;%LINEPROTO-5-UPDOWN: Line protocol on
GigabitEthernet0/1, changed state to up
5;Jan 01 2000 00:47:34;%AAA-5-LOGIN: New telnet connection for
user admin, source 192.168.100.131  ACCEPTED
5;Jan 01 2000 00:47:43;%AAA-5-LOGIN: New telnet connection for
user admin, source 192.168.100.149  ACCEPTED
5;Jan 01 2000 00:50:45;%SYSTEM-5-INFO: Logging host is set to
enabled with host 192.168.100.149 (192.168.100.149), port 514,
severity emerg, alert, crit, error, warning, notice
5;Jan 01 2000 00:52:54;%SYSTEM-5-INFO: Logging host is set to
enabled with host 192.168.100.149 (192.168.100.149), port 514,
severity emerg, alert, crit, error, warning, notice
SC31020#
```

arp table Display arp table.

Syntax

show arp

Default
Null

Command Mode
Privileged Configuration mode

Usage
Use this command to configure the system management ip.

Example

```
SC31020# show
arpAddress       HWtype  HWaddress           Flags Mask      Iface
192.168.100.149  ether   40:16:7E:B1:EB:6D   C               eth0
```

configure static MAC binding

Configure the MAC addresses of the server and other important equipment to the static MAC address table.

Syntax

mac-address static *mac-address* **vlan** *vlan-id* **interface gigabitEthernet** *port-id*

no mac-address static *mac-address* **vlan** *vlan-id* **interface gigabitEthernet** *port-id*

mac-address - Add the mac address

vlan-id - Add the specified vlan

port-id - The interface number bound to it

Default
Null

Command Mode
Global Configuration mode

Usage
If you bind a MAC address to a designated port as a static address, it will not age with aging time.

Example

```
SC31020(config)#  mac-address static 0001.7A55.E7D2 vlan 1 interfaces
  GigabitEthernet 0/1
SC31020(config)# no mac-address static 0001.7A55.E7D2 vlan 1
```

show mac-address static

Display static mac-address all in switch.

Syntax

show mac-address static

MAC address drop

When a MAC address is filtered out in a specified vlan, the MAC data can not be forwarded through this switch. Use the no command to delete the configuration.

Syntax

mac-address static *mac-address* **vlan** *vlan-id* **drop**

no mac-address static *mac-address* **vlan** *vlan-id* **drop**

drop - The mac address to filter

Default
Null

Command Mode
Global Configuration mode

Usage
If you will be a MAC address in a designated vlan filter out, then the MAC data can not be forwarded through this switch.

Example

```
SC31020(config)#  mac-address static 0001.7A55.E7D5 vlan 1 drop
```

show mac-address drop

Display drop mac-address all in switch.

Syntax

show mac-address drop

mac-address aging-time

Configure the aging time of the MAC address.

Syntax

mac-address aging-time

aging-time - <10-630> Aging time value

Default
630s

Command Mode
Global Configuration mode

Usage
Use this command to drop some MAC address.

Example

```
SC31020(config)#  mac-address aging-time 500
```

show mac-address aging-time

Display mac-address aging-time.

Syntax

show mac-address aging-time

show mac-address count

Display the number of MAC addresses in the FDB table.

Syntax

show mac-address count

count - Displays the current number of mac addresses

Default

Null

Command Mode

Privileged Configuration mode

Usage

Use this command to drop some MAC address.

Example

```
SC31020# show mac-address count
Static Mac Address Count     : 0
Drop Mac Address Count       : 0
Dynamic Mac Address Count    : 15
Total number of entries      : 15
```

show mac-address

View information about all bound address tables.

Syntax

show mac-address [drop | dynamic | static | vlan vlan-id {dynamic | static} | interface port-number {drop | dynamic | static}]

show mac-address static - Displays the static MAC address.

show mac-address drop - Displays the filtered MAC address.

show mac-address dynamic - Displays the dynamic MAC address.

show mac-address interface - Displays the MAC address of the specified port

show mac-address vlan - Displays the MAC address of the specified VLAN

Default

Null

Command Mode

Privileged Configuration mode

Usage

Use this command to view all MAC address.

Example

