AVCOMM G3-8000

The 3rd Generation of 8000 series

User Manual

Command Line Interface (CLI)

Reference Products:

Product Name: The 3rd Generation of 8000 Series, Industrial Ethernet Switch, Fully Managed, PTP/TSN
Model Number: 8008TX, 8010GX2, 8012GX4, 8014GX4
Document Title: RM_CLI_EN, G3 8000_CLI_EN
Document Version: 3.2
Release Date: July, 2025

Company Information

Company Name: Avcomm Technologies, Inc.
Address: 1300 Bay Area, B229, Houston, TX 77058, United States of America
Phone: +1 713-933-4534
Email: info@avcomm.us
Website: www.avcomm.us

Technical Support

If you encounter any problems during installation or operation of this product, please contact our technical support team.
Technical Support Email: support@avcomm.us
Technical Support Phone: +1 713-933-4534
Business Hours: Monday – Friday, 08:00 – 18:00 US. Central Time

Sales Information

For product purchasing, pricing, or distributor information, please contact our sales team.
Sales Email: sales@avcomm.us
Sales Phone: +1 713-933-4534

AVCOMM®
— INDUSTRIAL AI —

Disclaimer

The information in this document is subject to change without notice and does not represent a commitment on the part of Avcomm Technologies, Inc.

Avcomm Technolgoies, Inc. assumes no responsibility for any errors that may appear in this document. In no event shall Avcomm Technolgoies, Inc. be liable for direct, indirect, special, incidental, or consequential damages resulting from the use of this product or the information contained in this document.

Trademarks

All trademarks, registered trademarks, and product names mentioned in this document are the property of their respective owners.

Compliance and Certifications

This product complies with applicable standards and regulations.
Certifications may include but are not limited to:
CE
FCC
RoHS
Other applicable certifications

Content

Safety Instructions

⚠ WARNING

UNCONTROLLED MACHINE ACTIONS

To avoid uncontrolled machine actions caused by data loss, configure all the data transmission devices individually.

Before you start any machine which is controlled via data transmission, be sure to complete the configuration of all data transmission devices.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

About This Manual

The "Command Line Interface" reference manual contains detailed information on using the Command Line Interface to operate the individual functions of the device.
The manual is designed to describe configuration steps, and support for features should be based on the specific device.

Command Structure

The Command Line Interface (CLI) syntax, conventions and terminology are described in this section. Each CLI command is illustrated using the structure outlined below.

Format

Some commands, such as `clear ip statistics`, do not require parameters. Other commands, such as `ip route`, have parameters for which you must supply a value. Parameters are positional - you must type the values in the correct order. Optional parameters will follow required parameters. For example:

Example 1

`ip route <ipv4_subnet> <ipv4_ucast> [ distance <1-255> ]`

- `ip route`
  is the command name.
- `<ipv4_subnet> <ipv4_ucast>`
  are the required values for the command.
- `[ distance <1-255> ]`
  is the optional value for the command.

Example 2

`ip address <ipv4_subnet>`

- `ip address`
  is the command name.
- `<ipv4_subnet>`
  is the required parameter for the command.

Example 3

`clear ip statistics`

- `clear ip statistics`
  is the command name.

Command

The following conventions apply to the command name:

- The command name is displayed in this document in courier font and is to be typed exactly as shown.
- Once you have entered enough letters of a command name to uniquely identify the command, pressing the *<Tab key>* will cause the system to complete the word.
- Entering Ctrl-Z will return you to the root level command prompt.

Parameters

Parameters are order dependent.
Which are to be replaced with a name or number.
Parameters may be mandatory values, optional values, choices, or a combination.

- *<parameter>*. The **<>** angle brackets indicate that a mandatory parameter is to be entered in place of the brackets and text inside them.
- `[parameter]`. The **[]** square brackets indicate that an optional parameter may be entered in place of the brackets and text inside them.
- `choice1 | choice2`. Vertical bars "`|`" separate alternative, mutually exclusive, elements.
- The { } curly braces indicate that a parameter must be chosen from the list of choices.
- Braces within square brackets [{ }] indicate a required choice within an optional element.

Special keys

Certain special key combinations speed up use of the CLI. They are listed in this section. Also, help is available for the CLI by typing **HELP:**

Ctrl-A	go to beginning of line
Ctrl-E	go to end of line
Ctrl-F	go forward one character
Ctrl-B	go backward one character
Ctrl-D	delete current character
Ctrl-U, X	delete to beginning of line
Ctrl-K	delete to end of line
Ctrl-W	delete previous word
Ctrl-P	go to previous line in history buffer
Ctrl-Z	return to root command prompt
Tab	command-line completion
Exit	go to next lower command prompt
?	list choices

Quick Start Up

Quick Starting the Switch

- The device must be configured with IP information (IP address, subnet mask, and default gateway).
- Turn the Power on.
- Allow the device to load the software until the login prompt appears. The device‘s initial state is called the default mode.
- The device's serial port baud rate is 115200. It is recommended to use PuTTY or MobaXterm to log in.
- When the prompt asks for operator login, execute the following steps:

1. Type the word `admin` in the login area. Since a number of the Quick Setup commands require administrator account rights, we recommend logging into an administrator account. Press the enter key.
2. Enter the password `admin`.
3. Press the enter key.
4. The CLI Privileged EXEC prompt will be displayed.
   Privileged EXEC prompt:
   ```
   Switch#
   ```
5. Use “configure terminal” to switch to the Global Config mode from Privileged EXEC.
   Global Config prompt:
   ```
   Switch (config)#
   ```
6. Use “exit” to return to the previous mode.

Mode-based CLI

The CLI groups all the commands in appropriate modes according to the nature of the command. A sample of the CLI command modes are described below. Each of the command modes support specific software commands.

- APS Mode
- CFM MA Configuration Mode
- CFM MD Configuration Mode
- CFM MEP Configuration Mode
- DHCP Pool Configuration Mode
- ERPS Mode
- Global Configuration Mode
- IPMC Profile Mode
- JSON Notification Host Mode
- Keychain Mode
- Line Configuration Mode
- LLAG Mode
- Loopback Interface Mode
- MRP Configuration Mode
- OSPF Router Mode
- OSPFv3 Router Mode
- Port Configuration Mode
- QoS Egress Map Mode
- QoS Ingress Map Mode
- RedBox Mode
- RIP Router Mode
- SNMP Server Host Mode
- STP Aggregation Mode
- STREAM Configuration Mode
- STREAM-COLLECTION Configuration Mode
- TSN FRER configuration Mode
- TSN PSFP Flow Meter Mode
- TSN PSFP Stream Filter Mode
- TSN PSFP Stream Gate Mode
- Uart Mode
- User Exec Mode
- VLAN Configuration Mode
- VLAN Interface Mode

Mode-based Command Hierarchy

The CLI is divided into various modes. The Commands in one mode are not available until the operator switches to that particular mode, with the exception of the User Exec mode commands.
The commands available to the operator at any point in time depend upon the mode. Entering a question mark (?) at the CLI prompt, displays a list of the available commands and descriptions of the commands. The CLI provides the following modes:

APS Mode

This mode groups all the commands pertaining to APS. The command prompt shown at this level is:

```
Switch(config)# aps 1
Switch(config-aps)#
```

CFM MA Configuration Mode

This mode groups all the commands pertaining to CFM MA. The command prompt shown at this level is:

```
Switch(config-cfm-dmn)# service aaa
Switch(config-cfm-dmn-svc)#
```

CFM MD Configuration Mode

This mode groups all the commands pertaining to CFM MD. The command prompt shown at this level is:

```
Switch(config)# cfm domain aaa
Switch(config-cfm-dmn)#
```

CFM MEP Configuration Mode

This mode groups all the commands pertaining to CFM MEP. The command prompt shown at this level is:

```
Switch(config-cfm-dmn-svc)# mep 1
Switch(config-cfm-dmn-svc-mep)#
```

DHCP Pool Configuration Mode

This mode groups all the commands pertaining to DHCP Pool. The command prompt shown at this level is:

```
Switch(config)# ip dhcp pool aaa
Switch(config-dhcp-pool)#
```

ERPS Mode

This mode groups all the commands pertaining to ERPS. The command prompt shown at this level is:

```
Switch(config)# erps 1
Switch(config-erps)#
```

Global Configuration Mode

This mode permits the operator to make modifications to the running configuration. General setup commands are grouped in this mode.
From the Global Configuration mode, the operator can enter the System Configuration mode, the Physical Port Configuration mode, the Interface Configuration mode, or the Protocol Specific modes specified below. The command prompt at this level is:

```
Switch# configure terminal
Switch(config)#
```

IPMC Profile Mode

This mode groups all the commands pertaining to IPMC Profile. The command prompt shown at this level is:

```
Switch(config)# ipmc profile aaa
Switch(config-ipmc-profile)#
```

JSON Notification Host Mode

This mode groups all the commands pertaining to JSON Notification Host. The command prompt shown at this level is:

```
Switch(config)# json notification host aaa
Switch(config-json-noti-host)#
```

Keychain Mode

This mode groups all the commands pertaining to Keychain. The command prompt shown at this level is:

```
Switch(config)# key chain aaa
Switch(config-keychain)#
```

Line Configuration Mode

This mode groups all the commands pertaining to Line. The command prompt shown at this level is:

```
Switch(config)# line 1
Switch(config-line)#
```

LLAG Mode

This mode groups all the commands pertaining to LLAG. The command prompt shown at this level is:

```
Switch(config)# interface llag 1
Switch(config-llag)#
```

Loopback Interface Mode

This mode groups all the commands pertaining to loopback Interface. The command prompt shown at this level is:

```
Switch(config)# interface loopback 1
Switch(config-if-lo)#
```

MRP Configuration Mode

This mode groups all the commands pertaining to MRP. The command prompt shown at this level is:

```
Switch(config)# media-redundancy 1
Switch(config-media-redundancy)#
```

OSPF Router Mode

This mode groups all the commands pertaining to OSPF Router. The command prompt shown at this level is:

```
Switch(config)# router ospf
Switch(config-router)#
```

OSPFv3 Router Mode

This mode groups all the commands pertaining to OSPFv3 Router. The command prompt shown at this level is:

```
Switch(config)# router ospf6
Switch(config-router)#
```

Port Configuration Mode

This mode groups all the commands pertaining to Port List. The command prompt shown at this level is:

```
Switch(config)# interface GigabitEthernet 1/2
Switch(config-if)#
```

QoS Egress Map Mode

This mode groups all the commands pertaining to QoS Egress Map. The command prompt shown at this level is:

```
Switch(config)# qos map egress 1
Switch(config-qos-map-egress)#
```

QoS Ingress Map Mode

This mode groups all the commands pertaining to QoS Ingress Map. The command prompt shown at this level is:

```
Switch(config)# qos map ingress 1
Switch(config-qos-map-ingress)#
```

RedBox Mode

This mode groups all the commands pertaining to RedBox. The command prompt shown at this level is:

```
Switch(config)# redbox 1
Switch(config-redbox)#
```

RIP Router Mode

This mode groups all the commands pertaining to RIP Router. The command prompt shown at this level is:

```
Switch(config)# router rip
Switch(config-router)#
```

SNMP Server Host Mode

This mode groups all the commands pertaining to SNMP Server Host. The command prompt shown at this level is:

```
Switch(config)# snmp-server host aaa
Switch(config-snmps-host)#
```

STP Aggregation Mode

This mode groups all the commands pertaining to STP Aggregation. The command prompt shown at this level is:

```
Switch(config)# spanning-tree aggregation
Switch(config-stp-aggr)#
```

STREAM Configuration Mode

This mode groups all commands related to Stream configuration. The command prompt displayed at this level is:

```
Switch(config)# stream 1
Switch(config-stream)#
```

STREAM-COLLECTION Configuration Mode

This mode groups all commands related to Stream- collection configuration. The command prompt displayed at this level is:

```
Switch(config)# stream-collection 1
Switch(config-stream-collection)#
```

TSN FRER configuration Mode

This mode groups all the commands configuration to TSN FRER. The command prompt shown at this level is:

```
Switch(config)# tsn frer 1
Switch(config-frer)#
```

TSN PSFP Flow Meter Mode

This mode groups all the commands pertaining to TSN PSFP Flow Meter. The command prompt shown at this level is:

```
Switch(config)# tsn flow meter 1
Switch(config-flow-meter)#
```

TSN PSFP Stream Filter Mode

This mode groups all the commands pertaining to TSN PSFP Stream Filte. The command prompt shown at this level is:

```
Switch(config)# tsn stream filter 1
Switch(config-stream-filter)#
```

TSN PSFP Stream Gate Mode

This mode groups all the commands pertaining to TSN PSFP Stream Gate. The command prompt shown at this level is:

```
Switch(config)# tsn stream gate 1
Switch(config-stream-gate)#
```

Uart Mode

This mode groups all the commands pertaining to Uart. The command prompt shown at this level is:

```
Switch(config)# uart 1
Switch(config-uart)#
```

User EXEC Mode

To have access to the full suite of commands, the operator must enter the User EXEC Mode. Users authenticated by login are able to enter the User EXEC Mode. From User EXEC Mode, the operator can issue any Exec command, enter the VLAN mode or enter the Global Configuration mode. The command prompt shown at this level is:

```
Switch#
```

VLAN Configuration Mode

This mode groups all the commands pertaining to VLANs. The command prompt shown at this level is:

```
Switch(config)# vlan 1
Switch(config-vlan)#
```

VLAN Interface Mode

This mode groups all the commands pertaining to VLAN Interface. The command prompt shown at this level is:

```
Switch(config)# interface vlan 1
Switch(config-if-vlan)#
```

"No" Form of a Command

"No" is a specific form of an existing command and does not represent a new or distinct command. Only the configuration commands are available in the "no" form. The behavior and the support details of the "no" form is captured as part of the mapping sheets.