```
SC31020# show mac-address all
```

show running-config View the current configuration.

Syntax

show running-config

Default
Null

Command Mode
Privileged Configuration mode

Usage
Use this command to view the current configuration.

Example

```
SC31020# show running-config
```

save configuration Save the current configuration of the switch.

Syntax

write

Default
Null

Command Mode
Privileged Configuration mode

Usage
Use this command to Save the current configuration of the switch.

Example

```
SC31020# write
```

restore-defaults Restore the switch configuration to the factory.

Syntax

restore-defaults

Default
Null

Command Mode
Privileged Configuration mode

Usage
Restore the switch configuration to the default.

Example

```
SC31020# restore-defaults
```

Firmware Upgrade

Firmware Upgrade

Syntax

flash:// - Copy from flash: file system. flash://startup-config flash://running-config flash://backup-config flash://ram.log

tftp:// - Copy from tftp: file system.(tftp://serverip/filename)

Default
Null

Command Mode
Privileged Configuration mode

Usage
Use this command to upgrade the system.

Example

```
SC31020# copy tftp://192.168.100.149/vmlinux.bix flash://image.bin
```

Firmware Backup

Firmware Backup

Syntax

flash:// - Copy from flash: file system. flash://startup-config flash://running-config flash://backup-config flash://ram.log

tftp:// - Copy from tftp: file system.(tftp://serverip/filename)

Default
Null

Command Mode
Privileged Configuration mode

Usage
Use this command to Export the current configuration of the system.

Example

```
SC31020# copy flash://running-config tftp://192.168.100.149/xxx
```

download configuration Download configuration.

Syntax

flash:// - Copy from flash: file system. flash://startup-config flash://running-config flash://backup-config flash://ram.log

tftp:// - Copy from tftp: file system.(tftp://serverip/filename)

Default
Null

Command Mode
Privileged Configuration mode

Usage
Use this command inport the current configuration of the system.

Example

```
copy tftp://192.168.100.149/xxx running-config
```

Memory information Display Memory information.

Syntax

show memory

Default
Null

Command Mode
Privileged Configuration mode

Usage
Use this command to Display Memory information.

Example

```
SC31020# show memory
total(KB)     used(KB)     free(KB)   shared(KB)   buffer(KB)   cache(KB)
-------------------+------------+------------+------------+------------+---
  ---------
Mem:          127372        76764        50608            0         2740
  24888
-/+ buffers/cache:          49136        78236
Swap:              0            0            0
SC31020#
```

CPU Information

Display CPU information.

Syntax

show cpu

Default
Null

Command Mode
Privileged Configuration mode

Usage
Use this command to Display CPU information.

Example

```
SC31020# show cpu
CPU:     5% used,    95% free
```

Flash Information

Display flash information.

Syntax

show flash

Default
Null

Command Mode
Privileged Configuration mode

Usage
Use this command to Display flash information.

Example

```
SC31020# show flash
       File Name             File Size        Modified
------------------------ ---------------- ------------------------
startup-config           1691             2000-01-01 00:49:44
rsa1                     976              2000-01-01 00:01:02
rsa2                     1679             2000-01-01 00:01:37
dsa2                     668              2000-01-01 00:02:04
ssl_cert                 891              2000-01-01 00:02:08
image                    7740274          2017-05-31 18:29:07
```

Cable Information

Display cable information.

Syntax

show cable-diag

Default
Null

Command Mode
Privileged Configuration mode

Usage
Use this command to Display cable information.

Example

```
SC31020# show cable-diag interfaces GigabitEthernet 0/1
Port    |  Speed | Local pair | Pair length | Pair status
-------+--------+------------+-------------+---------------
 gi0/1 |  auto  |    Pair A  |     6.00    | Normal
                   Pair B  |     6.00    | Normal
                   Pair C  |     6.00    | Normal
                   Pair D  |     6.00    | Normal
```

web-language

Configure switch web-language.

Syntax

web-language en

Default
Null

Command Mode
Global Configuration mode

Usage
Use this command to configure the switch web-language.

Example