Support for "No" Form

Almost every configuration command has a "no" form. In general, use the no form to reverse the action of a command or reset a value back to the default. For example, the `no shutdown` configuration command reverses the shutdown of an interface. Use the command without the keyword "no" to re-enable a disabled feature or to enable a feature that is disabled by default.

CLI Commands Introduction

This chapter provides detailed explanation of the Switching commands. The commands are divided into six functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. Every configuration command can be viewed in the show running-config or show dataplug-config.

System Information and Statistics

show running-config

This command displays the current settings for different protocols supported on the switch. With the optional keyword all-defaults, the default values of all configured protocols are displayed. Without the optional keyword, only the configured status of all interfaces is displayed.

Format

```
show running-config [ all-defaults ]
```

Mode

```
User EXEC Mode
```

show dataplug-config

This command displays all configurations saved in the dataplug on the switch.

Format

```
show dataplug-config
```

Mode

```
User EXEC Mode
```

1. Access Management

Access Management primarily handles the security and availability of resources within an organization. It controls the access of users and systems to networks, data, and applications.

1.1. access management

This chapter allows you to configure access management. The maximum number of entries is 16. If the type of the application matches any one of the access management entries, it allows access to the switch.

1.1.1. access management

This command is used to enable the access management.

Default

```
disable
```

Format

```
access management
```

Mode

```
Global Configuration Mode
```

■ no access management

This command is used to disable the access management.

Format

```
no access management
```

Mode

```
Global Configuration Mode
```

1.1.2. access management (ipv4 / ipv6)

This command is used to set the access management entry for IPv4 or IPv6 address. *<1-16>* represents ID of access management entry. *<1-4095>* represents the VLAN ID for the access management entry. *<ipv4_ucast>* represents IPv4 unicast address. *<ipv6_ucast>* represents IPv6 unicast address.

Default

```
none
```

Format

```
access management <1-16> <1-4095> <ipv4_ucast> [ to <end_addr> ] { [ http ] [ https ] [ snmp ] [ telnet ] [ ssh ] | all }
access management <1-16> <1-4095> <ipv6_ucast> [ to <end_addr> ] { [ http ] [ https ] [ snmp ] [ telnet ] [ ssh ] | all }
```

Mode

```
Global Configuration Mode
```

■ no access management (ipv4 / ipv6)

This command is used to delete the specific access management entry. *<1-16>* represents ID of access management entry.

Format

```
no access management <1-16>
```

Mode

```
Global Configuration Mode
```

1.2. show

1.2.1. show access management

This command is use without keywords to display the access management configuration, or use the statistics keyword to display statistics, or use the *<1~16>* keyword to display the specific access management entry. *<1-16>* represents ID of access management entry.

Format

```
show access management [ statistics | <1-16> ]
```

Mode

```
User EXEC Mode
```

1.3. clear

1.3.1. clear access management statistics

This command is used to clear the statistics maintained by access management.

Format

```
clear access management statistics
```

Mode

```
User EXEC Mode
```

2. ACL

ACL (Access Control List) can filter packets through the switch port configuration matching rules and packet processing operation. This can effectively prevent unauthorized users from accessing the network, and it also can control the traffic and save network resources.

2.1. access-list

This option allows you to configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

2.1.1. access-list policy

This command is used to configure the access-list policy value. *<0-255>* represents the value of policy ID specified in decimal or hexadecimal.

Default

```
0
```

Format

```
access-list policy <0-255>
```

Mode

```
Port Configuration Mode
```

■ no access-list policy

This command is used to restore access-list policy ID to 0.

Format

```
no access-list policy
```

Mode

```
Port Configuration Mode
```

2.1.2. access-list action

This command is used to configure access-list action.

Default

```
permit
```

Format

```
access-list action { permit | deny }
```

Mode

```
Port Configuration Mode
```

2.1.3. access-list rate-limiter

This command is used to enable the access-list rate-limiter ID. *<1-16>* represents rate limiter ID.

Default

```
disable
```

Format

```
access-list rate-limiter <1-16>
```

Mode

```
Port Configuration Mode
```

no access-list rate-limiter

This command is used to disable the access-list rate-limiter.

Format

```
no access-list rate-limiter
```

Mode

```
Port Configuration Mode
```

2.1.4. access-list redirect

This command is used to configure the access-list redirect interface. <*port_type_id*> represents the interface to configure. <*port_type_list*> represents the port list.

Default

```
disable
```

Format

```
access-list redirect interface { <port_type_id> | <port_type_list> }
```

Mode

```
Port Configuration Mode
```

no access-list redirect

This command is used to disable the access-list redirect.

Format

```
no access-list redirect
```

Mode

```
Port Configuration Mode
```

2.1.5. access-list mirror

This command is used to enable access-list mirror.

Default

```
disable
```

Format

```
access-list mirror
```

Mode

```
Port Configuration Mode
```

no access-list mirror

This command is used to disable access-list mirror.

Format

```
no access-list mirror
```

Mode

```
Port Configuration Mode
```

2.1.6. access-list logging

This command is used to enable access-list logging.
Note: The logging feature only works when the packet length is less than 1518 (without VLAN tags) and the System Log memory size and logging rate is limited.

Default

```
disable
```

Format

```
access-list logging
```

Mode

```
Port Configuration Mode
```

■ no access-list logging

This command is used to disable access-list logging.

Format

```
no access-list logging
```

Mode

```
Port Configuration Mode
```

2.1.7. access-list shutdown

This command is used to enable access-list shutdown. The shutdown feature only works when the packet length is less than 1518 (without VLAN tags).

Default

```
disable
```

Format

```
access-list shutdown
```

Mode

```
Port Configuration Mode
```

■ no access-list shutdown

This command is used to disable access-list shutdown.

Format

```
no access-list shutdown
```

Mode

```
Port Configuration Mode
```

2.1.8. access-list port-state

This command is used to enable access-list port-state. Re-enable shutdown port that was shutdown by access-list module.

Default

```
enable
```

Format

```
access-list port-state
```

Mode

```
Port Configuration Mode
```

no access-list port-state

This command is used to disable access-list port-state.

Format

```
no access-list port-state
```

Mode

```
Port Configuration Mode
```

2.1.9. access-list rate-limiter

This command is used to configure access-list rate-limiter. *<1~16>* represents rate limiter ID. *<0-131071>* represents packets per second. *<0-500000>* represents 10 packets per second. *<1-32767>* represents 100 packets per second. *<0-400000>* represents 25k bits per second. *<0-10000>* represents 100k bits per second.

Default

```
1 pps
```

Format

```
access-list rate-limiter [ <1-16> ] { pps <0-131071> | 10pps <0-500000> | 100pps
<1-32767> | 25kbps <0-400000> | 100kbps <0-10000> }
```

Mode

```
Global Configuration Mode
```

no access-list rate-limiter

This command is used to restore the default access-list rate-limiter setting. *<1~16>* represents rate limiter ID.

Format

```
no access-list rate-limiter [ <1~16> ]
```

Mode

```
Global Configuration Mode
```

2.1.10. access-list ace

This command is used to configure the access-list ace. The command without the update keyword will create or overwrite an existing ACE, any unspecified parameter will be set to its default value. Use the update keyword to update an existing ACE and only specified parameter are modified. The ACE must be ordered by an appropriate sequence, the received frame will only be hit on the first matched ACE. Use the next or last keyword to adjust the ACE's sequence order. *<ace_id>* represents ACE ID. “direction” the direction of data packets received or sent. “ports” ports. “frame-type” Frame type.“action” Access list action. “logging” Logging frame information.“mirror” Mirror frame to destination mirror port.“rate-limiter” Rate limiter.“redirect” Redirect frame to specific port.“shutdown” Shutdown incoming port.“tag” tag.“tag-priority” tag-priority.“vid” VID field.“dmac-type” The type of destination MAC address.“priority” The ACE with higher priority is found first.

Default

```
none
```

Format

```
access-list ace [ update ] <ace_id> [ direction ] [ ports ] [ policy ] [ frametype ]
[ action ] [ logging ] [ mirror ] [ rate-limiter ] [ redirect ] [ shutdown ] [ tag ]
[ tag-priority ] [ vid ] [ dmac-type ] [ priority ]
```

Mode

```
Global Configuration Mode
```

no access-list ace

This command is used to delete ACE entry. *<ace_id>* represents ACE ID.

Format

```
no access-list ace <ace_id>
```

Mode

```
Global Configuration Mode
```

2.2. default access-list

2.2.1. default access-list rate-limiter

This command is used to restore the default setting of access-list rate-limiter. *<1~16>* represents rate limiter ID.

Format

```
default access-list rate-limiter [ <1~16> ]
```

Mode

```
Global Configuration Mode
```

2.3. show

2.3.1. show access-list interface

This command is used to show access-list interface for the access-list interface configuration.

Format

```
show access-list [ interface [ <port_type_list> ] ]
```

Mode

```
User EXEC Mode
```

2.3.2. show access-list rate-limiter

This command is used to display access-list rate-limiter configuration. *<1~16>* represents rate limiter ID.

Format

```
show access-list rate-limiter [ <1~16> ]
```

Mode

```
User EXEC Mode
```

2.3.3. show access-list ace statistics

This command is used to display access-list ace configuration. *<1~256>* represents ACE ID.

Format

```
show access-list ace statistics [ <1~256> ]
```

Mode

```
User EXEC Mode
```

2.3.4. show access-list ace-status

This command is used without keywords to display the access-list ace status for all access-list users, or particularly the access-list user for the access-list ace status. Use conflicts keyword to display the access-list ace that doesn't apply on the hardware. In other word, it means the specific ACE is not applied to the hardware due to hardware limitations.

Format

```
show access-list ace-status [ static ] [ link-oam ] [ loop-protect ] [ dhcp ]
[ dhcp6-snooping ] [ ptp ] [ upnp ] [ arp-inspection ] [ cfm ] [ aps ] [ erps ] [ mrp ]
[ ip-source-guard ] [ ipv6-source-guard ] [ ip-mgmt ] [ ip ] [ conflicts ] [ switch
<switch_list> ]
```

Mode

```
User EXEC Mode
```

2.4. clear

2.4.1. clear access-list ace statistics

This command is used to clear the statistics maintained by access-list, including access-list interface statistics and ACE's statistics.

Format

```
clear access-list ace statistics
```

Mode

```
User EXEC Mode
```

3. Aggregation (aggr)

Aggregation enables the use of multiple ports in parallel to increase the link speed beyond the limits of a single port, and to increase the redundancy for higher availability. If the system has 6 ports, the maximum aggregation group is 3 (6 divided by 2).

3.1. aggregation

The aggregation feature uses the following hash factor to calculate the destination port for the frame. The default hash mode is source and destination MAC addresses.

3.1.1. aggregation mode

This command is used to set the hash mode for aggregation port selection. The supported modes are source MAC address, destination MAC address, source and destination MAC addresses, source IP address, destination IP address, and source and destination IP addresses.

Default

```
source and destination MAC addresses
```

Format

```
aggregation mode { [ smac ] | [ dmac ] | [ both-mac ] | [ sip ] | [ dip ] | [ both-ip ] }
```

Mode

```
Global Configuration Mode
```

■ no aggregation mode

This command is used to reset aggregation mode.

Format

```
no aggregation mode
```

Mode

```
Global Configuration Mode
```

3.1.2. aggregation group

This command is used to add a port to an aggregation group. Use mode keyword to configure aggregation mode to LACP (Active), Static or LACP (Passive). <*uint*> represents the aggregation group id.

Default

```
none
```

Format

```
aggregation group <uint> mode { active | on | passive }
```

Mode

```
Port Configuration Mode
```

■ no aggregation group

This command is used to delete a port from an aggregation group. <*uint*> represents the aggregation group id.

Format

```
no aggregation group <uint>
```

Mode

```
Port Configuration Mode
```

3.2. show

3.2.1. show aggregation

This command is use without keywords to show aggregations. Use mode keyword to show aggregation mode.

Format

```
show aggregation [ mode ]
```

Mode

```
User EXEC Mode
```

4. APS

The APS module implements the protocol and linear protection switching mechanisms for point-to-point VLAN-based ETH SNC in Ethernet transport networks. Automatic Protection Switching is defined by the ITU G.8031 standard.

4.1. working-mep

4.1.1. working-mep domain service mep-id

This command is use to specify which MEP provides signal-fail for the working port.

Default

```
none
```

Format

```
working-mep domain <kword1-15> service <kword1-15> mep-id <1-8191>
```

Mode

```
APS Mode
```

no working-mep

This command is use to remove working-mep (not really useful, but can be output from 'show running-config all-defaults').

Format

```
no working-mep
```

Mode

```
APS Mode
```

4.2. protect-mep

4.2.1. protect-mep domain service mep-id

This command is use to specify which MEP provides signal-fail for the protect port.

Default

```
none
```

Format

```
protect-mep domain <kword1-15> service <kword1-15> mep-id <1-8191>
```

Mode

```
APS Mode
```

no protect-mep

This command is use to remove protect-mep (not really useful, but can be output from 'show running-config all-defaults').