```
SC31020(config)# web-language en
```

show web-language Display the switch web-language.

Syntax

show web-language

ip address Configure system management ip.

Syntax

Ip address x.x.x.x

Ip address - The int is In the rang of <0-255>

mask - The int is In the rang of <0-255>

default-gateway - The int is In the rang of <0-255>

Default
192.168.2.10

Command Mode
Global Configuration mode

Usage
Use this command to configure the system management ip.

Example

```
SC31020(config)# ip address 192.168.2.10 mask 255.255.255.0
SC31020(config)# ip default-gateway 192.168.2.1
```

show ip Display management ip information.

Syntax

show ip

show version Displays the current version of switch.

Syntax

show version

Default
Null

Command Mode
Privileged Configuration mode

Usage
View the current version.

Example

```
SC31020 Operating System Software
SC31020 system image file (system-firmware.bin), version 17257, Compiled   on
  Jun 15 2017 - 18:52:19
Copyright@2016 SC31020 Systems, Inc.
SC31020 Version Information
Hardware Version  : B1
SN number         : 11000001
MAC Address       : 00E0.4C00.0000
Loader Version    : 1.00.002
Loader Date       : Mar 09 2020 - 11:49:09
Firmware Version  : v0.0.0.1
Firmware Date     : Jun 15 2020 - 18:52:19
System Uptime is 8 hours 54 minutes 48 seconds
```

Ip dhcp server Enable dhcp server.

Syntax

ip dhcp server

Default
Null

Command Mode
Global Configuration mode

Usage
Enable dhcp server.

Example

```
SC31020(config)# ip dhcp server
SC31020(config)# no ip dhcp server
```

show ip dhcp server Display ip dhcp server information.

Syntax

show ip dhcp server

ip dhcpserver Configure DHCP server

Syntax

ip dhcpserver

pool - IP Pool is A.B.C.D-E.F.G.H. Between addresses is '-

Default
Null

Command Mode
Global Configuration mode

Usage
Set the DHCP server to assign ip to client.

Example

```
SC31020(config)# ip dhcpserver pool 192.168.2.100-192.168.2.200
```

show ip dhcp server Display ip dhcp server information.

Syntax

show ip dhcp server

39 DHCP Relay

DHCP Relay

dhcp relay enable Enable ip dhcp relay.

Syntax

Ip dhcp relay - Enable the ip dhcp relay

Default
Disabled

Command Mode
Global Configuration mode

Usage
Use this command to configure and enable the ip dhcp relay globally.

Example

```
SC31020(config)# ip dhcp relay
SC31020(config)# no ip dhcp relay
```

show ip dhcp relay Display ip dhcp relay information.

Syntax

show ip dhcp relay

dhcp-relay vlan Enable DHCP relay information 82 for VLAN.

Syntax

dhcp-relay vlan - Enable the dhcp-relay vlan

Default
Disabled

Command Mode
Global Configuration mode

Usage
There be DHCP relay information 82 for VLANs enabled.

Example

```
SC31020(config)# dhcp-relay vlan 1-4094
SC31020(config)# no dhcp-relay vlan 1-4094
```

show ip dhcp relay Display ip dhcp relay information.

Syntax

show ip dhcp relay

Ip dhcp relay Enable DHCP relay information 82 for ports

Syntax

Ip dhcp relay - Enable the ip dhcp relay

Default
Disabled

Command Mode
Interface Configuration mode

Usage
There be DHCP relay information 82 for VLANs enabled

Example