Format

```
no protect-mep
```

Mode

```
APS Mode
```

4.3. working

4.3.1. working interface

This command is use to assign an interface to the working port.

Default

none

Format

working interface *<port_type_id>*

Mode

APS Mode

4.3.2. working sf-trigger service mep-id

This command is use to choose whether the working port's interface link state or a MEP installed on working's interface is used as signal-fail trigger.

Default

none

Format

working sf-trigger { link | { mep domain *<kword1-15>* service *<kword1-15>* mep-id *<1-8191>* } }

Mode

APS Mode

4.4. protect

4.4.1. protect interface

This command is use to assign an interface to the protect port.

Default

none

Format

protect interface *<port_type_id>*

Mode

APS Mode

4.4.2. protect sf-trigger service mep-id

This command is use to choose whether the protect port's interface link state or a MEP installed on protect's interface is used as signal-fail trigger.

Default

none

Format

protect sf-trigger { link | { mep domain *<kword1-15>* service *<kword1-15>* mep-id *<1-8191>* } }

Mode

APS Mode

4.5. smac

4.5.1. smac

This command is use to set a source MAC address to be used in L-APS PDUs. Default to use interface's.

Default

```
none
```

Format

```
smac <mac_ucast>
```

Mode

```
APS Mode
```

no smac

This command is use to set source MAC address used in L-APS PDUs to protect port's interface's MAC address.

Format

```
no smac
```

Mode

```
APS Mode
```

4.6. vlan

4.6.1. vlan

This command is use to insert or don't insert a VLAN tag with this VLAN ID in L-APS PDUs.

Default

```
none
```

Format

```
vlan { untagged | <vlan_id> [ pcp <0-7> ] }
```

Mode

```
APS Mode
```

4.7. level

4.7.1. level

This command is use to set the MD/MEG level used in L-APS PDUs. Default is 0.

Default

```
none
```

Format

```
level <0-7>
```

Mode

```
APS Mode
```

4.8. mode

4.8.1. mode

This command is use to specify the APS architecture and direction.

Default

```
none
```

Format

```
mode { 1-for-1 | bidirectional-1-plus-1 | unidirectional-1-plus-1 [ tx-aps ] }
```

Mode

```
APS Mode
```

4.9. revertive

4.9.1. revertive

This command is use to traffic switches back to the working port after the wait-to-restore timer has expired after the defect conditions causing a switch have cleared.

Default

```
none
```

Format

```
revertive
```

Mode

```
APS Mode
```

■ no revertive

This command is use to traffic is allowed to remain on the protect port after the switch has cleared the protected port.

Format

```
no revertive
```

Mode

```
APS Mode
```

4.10. wait-to-restore

4.10.1. wait-to-restore

This command is use to only used in revertive mode. Indicates the number of seconds after a defect has cleared until operation is switched back to the working port.

Default

```
none
```

Format

```
wait-to-restore <uint>
```

Mode

```
APS Mode
```

4.11. hold-off-time

4.11.1. hold-off-time

This command is use to when a new (or more severe) defect occurs, the hold-off timer will be started and the event will be reported after the timer expires.

Default

```
none
```

Format

```
hold-off-time <uint>
```

Mode

```
APS Mode
```

4.12. admin-state

4.12.1. admin-state

This command is use to enable or disable this APS instance.

Default

```
none
```

Format

```
admin-state { enable | disable }
```

Mode

```
APS Mode
```

4.13. aps

4.13.1. aps clear

This command is use to clear a switchover (FS, MS-to-W, MS-to-P), lockout (LO), exercise (EXER) request and a WTR condition.

Default

```
none
```

Format

```
aps <uint> clear
```

Mode

```
User EXEC Mode
```

4.13.2. aps exercise

This command is use to exercise an APS instance. Use 'aps <inst> clear' to clear the request.

Default

none

Format

aps *<uint>* exercise

Mode

User EXEC Mode

4.13.3. aps freeze

This command is use to freezes the state of the APS instance. While in this mode, additional near-end commands, condition changes, and received APS information are ignored. Use 'no aps <inst> freeze' to get out of this mode.

Default

none

Format

aps *<uint>* freeze

Mode

User EXEC Mode

4.13.4. aps lockout

This command is use to lock the protection instance of APS. Use 'aps <inst> clear' to clear the request.

Default

none

Format

aps *<uint>* lockout

Mode

User EXEC Mode

4.13.5. aps switch

This command is use to requests to switch from the working path to the protection path, or vice versa. Use 'aps <inst> clear' to clear the request.

Default

none

Format

aps *<uint>* switch

Mode

User EXEC Mode

4.14. show

4.14.1. show aps

This command is use to show APS PDU Rx and Tx counters.

Default

none

Format

show aps [*<range_list>*] [statistics]

Mode

User EXEC Mode

4.15. clear

4.15.1. clear aps statistics

This command is use to clear the counters of one or more APS instances.

Default

none

Format

clear aps [*<range_list>*] statistics

Mode

User EXEC Mode

5. ARP Inspection

ARP (Address Resolution Protocol) is a TCP/IP protocol that used to convert an IP address into a physical address. When a host sends messages, the ARP requests containing with destination IP address will be broadcasted to all the hosts on the network. It the returned messages will be received to determine the physical address of the destination; After receiving the messages, the IP address and physical address will be stored into the local ARP cache and kept for a certain time. It only need to refer to ARP cache to conserve resources when next request happened.
ARP Inspection is a secure feature. Several types of attacks can be launched on Layer 2 networks connected to hosts or devices through ARP cache 'poisoning'. This function is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

5.1. ip arp inspection

Note: only if the global configuration and port configuration are enabled, the ARP inspection will be enabled on the specified port. When disable "check VLAN", the ARP inspection log type indicates the port setting. When enable "check VLAN", ARP inspection log type indicates the VLAN setting.

5.1.1. ip arp inspection

This command is used to globally enable ARP inspection.

Default

```
disable
```

Format

```
ip arp inspection
```

Mode

```
Global Configuration Mode
```

no ip arp inspection

This command is used to globally disable ARP inspection.

Format

```
no ip arp inspection
```

Mode

```
Global Configuration Mode
```

5.1.2. ip arp inspection translate

This command is used to translate all dynamic entries in ARP inspection table to static entries.

Format

```
ip arp inspection translate
```

Mode

```
Global Configuration Mode
```

5.1.3. ip arp inspection trust

This command is used to enable a port as trusted for ARP inspection purposes.

Default

```
disable
```

Format

```
ip arp inspection trust
```

Mode

```
Port Configuration Mode
```

■ no ip arp inspection trust

This command is used to disable a port as trusted for ARP inspection purposes.

Format

```
no ip arp inspection trust
```

Mode

```
Port Configuration Mode
```

5.1.4. ip arp inspection check-vlan

This command is used to enable a port as VLAN mode for ARP inspection purposes.

Default

```
disable
```

Format

```
ip arp inspection check-vlan
```

Mode

```
Port Configuration Mode
```

■ no ip arp inspection check-vlan

This command is used to disable a port as VLAN mode for ARP inspection purposes.

Format

```
no ip arp inspection check-vlan
```

Mode

```
Port Configuration Mode
```

5.1.5. ip arp inspection logging

This command is used to configure a port as some logging mode for ARP inspection purposes.

Default

```
none
```

Format

```
ip arp inspection logging { deny | permit | all }
```

Mode

```
Port Configuration Mode
```

■ no ip arp inspection logging

This command is used to configure a port as logging none.

Format

```
no ip arp inspection logging
```

Mode

```
Port Configuration Mode
```

5.1.6. ip arp inspection vlan

This command is used to enable ARP detection on the specified VLAN. <*vlan_list*> represents ARP inspection VLAN list.

Default

disable

Format

ip arp inspection vlan <*vlan_list*>

Mode

Global Configuration Mode

■ no ip arp inspection vlan

This command is used to disable ARP detection on the specified VLAN. <*vlan_list*> represents ARP inspection VLAN list.

Format

no ip arp inspection vlan <*vlan_list*>

Mode

Global Configuration Mode

5.1.7. ip arp inspection vlan logging

This command is used to configure ARP inspection VLAN logging mode. <*vlan_list*> represents ARP inspection VLAN list.

Default

none

Format

ip arp inspection vlan <*vlan_list*> logging { deny | permit | all }

Mode

Global Configuration Mode

■ no ip arp inspection vlan logging

This command is used to configure ARP inspection VLAN logging mode to none. <*vlan_list*> represents ARP inspection VLAN list.

Format

no ip arp inspection vlan <*vlan_list*> logging

Mode

Global Configuration Mode

5.1.8. ip arp inspection entry

This command is used to configure static table of ARP inspection. <*port_type_id*> represents ARP inspection entry interface configuration. <*vlan_id*> represents VLAN id to configure. <*mac_ucast*> represents MAC address to configure. <*ipv4_ucast*> represents ipv4 address to configure.

Default

none

Format

ip arp inspection entry interface <*port_type_id*> <*vlan_id*> <*mac_ucast*> <*ipv4_ucast*>

Mode

Global Configuration Mode

no ip arp inspection entry

This command is used to delete static table of ARP inspection. *<port_type_id>* represents ARP inspection entry interface. *<vlan_id>* represents VLAN id. *<mac_ucast>* represents MAC address. *<ipv4_ucast>* represents ipv4 address.

Format

```
no ip arp inspection entry interface <port_type_id> <vlan_id> <mac_ucast> <ipv4_ucast>
```

Mode

```
Global Configuration Mode
```

5.1.9. ip arp inspection translate

This command is used to translate dynamic ARP inspection entry interface configuration to static entries. *<port_type_id>* represents ARP inspection entry interface. *<vlan_id>* represents VLAN id. *<mac_ucast>* represents MAC address. *<ipv4_ucast>* represents ipv4 address.

Format

```
ip arp inspection translate [ interface <port_type_id> <vlan_id> <mac_ucast> <ipv4_ucast> ]
```

Mode

```
Global Configuration Mode
```

5.2. show

5.2.1. show ip arp inspection interface

This command is used to display configured ARP inspection in per port. *<port_type_list>* represents port list.

Format

```
show ip arp inspection interface <port_type_list>
```

Mode

```
User EXEC Mode
```

5.2.2. show ip arp inspection vlan

This command is used to display configured ARP inspection in pre vlan. *<vlan_list>* represents ARP inspection VLAN list.

Format

```
show ip arp inspection vlan <vlan_list>
```

Mode

```
User EXEC Mode
```

5.2.3. show ip arp inspection entry

This command is used to display ARP inspection entry interface configuration. dhcp-snooping represents learn from DHCP snooping, static represents set from static entries, *<port_type_list>* represents ARP inspection entry interface.

Format

```
show ip arp inspection entry [ dhcp-snooping | static ] [ interface <port_type_list> ]
```

Mode

```
User EXEC Mode
```

6. Auth

Auth (Authentication) is the process of verifying a user's identity in computer systems, network services, or applications. Its primary purpose is to ensure that users or systems attempting to access resources can demonstrate that their claimed identities are genuine and valid.

6.1. radius-server

RADIUS (Remote Authentication Dial In User Service) is defined by RFC2865 and RFC2866. It is currently the most widely used AAA protocol. AAA is a management framework, so that it can be implemented using multiple protocols. RADIUS is a C/S structure protocol, the first client of which is NAS (Net Access Server). Any computer running RADIUS client software can be a RADIUS client. With flexible mechanisms, RADIUS authentication protocol can utilize PAP, CHAP or Unix login authentication and other methods. RADIUS is an extensible protocol, all the work it carried out is based on the vector of Attribute-Length-Value. RADIUS also supports the expansion of the vendor-specific properties.
RADIUS is a networking protocol that provides centralized authentication, authorization, and accounting management for users or computers to connect to and use network services.

6.1.1. radius-server timeout

This command is used to configure the global RADIUS timeout value, to wait for a reply from a RADIUS server before retransmitting the request. *<1-1000>* represents wait time in seconds.

Default

```
5
```

Format

```
radius-server timeout <1-1000>
```

Mode

```
Global Configuration Mode
```

■ no radius-server timeout

This command is used to reset the global RADIUS timeout value to default.

Format

```
no radius-server timeout
```

Mode

```
Global Configuration Mode
```

6.1.2. radius-server retransmit

This command is used to configure the global RADIUS retransmit value, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead. *<1-1000>* represents number of retries for a transaction.

Default

```
3
```

Format

```
radius-server retransmit <1-1000>
```

Mode

```
Global Configuration Mode
```

no radius-server retransmit

This command is used to reset the global RADIUS retransmit value to default.

Format

```
no radius-server retransmit
```

Mode

```
Global Configuration Mode
```

6.1.3. radius-server deadtime

This command is used to configure the global RADIUS deadtime value, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. *<1-1440>* represents time in minutes.

Default

```
0
```

Format

```
radius-server deadtime <1-1440>
```

Mode

```
Global Configuration Mode
```

no radius-server deadtime

This command is used to reset the global RADIUS deadtime value to default.

Format

```
no radius-server deadtime
```

Mode

```
Global Configuration Mode
```

6.1.4. radius-server key

This command is used to configure the global RADIUS key. *<line1-63>* represents the UNENCRYPTED (Plain Text) secret key. Notice that you have no chance to get the Plain Text secret key after this command. The system will always display the ENCRYPTED password. *<word96-224>* represents the ENCRYPTED (hidden) secret key. Notice the ENCRYPTED secret key will be decoded by system internally. You cannot directly use it as same as the Plain Text and it is not human-readable text normally.

Default

```
none
```

Format

```
radius-server key { [ unencrypted ] <line1-63> | encrypted <word96-224> }
```

Mode

```
Global Configuration Mode
```

no radius-server key

This command is used to remove the global RADIUS key.

Format

```
no radius-server key
```

Mode

```
Global Configuration Mode
```

6.1.5. radius-server attribute 4

This command is used to configure the NAS IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. *<ipv4_ucast>* represents the IPv4 address.

Default

```
none
```

Format

```
radius-server attribute 4 <ipv4_ucast>
```

Mode

```
Global Configuration Mode
```

■ no radius-server attribute 4

This command is used to remove the NAS IPv4 address.

Format

```
no radius-server attribute 4
```

Mode

```
Global Configuration Mode
```

6.1.6. radius-server attribute 95

This command is used to configure the NAS IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. *<ipv6_ucast>* represents the IPv6 address.

Default

```
none
```

Format

```
radius-server attribute 95 <ipv6_ucast>
```

Mode

```
Global Configuration Mode
```

■ no radius-server attribute 95

This command is used to remove the NAS IPv6 address.

Format

```
no radius-server attribute 95
```

Mode

```
Global Configuration Mode
```

6.1.7. radius-server attribute 32

This command is used to configure the NAS identifier to be used as attribute 32 in RADIUS Access-Request packets. *<line1-253>* represents NAS identifier.

Default

```
none
```

Format

```
radius-server attribute 32 <line1-253>
```

Mode

```
Global Configuration Mode
```

no radius-server attribute 32

This command is used to remove the NAS identifier.

Format

```
no radius-server attribute 32
```

Mode

```
Global Configuration Mode
```

6.1.8. radius-server host

This command is used to add a new RADIUS host. <*word1-255*> represents hostname or IPv4/IPv6 address. <*0-65535*> from auth-port represents UDP port number or 0 to disable authentication. <*0-65535*> from acct-port represents UDP port number or 0 to disable accounting. <*1-1000*> from timeout represents wait time in seconds. <*1-1000*> from retransmit represents number of retries for a transaction. <*line1-63*> represents the UNENCRYPTED (Plain Text) secret key. Notice that you have no chance to get the Plain Text secret key after this command. The system will always display the ENCRYPTED password. <*word96-224*> represents the ENCRYPTED (hidden) secret key. Notice the ENCRYPTED secret key will be decoded by system internally. You cannot directly use it as same as the Plain Text and it is not human-readable text normally.

Default

```
none
```

Format

```
radius-server host <word1-255> [ auth-port <0-65535> ] [ acct-port <0-65535> ]
[ timeout <1-1000> ] [ retransmit <1-1000> ] [ key { [ unencrypted ] <line1-63> | encrypted
<word96-224> } ]
```

Mode

```
Global Configuration Mode
```

no radius-server host

This command is used to delete an existing RADIUS host. <*word1-255*> represents hostname or IPv4/IPv6 address. <*0-65535*> from auth-port represents UDP port number or 0 to disable authentication. <*0-65535*> from acct-port represents UDP port number or 0 to disable accounting.

Format

```
no radius-server host <word1-255> [ auth-port <0-65535> ] [ acct-port <0-65535> ]
```

Mode

```
Global Configuration Mode
```

6.2. tacacs-server

TACACS+ (Terminal Access Controller Access Control System) is similar with IDsentrie's RADIUS protocol. However, TACACS+ utilizes TCP protocol, while RADIUS utilizes UDP. Their vital role is 3A (Authentication, Authorization and Accounting). TACACS + provides a multi-protocol support, for example, IP and AppleTalk. General operations are all encrypted packets to provide more secure communications.

6.2.1. tacacs-server timeout

This command is used to configure the global TACACS+ timeout value, to wait for a reply from a TACACS+ server before it is considered to be dead. <*1-1000*> represents wait time in seconds.

Default

```
5
```

Format

```
tacacs-server timeout <1-1000>
```

Mode

```
Global Configuration Mode
```

no tacacs-server timeout

This command is used to reset the global TACACS+ timeout value to default.

Format

```
no tacacs-server timeout
```

Mode

```
Global Configuration Mode
```

6.2.2. tacacs-server deadtime

This command is used to configure the global TACACS+ deadtime value, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. *<1-1440>* represents time in minutes.

Default

```
0
```

Format

```
tacacs-server deadtime <1-1440>
```

Mode

```
Global Configuration Mode
```

no tacacs-server deadtime

This command is used to reset the global TACACS+ deadtime value to default.

Format

```
no tacacs-server deadtime
```

Mode

```
Global Configuration Mode
```

6.2.3. tacacs-server key

This command is used to configure the global TACACS+ key. *<line1-63>* represents the UNENCRYPTED (Plain Text) secret key. Notice that you have no chance to get the Plain Text secret key after this command. The system will always display the ENCRYPTED password. *<word96-224>* represents the ENCRYPTED (hidden) secret key. Notice the ENCRYPTED secret key will be decoded by system internally. You cannot directly use it as same as the Plain Text and it is not human-readable text normally.

Default

```
none
```

Format

```
tacacs-server key { [ unencrypted ] <line1-63> | encrypted <word96-224> }
```

Mode

```
Global Configuration Mode
```

no tacacs-server key

This command is used to remove the global TACACS+ key.

Format

```
no tacacs-server key
```

Mode

```
Global Configuration Mode
```

6.2.4. tacacs-server host

This command is used to add a new TACACS+ host. *<word1-255>* represents hostname or IPv4/IPv6 address. *<0-65535>* represents TCP port for TACACS+ server. *<1-1000>* represents wait time in seconds. *<line1-63>* represents the UNENCRYPTED (Plain Text) secret key. Notice that you have no chance to get the Plain Text secret key after this command. The system will always display the ENCRYPTED password. *<word96-224>* represents the ENCRYPTED (hidden) secret key. Notice the ENCRYPTED secret key will be decoded by system internally. You cannot directly use it as same as the Plain Text and it is not human-readable text normally.

Default

none

Format

tacacs-server host *<word1-255>* [port *<0-65535>*] [timeout *<1-1000>*] [key { [unencrypted] *<line1-63>* | encrypted *<word96-224>* }]

Mode

Global Configuration Mode

no tacacs-server host

This command is used to delete an existing TACACS+ host. *<word1-255>* represents hostname or IPv4/IPv6 address. *<0-65535>* represents TCP port for TACACS+ server.

Format

no tacacs-server host *<word1-255>* [port *<0-65535>*]

Mode

Global Configuration Mode

6.3. aaa

6.3.1. aaa authentication

This command is used to configure the authentication method. You can configure authentication through four methods: console, telnet, http, and ssh. *<local>* represents using the local user database on the switch for authentication. *<radius>* represents using a remote RADIUS server for authentication. *<tacacs>* represents remote TACACS+ server authentication.

Default

none

Format

aaa authentication login { console | telnet | ssh | http } { [local | radius | tacacs] }

Mode

Global Configuration Mode

no aaa authentication

This command is used to delete authentication methods.

Format

no aaa authentication login { console | telnet | ssh | http }

Mode

Global Configuration Mode

6.3.2. aaa authorization

This command is used to configure the command authorization method. You can configure command authorization through console, telnet, and ssh. The command authorization section allows you to limit the CLI commands available to a user. *<tacacs>* represents using remote TACACS+ server(s) for command authorization. If all remote servers are offline, the user is granted access to CLI commands according to his privilege level. *<0-15>* represents the authorization command level. *<config-commands>* represents also authorize configuration commands.

Default

```
none
```

Format

```
aaa authorization { console | telnet | ssh } tacacs commands <0-15> [ config-commands ]
```

Mode

```
Global Configuration Mode
```

no aaa authorization

This command is used to remove command authorization methods.

Format

```
no aaa authorization { console | telnet | ssh }
```

Mode

```
Global Configuration Mode
```

6.3.3. aaa accounting

This command is used to configure accounting method. You can configure accounting through three methods: console, telnet, and ssh. *<tacacs>* represents using a remote TACACS+ server for accounting. *<0-15>* represents the accounting command level. *<exec>* represents enable the exec (login) of accounting.

Default

```
none
```

Format

```
aaa accounting { console | telnet | ssh } tacacs { [ commands <0-15> ] [ exec ] }
```

Mode

```
Global Configuration Mode
```

no aaa accounting

This command is used to delete a accounting method.

Format

```
no aaa accounting { console | telnet | ssh }
```

Mode

```
Global Configuration Mode
```

6.4. show

6.4.1. show tacacs-server

This command is used to view the current TACACS+ configuration.

Format

```
show tacacs-server
```

Mode

```
User EXEC Mode
```

6.4.2. show radius-server

This command is used to view the current RADIUS configuration and statistics.

Format

```
show radius-server [ statistics ]
```

Mode

```
User EXEC Mode
```

7. BYPASS

7.1. bypass

7.1.1. bypass off group interface interface

Configure bypass group members and status.<*uint*> restricted to 1 and 2 represents the bypass group IDs.

{ normal | enhance } indicates the selectable modes, where normal is the standard mode and enhance is the enhanced mode.<*port_type_id*> designates the port type to be assigned to the bypass group.

Default

```
none
```

Format

```
bypass off group <uint> { normal | enhance } interface <port_type_id> interface <port_type_id>
```

Mode

```
Global Configuration Mode
```

■ bypass on group

This command is used to delete ports in the BYPASS group.

Format

```
bypass on group <id>
```

Mode

```
Global Configuration Mode
```

7.1.2. bypass monitor

This command is used to set the CPU threshold and monitoring duration, as well as the memory threshold and monitoring duration, for the BYPASS group.

Default

```
bypass monitor cpu threshold 90 cycle-time 10
bypass monitor memory threshold 90 cycle-time 10
```

Format

```
bypass monitor { cpu | memory } threshold <50-100> cycle-time <5-50>
```

Mode

```
Global Configuration Mode
```

■ no bypass monitor

This command is used to disable the CPU threshold and monitoring duration, as well as the memory threshold and monitoring duration, for the BYPASS group.

Format

```
no bypass monitor { cpu | memory }
```

Mode

```
Global Configuration Mode
```

7.1.3. bypass detection time

Configure the initial startup detection time for the bypass configuration.<*3-60*> specifies the initial startup time (unit: minutes) for the bypass configuration.

Default

```
10
```

Format

```
bypass detection time <3-60>
```

Mode

```
Global Configuration Mode
```

■ no bypass detection time

This command is used to restore the first startup detection time of the bypass device to its default value.

Format

```
no bypass detection time
```

Mode

```
Global Configuration Mode
```

7.2. show

7.2.1. show bypass

This command is used to display the port information of the BYPASS group.

Format

```
show bypass
```

Mode

```
User EXEC Mode
```

8. CFM

CFM (Connectivity Fault Management) is typically used for managing fault detection, isolation, and reporting in Ethernet networks. It is part of the IEEE 802.1ag standard and is also described in the ITU-T Y.1731 standard. CFM provides a set of mechanisms to monitor and maintain the performance of end-to-end Ethernet service layers.

8.1. cfm

8.1.1. cfm sender-id-tlv

This command is used to enables sending ID TLV.

Default

none

Format

```
cfm sender-id-tlv { disable | chassis | management | chassis-management }
```

Parameter

- Disable

  Exclude Sender ID TLV from PDUs (default).

- Chassis

  Enable Sender ID TLV and send Chassis ID (MAC Address).

- Management

  Enable Sender ID TLV and send Management address (IPv4 Address).

- Chassis-management

  Enable Sender ID TLV and send both Chassis ID (MAC Address) and Management Address (IPv4 Address).

Mode

Global Configuration Mode

8.1.2. cfm port-status-tlv

This command is used to include or exclude Port Status TLV in CCM PDUs (may be overridden in domain and service).

Default

none

Format

```
cfm port-status-tlv { disable | enable }
```

Mode

Global Configuration Mode

8.1.3. cfm interface-status-tlv

This command is used to include or exclude Interface Status TLV in CCM PDUs (may be overridden in domain and service).

Default

none

Format

cfm interface-status-tlv { disable | enable }

Mode

Global Configuration Mode

8.1.4. cfm organization-specific-tlv

This command is used to include or exclude Organization-Specific TLV in PDUs (may be overridden in domain and service).

Default

none

Format

cfm organization-specific-tlv { disable | enable oui *<oui>* subtype *<0-255>* value *<string63>* }

Parameter

- disable

  Exclude Organization-Specific TLV from PDUs (default).

- Enable

  Include Organization-Specific TLV in PDUs.

- oui

  Specify the OUI to use, the OUI on form XX-XX-XX.

- subtype

  Choose the subtype to put in CFM PDUs.

- value

  Choose the value to put in the organization-specific TLV's value field.

Mode

Global Configuration Mode

8.1.5. cfm domain

This command is used to maintenance domain (MD).

Default

none

Format

cfm domain *<kword1-15>*

Mode

Global Configuration Mode

Example

```
(config)# cfm domain dmn
(config-cfm-dmn)#
```

no cfm domain

This command is used to delete a maintenance domain and all its services and all the services' MEPs.

Format

```
no cfm domain { <kword1-15> | all }
```

Mode

```
Global Configuration Mode
```

8.2. format

8.2.1. format (CFM MD)

This command is used to change format of this domain.