```
SC31020(config-if-GigabitEthernet0/1)# ip dhcp relay
SC31020(config-if-GigabitEthernet0/1)# no ip dhcp relay
```

show dhcp-relay interfaces GigabitEthernet 0/1 Display ip DHCP relay information for ports.

Syntax

show dhcp-relay interfaces GigabitEthernet 0/1

option 82 of remote-ID Configure DHCP relay information 82 of remote-ID.

Syntax

dhcp-relay option remote-id

STRING - ID string (1~63)

Default
DUT's MAC address

Command Mode
Global Configuration mode

Usage
A "remote ID" containing the switch's information as a trusted identifier for the remote high-speed modem.

Example

```
SC31020(config)# dhcp-relay option remote-id 192.168.2.10
```

show dhcp-relay Display DHCP relay information.

Syntax

show dhcp-relay

option 82 of CID Configure DHCP relay information 82 of circuit-ID.

Syntax

dhcp-relay interfaces GigabitEthernet 0/5

STRING - ID string (1~63)

Default
CID in DHCP relay information 82 of L2 relay contains VLAN-unit-port information from which the packet is received.

Command Mode
Interface Configuration mode

Usage
It indicates that the received DHCP request message is from the link identifier.

Example

```
SC31020(config-if-GigabitEthernet0/5)# dhcp-relay vlan 1 option circuit-id v5
```

show dhcp-relay interfaces GigabitEthernet 0/5

Display DCHCP relay of CID information.

Syntax

show dhcp-relay interfaces GigabitEthernet 0/5

DHCP relay policy

Configure global DHCP relay policy.

Syntax

dhcp-relay option action (drop | keep | replace)

drop - Drop packets with option82

keep - Keep original option82

replace - Replace option82 content by switch setting

Default
The global DHCP relay policy shall be drop.

Command Mode
Global Configuration mode

Usage
DHCP relay information 82 of L2 relay policy.

Example

```
SC31020(config)# dhcp-relay option action drop
```

show dhcp-relay

Display DHCP relay information.

Syntax

show dhcp-relay

ip dhcp relay ttl remark

Set DHCP relay information of L2 relay remarked TTL value.

Syntax

ip dhcp relay ttl remark <0-120>

<0-120> - TTL remark value

Default
Disabled

Command Mode
Global Configuration mode

Usage
Set DHCP relay information of L2 relay remarked TTL value.

Example

```
SC31020(config)# ip dhcp relay ttl remark 50
```

show ip dhcp relay Display DHCP relay information.

Syntax

show ip dhcp relay

DHCP relay server address Configure the server ip address.

Syntax

ip helper-address *x.x.x.x*

x.x.x.x - Server ip address

Default
The global DHCP relay server address shall be zero in system.

Command Mode
Global Configuration mode

Usage
Configure the server ip address .

Example