Default

```
none
```

Format

```
format { none | string <string1-43> }
```

Mode

```
CFM MD Configuration Mode
```

Example

```
(config-cfm-dmn)# format none
```

8.2.2. format (CFM MA)

This command is used to configure the format used in MAID/MEGID for this service (maintenance association).

Default

```
none
```

Format

```
format { string <string1-45> | integer <0-65535> | primary-vid | icc <string13-13>
| icc-cc <string15-15> }
```

Mode

```
CFM MA Configuration Mode
```

Example

```
(config-cfm-dmn-svc)# format string "2"
```

8.3. sender-id-tlv

8.3.1. sender-id-tlv (CFM MD)

This command enables or disables sender ID TLV format to be used in PDUs in this domain (may be over ridden in service).

Default

```
disable
```

Format

```
sender-id-tlv { disable | chassis | management | chassis-management | defer }
```

Parameter

- `disable`

  Exclude Sender ID TLV from PDUs in this domain.

- `chassis`

  Enable Sender ID TLV and send Chassis ID (MAC Address).

- `management`

  Enable Sender ID TLV and send Management address (IPv4 Address).

- `chassis-management`

  Enable Sender ID TLV and send both Chassis ID (MAC Address) and Management ID.

- `defer`

  Let the global CFM configuration determine whether to send Sender ID TLVs on PDUs in this domain (default).

Mode

```
CFM MD Configuration Mode
```

8.3.2. sender-id-tlv (CFM MA)

This command is used to default Sender ID TLV format to be used in PDUs in MEPs running in this service.

Default

```
none
```

Format

```
sender-id-tlv { disable | chassis | management | chassis-management | defer }
```

Mode

```
CFM MA Configuration Mode
```

8.4. port-status-tlv

8.4.1. port-status-tlv (CFM MD)

This command Include or exclude Port Status TLV in PDUs included in this domain or let higher level determine (may be overridden in service).

Default

```
enable
```

Format

```
port-status-tlv { disable | enable | defer }
```

Parameter

- `disable`

  `Exclude Port Status TLV from PDUs in this domain.`

- `enable`

  `Include Port Status TLV in PDUs in this domain.`

- `defer`

  `Let the global CFM configuration determine whether to include Port Status TLV in PDUs in this domain (default).`

Mode

```
CFM MD Configuration Mode
```

8.4.2. port-status-tlv (CFM MA)

This command include or exclude Port Status TLV in PDUs for MEPs included in this service or let domain determine.

Default

```
none
```

Format

```
port-status-tlv { disable | enable | defer }
```

Mode

```
CFM MA Configuration Mode
```

8.5. interface-status-tlv

8.5.1. interface-status-tlv (CFM MD)

This command Include or exclude Interface Status TLV in PDUs included in this domain or let higher level determine (may be overridden in service).

Default

```
disable
```

Format

```
interface-status-tlv { disable | enable | defer }
```

Parameter

- `disable`

  `Exclude Interface Status TLV from PDUs in this domain.`

- `enable`

  `Include Interface Status TLV in PDUs domain.`

- `defer`

  `Let the global CFM configuration determine whether to include Interface Status TLV in PDUs in this domain (default).`

Mode

```
CFM MD Configuration Mode
```

8.5.2. interface-status-tlv (CFM MA)

This command include or exclude Interface Status TLV in PDUs included in MEPs running in this service or let domain determine.

Default

```
none
```

Format

```
interface-status-tlv { disable | enable | defer }
```

Mode

```
CFM MA Configuration Mode
```

8.6. organization-specific-tlv

8.6.1. organization-specific-tlv (CFM MD)

This command Include or exclude Organization-Specific TLV in PDUs included in this MD or let higher level determine (may be overridden in service).

Default

```
disable
```

Format

```
organization-specific-tlv { disable | defer }
```

Parameter

- `disable`

  `Exclude Organization-Specific TLV from PDUs in this domain.`

- `defer`

  `Let the global CFM configuration determine whether to include an Organization-Specific TLV in PDUs in this domain (default).`

Mode

```
CFM MD Configuration Mode
```

8.6.2. organization-specific-tlv (CFM MA)

This command include or exclude Organization-Specific TLV in PDUs on MEPs running in this service or let the domain determine.

Default

```
none
```

Format

```
organization-specific-tlv { disable | defer }
```

Mode

```
CFM MA Configuration Mode
```

8.7. level

8.7.1. level

This command is used to specify the level (MEG-level) for this domain.

Default

```
0
```

Format

```
level <0-7>
```

Mode

```
CFM MD Configuration Mode
```

Example

```
(config-cfm-dmn)# level 7
```

8.8. service

8.8.1. service

This command is used to this command create or modify a service (Maintenance Association/MA).

Default

```
none
```

Format

```
service <kword1-15>
```

Mode

```
CFM MD Configuration Mode
```

Example

```
(config-cfm-dmn)# service aaa
(config-cfm-dmn-svc)#
```

no service

This command is used to this command delete a service/maintenance association and all its MEPs.

Format

```
no service { <kword1-15> | all }
```

Mode

```
CFM MD Configuration Mode
```

8.9. type

8.9.1. type

This command is used to specify whether MEPs created in this service are port or VLAN MEPs.

Default

```
port
```

Format

```
type { port | vlan <1-4095> }
```

Mode

```
CFM MA Configuration Mode
```

Example

```
(config-cfm-dmn-svc)#type port
```

8.10. continuity-check interval

8.10.1. continuity-check interval

This command specify the CCM interval for all MEPs in this service (maintenance association).

Default

```
none
```

Format

```
continuity-check interval { 3.3ms | 10ms | 100ms | 1s | 10s | 1min | 10min }
```

Mode

```
CFM MA Configuration Mode
```

8.11. mep

8.11.1. mep

This command create or modify a Maintenance association EndPoint (MEP).

Default

```
none
```

Format

```
mep <1-8191>
```

Mode

```
CFM MA Configuration Mode
```

Example

```
(config-cfm-dmn-svc)# mep 1
(config-cfm-dmn-svc-mep)#
```

no mep

This command delete a particular MEP or all MEPs in this service.

Format

```
no mep { <1-8191> | all }
```

Mode

```
CFM MA Configuration Mode
```

8.12. direction

8.12.1. direction

This command sets whether this MEP is an Up- or a Down-MEP.

Default

```
none
```

Format

```
direction { up | down }
```

Mode

```
CFM MEP Configuration Mode
```

Example

```
(config-cfm-dmn-svc-mep)# direction up
```

8.13. interface

8.13.1. interface

This command is used to choose which port this MEP is installed on.

Default

```
none
```

Format

```
interface <port_type_id>
```

Mode

```
CFM MEP Configuration Mode
```

8.14. vlan

8.14.1. vlan

This command is used to specify the VLAN for this MEP (default is that it inherits it from its service/maintenance association).

Default

```
none
```

Format

```
vlan { inherit | <1-4095> }
```

Mode

```
CFM MEP Configuration Mode
```

8.15. pcp

8.15.1. pcp

This command is used to specify the VLAN for this MEP (default is that it inherits it from its service/maintenance association).

Default

```
none
```

Format

```
pcp <0-7>
```

Mode

```
CFM MEP Configuration Mode
```

8.16. smac

8.16.1. smac

This command is used to select a unicast MAC address to be used as source MAC address in PDUs for this MEP.

Default

```
0
```

Format

```
smac <mac_ucast>
```

Mode

```
CFM MEP Configuration Mode
```

no smac

This command is used to delete smac as the default value to be used.

Format

```
no smac
```

Mode

```
CFM MEP Configuration Mode
```

8.17. continuity-check

8.17.1. continuity-check

This command is used to enable generation of continuity-check messages (CCMs).

Default

```
disable
```

Format

```
continuity-check
```

Mode

```
CFM MEP Configuration Mode
```

Example

```
(config-cfm-dmn-svc-mep)# continuity-check
```

no continuity-check

This command is used to disable generation of continuity-check messages (CCMs).

Format

```
no continuity-check
```

Mode

```
CFM MEP Configuration Mode
```

Example

```
(config-cfm-dmn-svc-mep)# no continuity-check
```

8.18. remote mep

8.18.1. remote mep

This command is used to specify the Remote MEPs that this MEP is expected to receive CCM PDUs from.

Default

```
none
```

Format

```
remote mep <1-8191>
```

Mode

```
CFM MEP Configuration Mode
```

Example

```
(config-cfm-dmn-svc-mep)# remote mep 2024
```

no remote mep

This command is used to specify the Remote MEPs to no longer monitor on this MEP.

Default

```
none
```

Format

```
no remote mep { <1-8191> | all }
```

Mode

```
CFM MEP Configuration Mode
```

Example

```
(config-cfm-dmn-svc-mep)# no remote mep 2024
```

8.19. alarm-level

8.19.1. alarm-level

This command is used to if a defect is detected with a priority higher than this level, a fault alarm notification will be generated.

Default

```
2
```

Format

```
alarm-level <1-6>
```

Mode

```
CFM MEP Configuration Mode
```

Example

```
(config-cfm-dmn-svc-mep)# alarm-level 4
```

8.20. alarm-time-absent

8.20.1. alarm-time-absent

This command is used to the time in milliseconds that defects must be absent before a fault alarm notification is reset.

Default

```
10000
```

Format

```
alarm-time-absent <2500-10000>
```

Mode

```
CFM MEP Configuration Mode
```

Example

```
(config-cfm-dmn-svc-mep)# alarm-time-absent 10000
```

8.21. alarm-time-present

8.21.1. alarm-time-present

This command is used to the time in milliseconds that defects must be present before a fault alarm notification is issued.

Default

```
2500
```

Format

```
alarm-time-present <2500-10000>
```

Mode

```
CFM MEP Configuration Mode
```

Example

```
(config-cfm-dmn-svc-mep)# alarm-time-present 2500
```

8.22. admin-state

8.22.1. admin-state

This command is used to enable or disable this MEP.

Default

```
disable
```

Format

```
admin-state { enable | disable }
```

Mode

```
CFM MA Configuration Mode
```

Example

```
(config-cfm-dmn-svc-mep)# admin-state enable
```

8.23. show

8.23.1. show cfm services

This command is used to this command is used to show CFM services.

Format

```
show cfm services [ domain <kword1-15> ] [ service <kword1-15> ] [ details ]
```

Mode

```
User EXEC Mode
```

8.23.2. show cfm domains

This command is used to show CFM domains.

Format

```
show cfm domains [ domain <kword1-15> ] [ details ]
```

Mode

```
User EXEC Mode
```

8.23.3. show cfm meps

This command is used to show MEPs.

Format

```
show cfm meps [ domain <kword1-15> ] [ service <kword1-15> ] [ mep-id <1-8191> ]
[ details ]
```

Mode

```
User EXEC Mode
```

8.23.4. show cfm errors

This command is used to show errors.

Format

```
show cfm errors
```

Mode

```
User EXEC Mode
```

8.24. clear

8.24.1. clear cfm meps

This command is used to clear MEP statistics.

Format

```
clear cfm meps [ domain <kword1-15> ] [ service <kword1-15> ] [ mep-id <1-8191> ]
statistics
```

Mode

```
User EXEC Mode
```

9. Clock

The Clock is used to maintain consistency of the internal time within a device and provide timestamps for data flows and operational logs passing through the switch. This function is crucial for security audits, troubleshooting, log recording, and time-stamping of messages within the network.

9.1. clock

9.1.1. clock timezone

This command is used to configure the time zone.

Default

```
none
```

Format

```
clock timezone <word16> <-23-23> [ <0-59> [ <0-9> ] ]
```

Mode

```
Global Configuration Mode
```

■ no clock timezone

This command disables the time zone.

Format

```
no clock timezone
```

Mode

```
Global Configuration Mode
```

9.1.2. time set

This command is used to configure the current system time.

Default

```
System acquisition
```

Format

```
time set <date> <time>
```

Mode

```
Global Configuration Mode
```

9.1.3. clock summer-time recurring

This command is used to configure the recurring summer time.

Default

```
none
```

Format

```
clock summer-time <word16> recurring [ <1-5> <1-7> <1-12> <hhmm> <1-5> <1-7> <1-12>
<hhmm> [ <1-1439> ] ]
```

Mode

```
Global Configuration Mode
```

9.1.4. clock summer-time nonrecurring

This command is used to configure the absolute summer time.

Default

none

Format

clock summer-time nonrecurring [*<1-12> <1-31> <2000-2097> <hhmm> <1-12> <1-31> <2000-2097> <hhmm>* [*<1-1439>*]]

Mode

Global Configuration Mode

■ no clock summer-time

This command is used to set the daylight saving time as the default.

Default

none

Format

no clock summer-time

Mode

Global Configuration Mode

9.2. show

9.2.1. show clock detail

This command displays the detailed information about the time configuration.

Format

show clock detail

Mode

User EXEC Mode

10. Copper Cable Test

Copper Cable Test refers to a series of tests used to assess the quality of cable lines and the status of their connections. These tests are commonly carried out using professional testing tools or through test systems integrated within network devices, such as switches. The tests include wire continuity, wire pair verification, length measurement, and cross-talk testing, among others.

10.1. cable-test

1.1.1.cable-test

This command is used to request the port of the virtual physical layer cable diagnosis to diagnose the cable. [{ interface *<port_type_list>* }] is an optional parameter, which only displays only results for a specific physical port.

Default

none

Format

cable-test [{ interface *<port_type_list>* }]

Mode

User EXEC Mode

10.2. show

1.1.2.show interface cable-test

This command displays the diagnostic results for the virtual physical layer cable located at the interface *<port_type_list>* port.

Default

none

Format

show interface *<port_type_list>* cable-test

Mode

User EXEC Mode

11. DDMI

DDMI (Digital Diagnostics Monitoring Interface). It provides an enhanced digital diagnostic monitoring interface for optical transceivers which allows real time access to device operating parameters.

11.1. ddmi

11.1.1. ddmi

This command is used to enable DDMI.

Default

```
disable
```

Format

```
ddmi
```

Mode

```
Global Configuration Mode
```

■ no ddmi

This command is used to disable DDMI.

Format

```
no ddmi
```

Mode

```
Global Configuration Mode
```

11.2. show

11.2.1. show ddmi brief

This command is used to display the ddmi summary information.

Format

```
show ddmi brief
```

Mode

```
User EXEC Mode
```

11.2.2. show ddmi

This command is used to display DDMI configuration.

Format

```
show ddmi
```

Mode

```
User EXEC Mode
```

11.2.3. show interface

This command is used to display DDMI detailed information. *<port_type_list>* represents DDMI port.

Format

```
show interface <port_type_list> transceiver
```

Mode

```
User EXEC Mode
```

12. DHCP Server

DHCP (Dynamic Host Configuration Protocol) is used to assign IP address, mask and the default gateway. DHCP can also automatically configure other options for the terminal device such as DNS server, domain name (like apple.com), time zones, NTP servers and other configurations. Some manufacturers use their own development of third-party software and their own configuration information to achieve the automatic configuration of the terminal equipment by DHCP protocol.

12.1. ip

Enable/disable the DHCP server in global mode or VLAN mode.

12.1.1. ip dhcp server

This command enable DHCP server per system and per VLAN.

Default

```
none
```

Format

```
ip dhcp server
```

Mode

```
Global Configuration Mode/VLAN Interface Mode
```

no ip dhcp server

This command disable DHCP server per system and per VLAN.

Format

```
no ip dhcp server
```

Mode

```
Global Configuration Mode/VLAN Interface Mode
```

12.1.2. ip dhcp excluded-address

This command configures excluded IP addresses. DHCP server will not allocate these excluded IP addresses to DHCP client.

Default

```
none
```

Format

```
ip dhcp excluded-address <ipv4_addr> [ <ipv4_addr> ]
```

Mode

```
Global Configuration Mode
```

12.1.3. ip dhcp pool

This command is used to configuring DHCP address pool.

Default

```
none
```

Format

```
ip dhcp pool <pool_name>
```

Mode

```
DHCP Pool Configuration Mode
```

no ip dhcp pool

This command is used to clear the configured DHCP address pool.

Format

```
no ip dhcp pool <word32>
```

Mode

```
Global Configuration Mode
```

12.2. host

12.2.1. host

This command is used to host-mode address pool IP range.

Default

```
none
```

Format

```
host <ipv4_ucast> <ipv4_netmask>
```

Mode

```
DHCP Pool Configuration Mode
```

no host

This command is used to clear the host-mode address pool IP range.

Format

```
no host
```

Mode

```
DHCP Pool Configuration Mode
```

12.3. network

12.3.1. network

This command is used to network mode address pool IP range.

Default

```
none
```

Format

```
network <ipv4_ucast> <ipv4_netmask>
```

Mode

```
DHCP Pool Configuration Mode
```

no network

This command is used to clear the network mode address pool IP range.

Format

```
no network
```

Mode

```
DHCP Pool Configuration Mode
```

12.4. lease

12.4.1. lease

This command is used to configure the lease time.

Default

```
none
```

Format

```
lease { <0-365> [ <0-23> [ <uint> ] ] | infinite }
```

Mode

```
DHCP Pool Configuration Mode
```

no lease

This command is used to clear the configured the lease time.

Format

```
no lease
```

Mode

```
DHCP Pool Configuration Mode
```

12.5. broadcast

12.5.1. broadcast

This command is used to configure the DHCP server and its clients to interact with each other on this IP, with the default value of 255.255.255.255.

Default

```
none
```

Format

```
broadcast <ipv4_addr>
```

Mode

```
DHCP Pool Configuration Mode
```

no broadcast

This command is used to set the broadcast of this node to be the default value.

Format

```
no broadcast
```

Mode

```
DHCP Pool Configuration Mode
```

12.6. dns-server

12.6.1. dns-server

This command is used to configure the DNS server of the DHCP client.

Default

none

Format

dns-server *<ipv4_ucast>* [*<ipv4_ucast>* [*<ipv4_ucast>* [*<ipv4_ucast>*]]]

Mode

DHCP Pool Configuration Mode

■ no dns-server

This command is used to configure the DNS server of the DHCP client to default.

Format

no dns-server

Mode

DHCP Pool Configuration Mode

12.7. default-router

12.7.1. default-router

This command is used to configure the default router of the DHCP client.

Default

none

Format

default-router *<ipv4_ucast>* [*<ipv4_ucast>* [*<ipv4_ucast>* [*<ipv4_ucast>*]]]

Mode

DHCP Pool Configuration Mode

■ no default-router

This command is used to configure the default router of the DHCP client to default.

Format

no default-router

Mode

DHCP Pool Configuration Mode

12.8. ntp-server

12.8.1. ntp-server

This command is used to configure the NTP server of the DHCP client.

Default

none

Format

ntp-server *<ipv4_ucast>* [*<ipv4_ucast>* [*<ipv4_ucast>* [*<ipv4_ucast>*]]]

Mode

DHCP Pool Configuration Mode

■ no ntp-server

This command is used to clear the configure the NTP server of the DHCP client.

Format

no ntp-server

Mode

DHCP Pool Configuration Mode

12.9. domain-name

12.9.1. domain-name

This command is used to set Domain name.

Default

none

Format

domain-name *<word32>*

Mode

DHCP Pool Configuration Mode

■ no domain-name

This command is used to clear the Domain name.

Format

no domain-name

Mode

DHCP Pool Configuration Mode

12.10. hardware-address

12.10.1. hardware-address

This command is used to set Client hardware address.

Default

```
none
```

Format

```
hardware-address <mac_ucast>
```

Mode

```
DHCP Pool Configuration Mode
```

■ no hardware-address

This command is used to clear the Client hardware address.

Format

```
no hardware-address
```

Mode

```
DHCP Pool Configuration Mode
```

12.11. netbios-name-server

12.11.1. netbios-name-server

This command is used to set NetBIOS (WINS) name servers.

Default

```
none
```

Format

```
netbios-name-server <ipv4_ucast> [ <ipv4_ucast> [ <ipv4_ucast> [ <ipv4_ucast> ] ] ]
```

Mode

```
DHCP Pool Configuration Mode
```

■ no netbios-name-server

This command is used to clear the NetBIOS (WINS) name servers.

Format

```
no netbios-name-server
```

Mode

```
DHCP Pool Configuration Mode
```

12.12. netbios-node-type

12.12.1. netbios-node-type

This command is used to set NetBIOS node type. b-node represents broadcast node, h-node represents hybrid node, m-node represents mixed node, p-node represents peer-to-peer node.

Default

```
none
```

Format

```
netbios-node-type { b-node | h-node | m-node | p-node }
```

Mode

```
DHCP Pool Configuration Mode
```

■ no netbios-node-type

This command is used to clear the NetBIOS node type.

Format

```
no netbios-node-type
```

Mode

```
DHCP Pool Configuration Mode
```

12.13. nis-domain-name

12.13.1. nis-domain-name

This command is used to set NIS domain name.

Default

```
none
```

Format

```
nis-domain-name <word32>
```

Mode

```
DHCP Pool Configuration Mode
```

■ no nis-domain-name

This command is used to clear the NIS domain name.

Format

```
no nis-domain-name
```

Mode

```
DHCP Pool Configuration Mode
```

12.14. nis-server

12.14.1. nis-server

This command is used to set Network information servers.

Default

```
none
```

Format

```
nis-server <ipv4_ucast> [ <ipv4_ucast> [ <ipv4_ucast> [ <ipv4_ucast> ] ] ]
```

Mode

```
DHCP Pool Configuration Mode
```

■ no nis-server

This command is used to clear the Network information servers.

Format

```
no nis-server
```

Mode

```
DHCP Pool Configuration Mode
```

12.15. netbios-scope

12.15.1. netbios-scope

This command is used to set NetBIOS scope.

Default

```
none
```

Format

```
netbios-scope <line32>
```

Mode

```
DHCP Pool Configuration Mode
```

■ no netbios-scope

This command is used to clear the NetBIOS scope.

Format

```
no netbios-scope
```

Mode

```
DHCP Pool Configuration Mode
```

12.16. client-identifier

12.16.1. client-identifier

This command is used to set Client identifier. fqdn represents it’s obsolete and use 'name' instead, name represents client identifier other than hardware type, *<line128>* represents 128 characters, mac-address represents MAC address type of client identifier, *<mac_addr>* represents MAC address of client.

Default

```
none
```

Format

```
client-identifier { { fqdn | name } <line64> | mac-address <mac_addr> }
```

Mode

```
DHCP Pool Configuration Mode
```

no client-identifier

This command is used to clear the Client identifier.

Format

```
no client-identifier
```

Mode

```
DHCP Pool Configuration Mode
```

12.17. client-name

12.17.1. client-name

This command is used to set Client host name.

Default

```
none
```

Format

```
client-name <word32>
```

Mode

```
DHCP Pool Configuration Mode
```

no client-name

This command is used to clear the Client host name.

Format

```
no client-name
```

Mode

```
DHCP Pool Configuration Mode
```

12.18. address

12.18.1. address

This command is used to offer fixed IP address to client on specific interface, overruling client ID.

Default

none

Format

address *<ipv4_addr>* interface *<port_type_id>*

Mode

DHCP Pool Configuration Mode

■ no address

This command is used to remove fixed address entry from pool.

Format

no address *<ipv4_addr>*

Mode

DHCP Pool Configuration Mode

12.19. vendor

12.19.1. vendor class-identifier

This command is used to vendor configuration.

Default

none

Format

vendor class-identifier *<string64>* specific-info *<word66>*

Mode

DHCP Pool Configuration Mode

■ no vendor class-identifier

This command is used to clear the vendor configuration.

Format

no vendor class-identifier *<string64>*

Mode

DHCP Pool Configuration Mode

12.20. reserved-only

12.20.1. reserved-only

This command is used to restrict addresses offered to clients to those specified by 'address' commands.

Default

```
none
```

Format

```
reserved-only
```

Mode

```
DHCP Pool Configuration Mode
```

■ no reserved-only

This command is used to remove fixed address entry.

Format

```
no reserved-only
```

Mode

```
DHCP Pool Configuration Mode
```

12.21. show

12.21.1. show ip dhcp server binding

This command is used to display the attribute status information of IP DHCP server binding. State represents state of binding, included allocated state, committed state, and expired state. Type represents type of binding, included automatic binding, manual binding for a specific host, and expired binding that is aged out.

Default

```
none
```

Format

```
show ip dhcp server binding [ state { allocated | committed | expired } ] [ type
{ automatic | manual | expired } ]
```

Mode

```
User EXEC Mode
```

12.21.2. show ip dhcp server binding (IPv4)

This command is used to display the IP information of IP DHCP server binding.

Default

```
none
```

Format

```
show ip dhcp server binding <ipv4_ucast>
```

Mode

```
User EXEC Mode
```

12.21.3. show ip dhcp server

This command is used to displays the configured IP DHCP Server.

Default

none

Format

show ip dhcp server

Mode

User EXEC Mode

12.21.4. show ip dhcp server statistics

This command is used to displays the configured IP DHCP Server statistics.

Default

none

Format

show ip dhcp server statistics

Mode

User EXEC Mode

12.21.5. show ip dhcp pool

This command is used to display one or more IP DHCP pool instances.

Default

none

Format

show ip dhcp pool [*<word32>*]

Mode

User EXEC Mode

12.21.6. show ip dhcp excluded-address

This command is used to display one or more IP DHCP excluded address.

Default

none

Format

show ip dhcp excluded-address

Mode

User EXEC Mode

12.22. clear

12.22.1. clear ip dhcp server binding

This command is used to clear the IP of the configured IP DHCP Server binding.

Default

```
none
```

Format

```
clear ip dhcp server binding <ipv4_ucast>
```

Mode

```
User EXEC Mode
```

12.22.2. clear ip dhcp server binding type

This command is used to clears the configured IP DHCP server binding IP by type.

Default

```
none
```

Format

```
clear ip dhcp server binding type { automatic | manual | expired }
```

Mode

```
User EXEC Mode
```

12.22.3. clear ip dhcp server statistics

This command is used to clear the counted IP DHCP server statistics.

Default

```
none
```

Format

```
clear ip dhcp server statistics
```

Mode

```
User EXEC Mode
```

13. DHCP Snooping

DHCP snooping is used to block untrusted intruders on switch ports when an intruder attempts to intervene between legitimate DHCP clients and servers by injecting fake DHCP reply packets.

13.1. ip

13.1.1. ip dhcp snooping

This command is used to enable global DHCP monitor mode.

Default

```
none
```

Format

```
ip dhcp snooping
```

Mode

```
Global Configuration Mode
```

13.1.2. ip dhcp snooping trust

This command to configure trusted interface.