```
SC31020(config)# ip helper-address 192.168.2.15
```

show ip dhcp relay Display ip DHCP relay information.

Syntax

show ip dhcp relay

Section III

Appendices

This section provides additional information and includes these items:

K Troubleshooting

Problems Accessing the Management Interface

Table 162: Troubleshooting Chart

Symptom	Action
Cannot connect using Telnet, or SNMP software	◆ Be sure the switch is powered up. ◆ Check network cabling between the management station and the switch. Make sure the ends are properly connected and there is no damage to the cable. Test the cable if necessary. ◆ Check that you have a valid network connection to the switch and that the port you are using has not been disabled. ◆ Be sure you have configured the VLAN interface through which the management station is connected with a valid IP address, subnet mask and default gateway. ◆ Be sure the management station has an IP address in the same subnet as the switch's IP interface to which it is connected. ◆ If you are trying to connect to the switch via the IP address for a tagged VLAN group, your management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag. ◆ If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.
Cannot connect using Secure Shell	◆ If you cannot connect using SSH, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time. ◆ Be sure the control parameters for the SSH server are properly configured on the switch, and that the SSH client software is properly configured on the management station. ◆ Be sure you have generated both an RSA and DSA public key on the switch, exported this key to the SSH client, and enabled SSH service. Try using another SSH client or check for updates to your SSH client application. ◆ Be sure you have set up an account on the switch for each SSH user, including user name, authentication level, and password. ◆ Be sure you have imported the client's public key to the switch (if public key authentication is used).
Forgot or lost the password	◆ Press and hold the reset button on the front panel for 5 seconds to reset to the default configuration (including the password).

License Information

This product includes copyrighted third-party software subject to the terms of the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other related free software licenses. The GPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, refer to the section "The GNU General Public License" below, or refer to the applicable license as included in the source-code archive.

The GNU General Public License

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

1. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

2. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

   In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

6. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

8. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

9. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

10. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

    Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

11. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

1. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

2. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Glossary

ACL Access Control List. ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (i.e., Layer 2) information.

ARP Address Resolution Protocol converts between IP addresses and MAC (hardware) addresses. ARP is used to locate the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next.

BOOTP Boot Protocol. BOOTP is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

BGP Border Gateway Protocol is a protocol used to make core routing decisions on the Internet. It maintains a table of IP networks to register reachability among autonomous systems (AS). BGP makes routing decisions based on path, network policies and/or rule-sets.

CoS Class of Service is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

DHCP Dynamic Host Control Protocol. Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

DHCP Option 82 A relay option for sending information about the requesting client (or an intermediate relay agent) in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server. This

information can be used by DHCP servers to assign fixed IP addresses, or set other services or policies for clients.

DHCP Snooping A technique used to enhance network security by snooping on DHCP server messages to track the physical location of hosts, ensure that hosts only use the IP addresses assigned to them, and ensure that only authorized DHCP servers are accessible.

DiffServ Differentiated Services provides quality of service on large networks by employing a well-defined set of building blocks from which a variety of aggregate forwarding behaviors may be built. Each packet carries information (DS byte) used by each hop to give it a particular forwarding treatment, or per-hop behavior, at each network node. DiffServ allocates different levels of service to users on the network with mechanisms such as traffic meters, shapers/droppers, packet markers at the boundaries of the network.

DNS Domain Name Service. A system used for translating host names for network nodes into IP addresses.

DSCP Differentiated Services Code Point Service. DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.

EAPOL Extensible Authentication Protocol over LAN. EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1X Port Authentication standard.

EUI Extended Universal Identifier is an address format used by IPv6 to identify the host portion of the network address. The interface identifier in EUI compatible addresses is based on the link-layer (MAC) address of an interface. Interface identifiers used in global unicast and other IPv6 address types are 64 bits long and may be constructed in the EUI-64 format. The modified EUI-64 format interface ID is derived from a 48-bit link-layer address by inserting the hexadecimal number FFFE between the upper three bytes (OUI field) and the lower 3 bytes (serial number) of the link layer address. To ensure that the chosen address is from a unique Ethernet MAC address, the 7th bit in the high-order byte is set to 1 (equivalent to the IEEE Global/Local bit) to indicate the uniqueness of the 48-bit address.

GARP Generic Attribute Registration Protocol. GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

GMRP Generic Multicast Registration Protocol. GMRP allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.

GVRP GARP VLAN Registration Protocol. Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

ICMP Internet Control Message Protocol is a network layer protocol that reports errors in processing IP packets. ICMP is also used by routers to feed back information about better routing choices.

IEEE 802.1D Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1p An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