Default

```
none
```

Format

```
ip dhcp snooping trust
```

Mode

```
Port Configuration Mode
```

13.2. show

13.2.1. show ip dhcp snooping table

This command to display the IP assigned information that is obtained from DHCP server except for local VLAN interface IP addresses.

Default

```
none
```

Format

```
show ip dhcp snooping table
```

Mode

```
User EXEC Mode
```

13.2.2. show ip dhcp snooping

This command is used to use the show ip dhcp snooping command without keywords to display the DHCP snooping configuration, or particularly the ip dhcp snooping statistics for the interface, or use the statistics keyword to display statistics.

Default

none

Format

show ip dhcp snooping [statistics] [interface *<port_type_list>*]

Mode

User EXEC Mode

13.3. clear

13.3.1. clear ip dhcp snooping statistics

This command to clear the statistics maintained by IP DHCP snooping, or particularly the IP DHCP snooping statistics for the interface.

Default

none

Format

clear ip dhcp snooping statistics [interface *<port_type_list>*]

Mode

User EXEC Mode

14. DHCP Relay

A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain. It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of GIADDR field to determine the assigned subnet. For such condition, please make sure the switch configuration of VLAN interface IP address and PVID(Port VLAN ID) correctly.

14.1. ip

14.1.1. ip dhcp relay

This command to enable the DHCP relay server. Use the no form of this command to disable the DHCP relay server.

Default

```
none
```

Format

```
ip dhcp relay
```

Mode

```
Global Configuration Mode
```

14.1.2. ip helper-address

This command to configure the host address of DHCP relay server.

Default

```
none
```

Format

```
ip helper-address <ipv4_ucast>
```

Mode

```
Global Configuration Mode
```

no ip helper-address

This command to clear the host address of DHCP relay server.

Format

```
no ip helper-address
```

Mode

```
Global Configuration Mode
```

14.1.3. ip dhcp relay information option

This command to enable the DHCP relay information option. Use the no form of this command to disable the DHCP relay information option.

Default

```
none
```

Format

```
ip dhcp relay information option
```

Mode

```
Global Configuration Mode
```

14.1.4. ip dhcp relay information policy

This command to configure the DHCP relay information policy. "drop" represents drop the package when receive a DHCP message that already contains relay information. "keep" represents keep the original relay information when receive a DHCP message that already contains it. "replace" represents Replace the original relay information when receive a DHCP message that already contains it.

Default

```
none
```

Format

```
ip dhcp relay information policy { drop | keep | replace }
```

Mode

```
Global Configuration Mode
```

no ip dhcp relay information policy

This command to restore the default DHCP relay information policy.

Format

```
no ip dhcp relay information policy
```

Mode

```
Global Configuration Mode
```

14.2. show

14.2.1. show ip dhcp relay

This command without keywords to display the DHCP relay configuration, or use the statistics keyword to display statistics.

Default

```
none
```

Format

```
show ip dhcp relay [ statistics ]
```

Mode

```
User EXEC Mode
```

14.3. clear

14.3.1. clear ip dhcp relay statistics

This command to clear the statistics maintained by IP DHCP relay.

Default

```
none
```

Format

```
clear ip dhcp relay statistics
```

Mode

```
User EXEC Mode
```

15. DHCPv6 Snooping

The IPv6 Dynamic Host Configuration Protocol (DHCPv6) is designed for IPv6 addressing schemes, assigning IPv6 addresses/prefixes and other network configuration parameters to hosts.

15.1. Ipv6 dhcp snooping

15.1.1. ipv6 dhcp snooping

This command to globally disable DHCP snooping.

Default

```
none
```

Format

```
ipv6 dhcp snooping
```

Mode

```
Global Configuration Mode
```

15.1.2. ipv6 dhcp snooping nh-unknown

This command to control how packets with unknown IPv6 extension headers are treated. "drop" packets with unknown IPv6 extension headers. "allow" packets with unknown IPv6 extension headers.

Default

```
none
```

Format

```
ipv6 dhcp snooping nh-unknown { drop | allow }
```

Mode

```
Global Configuration Mode
```

15.1.3. ipv6 dhcp snooping trust

This command to configure a port as untrusted for DHCP snooping purposes.

Default

```
none
```

Format

```
ipv6 dhcp snooping trust
```

Mode

```
Port Configuration Mode
```

15.2. show

15.2.1. show ipv6 dhcp snooping

This command to display the DHCPv6 snooping configuration.

Default

none

Format

show ipv6 dhcp snooping [interface *<port_type_list>*]

Mode

User EXEC Mode

15.2.2. show ipv6 dhcp snooping table

This command to show table of known DHCP clients with assigned addresses.

Default

none

Format

show ipv6 dhcp snooping table [all]

Mode

User EXEC Mode

15.2.3. show ipv6 dhcp snooping statistics

This command to display of the IPv6 DHCP snooping statistics.

Default

none

Format

show ipv6 dhcp snooping statistics [interface *<port_type_list>*] [zero-suppress]

Mode

User EXEC Mode

15.3. clear

15.3.1. clear ipv6 dhcp snooping statistics

This command to clear the IPv6 DHCP snooping statistics.

Default

none

Format

clear ipv6 dhcp snooping statistics [interface *<port_type_list>*]

Mode

User EXEC Mode

16. DHCPv6 Relay

16.1. Ipv6

16.1.1. ipv6 dhcp relay

This command is used to configure the ipv6 dhcp relay.

Default

none

Format

ipv6 dhcp relay [destination <*ipv6_ucast*>] interface vlan <*vlan_id*>

Mode

VLAN Interface Mode

no ipv6 dhcp relay

This command is used to clear the configured ipv6 dhcp relay.

Format

no ipv6 dhcp relay [{ destination <*ipv6_ucast*> interface vlan <*vlan_id*> } | { interface vlan <*vlan_id*> }]

Mode

VLAN Interface Mode

16.2. show

16.2.1. show ipv6 dhcp relay

This command is used to shows the configured ipv6 dhcp relay.

Default

none

Format

show ipv6 dhcp relay [interface vlan <*vlan_id*>]

Mode

User EXEC Mode

16.2.2. show ipv6 dhcp relay statistics

This command is used to shows the ipv6 dhcp relay statistics.

Default

none

Format

show ipv6 dhcp relay statistics [interface vlan <*vlan_id*>]

Mode

User EXEC Mode

16.3. clear

16.3.1. clear ipv6 dhcp relay statistics

This command is used to clear the ipv6 dhcp relay statistics.

Default

none

Format

clear ipv6 dhcp relay statistics [interface vlan *<vlan_id>* [interface vlan *<vlan_id>*]]

Mode

User EXEC Mode

17. DNS

DNS (Domain Name System) is used to translate domain names (such as www.example.com) into their corresponding IP addresses. This can be accomplished through a DNS client on a switch or through relevant DNS configurations.

17.1. ip dns

DNS server configuration includes IP DNS mapping switch and configuration of entries mapping domain names to IP addresses.

17.1.1. ip dns map

This command is used to enable IP DNS mapping switch.

Default

```
disable
```

Format

```
ip dns map
```

Mode

```
Global Configuration Mode
```

■ no ip dns map

This command is used to disable IP DNS mapping switch.

Format

```
no ip dns map
```

Mode

```
Global Configuration Mode
```

17.1.2. ip dns direct-map

This command is used to add the entry for mapping DNS domain names to IP addresses.

Default

```
NA
```

Format

```
ip dns direct-map <1-64> <domain_name> <ipv4_ucast>
```

Mode

```
Global Configuration Mode
```

■ no ip dns direct-map

This command is used to delete the entry for mapping DNS domain names to IP addresses.

Format

```
no ip dns direct-map <1-64> <domain_name> <ipv4_ucast>
```

Mode

```
Global Configuration Mode
```

17.2. ip name-server

17.2.1. ip name-server

This command is used to set the DNS server for resolving domain names.*<0-3>* represents preference of DNS server, default selection is 0. *<ipv4_ucast>* represents valid IPv4 unicast address, *<ipv6_ucast>* represents valid IPv6 unicast address. *<vlan_id>* represents VLAN Interface and VLAN identifier. "dhcp ipv4" represents DNS setting is derived from DHCPv4; Default selection. "dhcp ipv6" represents DNS setting is derived from DHCPv6.

Default

none

Format

ip name-server [*<0-3>*] { *<ipv4_ucast>* | { *<ipv6_ucast>* [interface vlan *<vlan_id>*] } | dhcp [ipv4 | ipv6] [interface vlan *<vlan_id>*] }

Mode

Global Configuration Mode

no ip name-server

This command is used to cancel the configuration.

Format

no ip name-server *<0-3>*

Mode

Global Configuration Mode

17.3. show

17.3.1. show ip name-server

This command is used to display the active domain name server information.

Default

none

Format

show ip name-server

Mode

User EXEC Mode

18. ERPS

ERPS (Ethernet Ring Protection Switching) is a mechanism for protection and recovery in Ethernet ring networks. Its primary function is to provide rapid fault detection and recovery to ensure continuity and reliability of data transmission within the ring network, particularly in the event of a link failure.

18.1. version

18.1.1. version

This command is used to specify whether to use G.8032v1 or G.8032v2 of the R-APS protocol.

Default

```
none
```

Format

```
version { v1 | v2 }
```

Mode

```
ERPS Mode
```

18.2. ring-type

18.2.1. ring-type

This command is used to controls whether this is a major ring or a sub-ring. Only major rings are supported if using G.8032v1. "major" represents make this a major ring, which always has two ring ports, sub-ring represents make this a non-interconnected sub-ring, which has two ring ports. "virtual-channel" represents configure this sub-ring with a R-APS virtual channel, that is, R-APS PDUs are not forwarded between ring-port links if one end is blocked. "interconnected-sub-ring" represents make this an interconnected sub-ring, which has only one ring port (port0), but connects to a major ring. "connected-ring" represents an interconnected sub-ring points to another ring with two ring ports (that is, that other ring cannot itself be an interconnected sub-ring), which receives flush notifications and may carry R-APS PDUs for the sub-ring. "propagate-topology-change" represents if a topology-change occurs on this interconnected sub-ring, the connected ring also flushes its FDB. If this keyword is specified, the connected ring will also send Flush R-APS Event PDU onto its ring ports.

Default

```
none
```

Format

```
ring-type { major | sub-ring [ virtual-channel ] | interconnected-sub-ring
{ connected-ring <uint> [ virtual-channel ] [ propagate-topology-change ] } }
```

Mode

```
ERPS Mode
```

18.3. ring-id

18.3.1. ring-id

This command is used to controls the Ring ID, which is used in the last byte of the DMAC of R-APS PDUs. Ring IDs of received R-APS PDUs must match the configured Ring ID.

Default

```
none
```

Format

```
ring-id <1-239>
```

Mode

```
ERPS Mode
```

18.4. node-id

18.4.1. node-id

This command is used to controls the Node ID used inside the R-APS PDUs to uniquely identify this node (switch). Defaults to using the switch.

Default

```
none
```

Format

```
node-id <mac_ucast>
```

Mode

```
ERPS Mode
```

no node-id

This command is used to set Node ID used inside R-APS PDUs to the switch's MAC address.

Format

```
no node-id
```

Mode

```
ERPS Mode
```

18.5. rpl

18.5.1. rpl

This command is used to controls whether this node holds the Ring Protection Link (RPL), and what role it has in that case. Use the no-form if this node doesn't hold the RPL.

Default

```
none
```

Format

```
rpl { owner | neighbor } { port0 | port1 }
```

Mode

```
ERPS Mode
```

no rpl

This command is used to configure instance to be normal ring node, that is, neither RPL owner or neighbor.

Format

```
no rpl
```

Mode

```
ERPS Mode
```

18.6. port0

18.6.1. port0 interface

This command is used to assign an interface to ring port0.

Default

```
none
```

Format

```
port0 interface <port_type_id>
```

Mode

```
ERPS Mode
```

18.6.2. port0 sf-trigger

This command is used to choose whether port0's interface link state or a MEP installed on port0's interface is used as signal-fail trigger.

Default

```
none
```

Format

```
port0 sf-trigger { link | { mep domain <kword1-15> service <kword1-15> mep-id
<1-8191> } }
```

Mode

```
ERPS Mode
```

18.6.3. port0 smac

This command is used to set a source MAC address to be used in R-APS PDUs transmitted on port0. Default to use interface's.

Default

```
none
```

Format

```
port0 smac <mac_ucast>
```

Mode

```
ERPS Mode
```

no port0 smac

This command is used to set source MAC address used in R-APS PDUs to ring port0's interface's MAC address.

Format

```
no port0 smac
```

Mode

```
ERPS Mode
```

18.7. port1

18.7.1. port1 interface

This command is used to assign an interface to ring port1.

Default

none

Format

port1 interface <*port_type_id*>

Mode

ERPS Mode

18.7.2. port1 sf-trigger

This command is used to choose whether port1's interface link state or a MEP installed on port1's interface is used as signal-fail trigger.

Default

none

Format

port1 sf-trigger { link | { mep domain <*kword1-15*> service <*kword1-15*> mep-id <*1-8191*> } }

Mode

ERPS Mode

18.7.3. port1 smac

This command is used to set a source MAC address to be used in R-APS PDUs transmitted on port1. Default to use interface's.