IEEE 802.1s An IEEE standard for the Multiple Spanning Tree Protocol (MSTP) which provides independent spanning trees for VLAN groups.

IEEE 802.1w An IEEE standard for the Rapid Spanning Tree Protocol (RSTP) which reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard. (Now incorporated in IEEE 802.1D-2004)

IEEE 802.1X Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

IEEE 802.3ac Defines frame extensions for VLAN tagging.

IEEE 802.3x Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links. (Now incorporated in IEEE 802.3-2002)

IGMP Internet Group Management Protocol. A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the "querier" and assumes responsibility for keeping track of group membership.

IGMP Proxy Proxies multicast group membership information onto the upstream interface based on IGMP messages monitored on downstream interfaces, and forwards multicast traffic based on that information. There is no need for multicast routing protocols in an simple tree that uses IGMP Proxy.

IGMP Query On each subnetwork, one IGMP-capable device will act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

IGMP Snooping Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

In-Band Management Management of the network from a station attached directly to the network.

IP Multicast Filtering A process whereby this switch can pass multicast traffic along to participating hosts.

IP Precedence The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories by default, but may be configured differently to suit the requirements for specific network applications.

LACP Link Aggregation Control Protocol. Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

Layer 2 Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

Layer 3 Network layer in the ISO 7-Layer Data Communications Protocol. This layer handles the routing functions for data moving from one open system to another.

Link Aggregation *See Port Trunk.*

LLDP Link Layer Discovery Protocol is used to discover basic information about neighboring devices in the local broadcast domain by using periodic broadcasts to advertise information such as device identification, capabilities and configuration settings.

MD5 MD5 Message-Digest is an algorithm that is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

MIB Management Information Base. An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

MRD Multicast Router Discovery is a A protocol used by IGMP snooping and multicast routing devices to discover which interfaces are attached to multicast routers. This process allows IGMP-enabled devices to determine where to send multicast source and group membership messages.

MSTP Multiple Spanning Tree Protocol can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group.

Multicast Switching A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

MVR Multicast VLAN Registration is a method of using a single network-wide multicast VLAN to transmit common services, such as such as television channels or video-on-demand, across a service-provider's network. MVR simplifies the configuration of multicast services by using a common VLAN for distribution, while still preserving security and data isolation for subscribers residing in both the MVR VLAN and other standard groups.

NTP Network Time Protocol provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

OSPF Open Shortest Path First is a link-state routing protocol that functions better over a larger network such as the Internet, as opposed to distance-vector routing protocols such as RIP. It includes features such as unlimited hop count, authentication of routing updates, and Variable Length Subnet Masks (VLSM).

Out-of-Band Management Management of the network from a station not attached to the network.

Port Authentication *See IEEE 802.1X*.

Port Mirroring A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

Port Trunk Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

QinQ QinQ tunneling is designed for service providers carrying traffic for multiple customers across their networks. It is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs.

QoS Quality of Service. QoS refers to the capability of a network to provide better service to selected traffic flows using features such as data prioritization, queuing, congestion avoidance and traffic shaping. These features effectively provide preferential treatment to specific flows either by raising the priority of one flow or limiting the priority of another flow.

RADIUS Remote Authentication Dial-in User Service. RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

RIP Routing Information Protocol seeks to find the shortest route to another device by minimizing the distance-vector, or hop count, which serves as a rough estimate of transmission cost. RIP-2 is a compatible upgrade to RIP. It adds useful capabilities for subnet routing, authentication, and multicast transmissions.

RMON Remote Monitoring. RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

RSTP Rapid Spanning Tree Protocol. RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

SMTP Simple Mail Transfer Protocol is a standard host-to-host mail transport protocol that operates over TCP, port 25.

SNMP Simple Network Management Protocol. The application protocol in the Internet suite of protocols which offers network management services.

SNTP Simple Network Time Protocol allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

SSH Secure Shell is a secure replacement for remote access functions, including Telnet. SSH can authenticate users with a cryptographic key, and encrypt data connections between management clients and the switch.

STA Spanning Tree Algorithm is a technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

TACACS+ Terminal Access Controller Access Control System Plus. TACACS+ is a logon authentication protocol that uses software running on a central server to control access to TACACS-compliant devices on the network.

TCP/IP Transmission Control Protocol/Internet Protocol. Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

Telnet Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

TFTP Trivial File Transfer Protocol. A TCP/IP protocol commonly used for software downloads.

UDP User Datagram Protocol. UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

UTC Universal Time Coordinate. UTC is a time scale that couples Greenwich Mean Time (based solely on the Earth's rotation rate) with highly accurate atomic time. The UTC does not have daylight saving time.

VLAN Virtual LAN. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

VRRP Virtual Router Redundancy Protocol uses a virtual IP address to support a primary router and multiple backup routers. The backups can be configured to take over the workload if the master fails or to load share the traffic. The primary goal of VRRP is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

XModem A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

Commands

Index