Default

none

Format

port1 smac <*mac_ucast*>

Mode

ERPS Mode

no port1 smac

This command is used to set source MAC address used in R-APS PDUs to ring port1's interface's MAC address.

Format

no port1 smac

Mode

ERPS Mode

18.8. control-vlan

18.8.1. control-vlan

This command is used to set the ERPS instance's control VLAN and PCP used in R-APS PDUs transmitted on both ring ports (if applicable).

Default

none

Format

control-vlan <*vlan_id*> [pcp <*0-7*>]

Mode

ERPS Mode

18.9. level

18.9.1. level

This command is used to set the MD/MEG level used in R-APS PDUs. Default is 7.

Default

none

Format

level <*0-7*>

Mode

ERPS Mode

18.10. protected-vlans

18.10.1. protected-vlans

This command is used to set the list of VLANs protected by this ERPS instance.

Default

none

Format

protected-vlans <*vlan_list*>

Mode

ERPS Mode

■ no protected-vlans

This command is used to clear the list of VLANs protected by this ERPS instance (not a valid command if instance is administratively enabled).

Format

no protected-vlans

Mode

ERPS Mode

18.11. revertive

18.11.1. revertive

This command is used to set this instance to be revertive, that is, restore to default after the wait-to-restore timer has expired.

Default

none

Format

revertive

Mode

ERPS Mode

no revertive

This command is used to set this instance to be non-revertive, that is, stay at the current protection after a signal fail. Wait-to-restore timer is not used in this mode.

Format

no revertive

Mode

ERPS Mode

18.12. wait-to-restore

18.12.1. wait-to-restore

This command is used to only used in revertive mode. Indicates the number of seconds after a defect has cleared until operation is switched back to the normal condition.

Default

none

Format

wait-to-restore <*uint*>

Mode

ERPS Mode

18.13. guard-time

18.13.1. guard-time

This command is used to the guard timer is used to prevent ring nodes from acting upon outdated R-APS PDUs upon topology changes.

Default

none

Format

guard-time <*uint*>

Mode

ERPS Mode

18.14. hold-off-time

18.14.1. hold-off-time

This command is used to when a new (or more severe) defect occurs, the hold-off timer will be started and the event will be reported after the timer expires.

Default

```
none
```

Format

```
hold-off-time <uint>
```

Mode

```
ERPS Mode
```

18.15. admin-state

18.15.1. admin-state

This command is used to enable or disable this ERPS instance.

Default

```
none
```

Format

```
admin-state { enable | disable }
```

Mode

```
ERPS Mode
```

18.16. erps

18.16.1. erps clear

This command is used to clear a switchover (FS or MS) request and a WTB/WTR condition and force reversion even if not revertive.

Default

```
none
```

Format

```
erps <uint> clear
```

Mode

```
User EXEC Mode
```

18.16.2. erps switch

This command is used to request a switchover from port0 to port1 or vice versa. Use 'erps <inst> clear' to clear the request.

Default

none

Format

erps <*uint*> switch { force | manual } { port0-to-port1 | port1-to-port0 }

Mode

User EXEC Mode

18.17. show

18.17.1. show erps

This command is used to show detailed status or statistics.

Default

none

Format

show erps [<*range_list*>] [statistics] [details]

Mode

User EXEC Mode

18.18. clear

18.18.1. clear erps

This command is used to clear the counters of one or more ERPS instances.

Default

none

Format

clear erps [<*range_list*>] statistics

Mode

User EXEC Mode

19. Firmware

Upgrade the firmware of the control switch. After the software image is uploaded, the firmware will be updated in about one minute, and the switch will reboot.

19.1. firmware

19.1.1. firmware upgrade

<*url_file*> represents Uniform Resource Locator. It is a specific character string that constitutes a reference to a resource.
Syntax: <*protocol*>: // [<*username*> [: <*password*>] @] <*host*> [:<*port*>] [/<*path*>] / <*file_name*>.
If the following special characters: space !"#$%&'()*+,/:;<=>?@[\]^`{|}~ need to be contained in the input URL string, they should be percent-encoded.
A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score (_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not allowed.

Format

```
firmware upgrade <url_file> [ save-host-key ] [ ftp-active ]
```

Mode

```
User EXEC Mode
```

19.1.2. firmware swap

This command is used to swap between Active and Backup firmware image.

Format

```
firmware swap
```

Mode

```
User EXEC Mode
```

20. FRER

FRER (Frame Replication and Elimination for Reliability) is used to enhance the reliability of data transmission in Ethernet environments. By ensuring that at least one copy of a data frame can reach its destination in the event of a network failure, FRER provides uninterrupted service. This method is particularly well-suited for Time-Sensitive Networking (TSN).

20.1. mode

20.1.1. mode

This command is used to configure mode of operation of this FRER instance. "generation" represents FRER instance generates R-Tags. "recovery" represents FRER instance operates in recovery mode.

Default

```
generation
```

Format

```
mode { generation | recovery }
```

Mode

```
TSN FRER configuration Mode
```

no mode

This command is used to default this FRER instance's mode of operation.

Format

```
no mode
```

Mode

```
TSN FRER configuration Mode
```

20.2. ingress

20.2.1. ingress stream-id-list

This command is used to select the ingress streams that should map to this FRER instance.

Default

```
none
```

Format

```
ingress stream-id-list <1-127>
```

Mode

```
TSN FRER configuration Mode
```

no ingress stream-id-list

This command is used to clear the list of ingress stream IDs.

Format

```
no ingress stream-id-list
```

Mode

```
TSN FRER configuration Mode
```

20.2.2. ingress stream-collection-id

This command is used to select the ingress streams collection that should map to this FRER instance. This cannot be used in indivudal recovery mode.

Default

```
disable
```

Format

```
ingress stream-collection-id <1-63>
```

Mode

```
TSN FRER configuration Mode
```

■ no ingress stream-collection-id

This command is used to clear the ingress stream collection ID.

Format

```
no ingress stream-collection-id
```

Mode

```
TSN FRER configuration Mode
```

20.2.3. ingress outer-tag pop

This command is used to in generation mode, remove a possible outer VLAN tag from ingressing frames before egressing with an R-tag and a possible outer FRER VLAN tag.

Default

```
none
```

Format

```
ingress outer-tag pop
```

Mode

```
TSN FRER configuration Mode
```

■ no ingress outer-tag pop

This command is used to preserve a possible outer VLAN tag beneath the R-tag on egress (generation mode, only).

Format

```
no ingress outer-tag pop
```

Mode

```
TSN FRER configuration Mode
```

20.3. frer-vlan

20.3.1. frer-vlan

This command is used to select the VLAN ID that ingress flows get classified to.

Default

```
none
```

Format

```
frer-vlan <vlan_id>
```

Mode

```
TSN FRER configuration Mode
```

no frer-vlan

This command is used to default the VLAN ID that ingress frames get classified to.

Format

```
no frer-vlan
```

Mode

```
TSN FRER configuration Mode
```

20.4. egress

20.4.1. egress interface

This command is used to select the egress ports that this FRER instance will hit.

Default

```
none
```

Format

```
egress interface <port_type_list>
```

Mode

```
TSN FRER configuration Mode
```

no egress interface

This command is used to unset the egress interfaces of this FRER instance.

Format

```
no egress interface
```

Mode

```
TSN FRER configuration Mode
```

20.5. recovery

20.5.1. recovery algorithm

This command is used to configure recovery algorithm. "match" represents run match recovery algorithm (802.1CB, clause 7.4.3.5). "vector" represents run vector recovery algorithm (802.1CB, clause 7.4.3.4). "history-length" represents select the vector algorithm's history length.

Default

```
vector history-length 2
```

Format

```
recovery algorithm { match | vector [ history-length <2-32> ] }
```

Mode

```
TSN FRER configuration Mode
```

■ no recovery algorithm

This command is used to default the recovery algorithm.

Format

```
no recovery algorithm
```

Mode

```
TSN FRER configuration Mode
```

20.5.2. recovery reset-timeout

This command is used to configure recovery function's reset-timeout in milliseconds.

Default

```
1000
```

Format

```
recovery reset-timeout <1-4095>
```

Mode

```
TSN FRER configuration Mode
```

■ no recovery reset-timeout

This command is used to default the recovery function's reset timeout.

Format

```
no recovery reset-timeout
```

Mode

```
TSN FRER configuration Mode
```

20.5.3. recovery take-no-sequence

This command is used to configure whether recovery function accepts non-R-tagged frames.

Default

```
disable
```

Format

```
recovery take-no-sequence
```

Mode

```
TSN FRER configuration Mode
```

no recovery take-no-sequence

This command is used to configure whether recovery function accepts non-R-tagged frames to default.

Format

```
no recovery take-no-sequence
```

Mode

```
TSN FRER configuration Mode
```

20.5.4. recovery individual

This command is used to enabled individual recovery.

Default

```
disable
```

Format

```
recovery individual
```

Mode

```
TSN FRER configuration Mode
```

no recovery individual

This command is used to disabled individual recovery.

Format

```
no recovery individual
```

Mode

```
TSN FRER configuration Mode
```

20.5.5. recovery terminate

This command is used to configure R-Tags are to be stripped by this FRER instance.

Default

```
disable
```

Format

```
recovery terminate
```

Mode

```
TSN FRER configuration Mode
```

no recovery terminate

This command is used to configure this FRER instance not to strip R-Tags.

Format

```
no recovery terminate
```

Mode

```
TSN FRER configuration Mode
```

20.5.6. recovery latent-error-detection

This command is used to enable the recovery latent error detection function. "difference" represents set the maximum allowed difference between discarded packets and passed packets before triggering the detection of a latent error. "period" represents set the period with which the latent error test function runs. "paths" represents set the number of member streams (ingress paths) that the latent error test function operates on. "reset-period" represents set the period between running the latent error reset function.

Default

```
disable
```

Format

```
recovery latent-error-detection [ difference <0-10000000> ] [ period <1000-86400000> ]
[ paths <2-8> ] [ reset-period <1000-86400000>]
```

Mode

```
TSN FRER configuration Mode
```

no recovery latent-error-detection

This command is used to disable the recovery latent error detection function.

Format

```
no recovery latent-error-detection [ difference <0-10000000> ] [ period
<1000-86400000> ] [ paths <2-8> ] [ reset-period <1000-86400000>]
```

Mode

```
TSN FRER configuration Mode
```

20.6. admin-state

20.6.1. admin-state

This command is used to enable or disable a FRER instance.

Default

```
disable
```

Format

```
admin-state { enable | disable }
```

Mode

```
TSN FRER configuration Mode
```

20.7. no tsn

20.7.1. no tsn frer

This command is used to delete a particular or all FRER instances.

Format

```
no tsn frer { <1-127,1> | all }
```

Mode

```
Global Configuration Mode
```

20.8. tsn

20.8.1. tsn frer

This command is used to if latent-error is not specified: In generation mode, this resets the sequence counter. In recovery mode, this resets all recovery algorithms for this FRER instance.

Format

```
tsn frer <1-127,1> reset [ latent-error ]
```

Mode

```
User EXEC Mode
```

20.9. show

20.9.1. show tsn frer

This command is used to show the state or counters of one or more FRER instances.

Format

```
show tsn frer [ <1~127> ] [ statistics ] [ details ]
```

Mode

```
User EXEC Mode
```

20.10. clear

20.10.1. clear tsn frer

This command is used to clear the counters of one or more FRER instances.

Format

```
clear tsn frer [ <1~127> ] statistics
```

Mode

```
User EXEC Mode
```

21. Green Ethernet

Green Ethernet reduces the power consumption of network devices during low load or even idle states through intelligent management. It can automatically adjust power consumption based on the connected devices or the length of the cable. The switch can automatically enter energy-saving mode when network traffic is low or disconnected ports are detected, reducing power consumption. Network devices can quickly enter a sleep state based on actual traffic demand and wake up rapidly to ensure network performance while reducing energy consumption. When a port is detected to be disconnected or without traffic for an extended period, the switch can selectively shutdown that port to further decrease energy consumption.

21.1. green-ethernet

21.1.1. green-ethernet eee optimize-for-power

This command is used to sets if EEE should be optimized for least power comsumption.

Default

```
disable
```

Format

```
green-ethernet eee optimize-for-power
```

Mode

```
Global Configuration Mode
```

■ no green-ethernet eee optimize-for-power

This command is used to sets if EEE should be optimized for least traffic latency.

Format

```
no green-ethernet eee optimize-for-power
```

Mode

```
Global Configuration Mode
```

21.1.2. green-ethernet eee

This command enables EEE mode.

Default

```
Disable
```

Format

```
green-ethernet eee
```

Mode

```
Port Configuration Mode
```

■ no green-ethernet eee

This command disables EEE mode.

Format

```
no green-ethernet eee
```

Mode

```
Port Configuration Mode
```

21.1.3. green-ethernet eee urgent-queues

This command enables EEE urgent queue. An urgent queue means that latency is kept to a minimum for traffic going to that queue. Note: EEE power savings will be reduced.

Default

```
disable
```

Format

```
green-ethernet eee urgent-queues [ <range_list> ]
```

Mode

```
Port Configuration Mode
```

■ no green-ethernet eee

This command disables EEE urgent queue.

Format

```
no green-ethernet eee
```

Mode

```
Port Configuration Mode
```

21.1.4. green-ethernet acti-phy

This command enable power saving for ports with no link partner.

Default

```
disable
```

Format

```
green-ethernet acti-phy
```

Mode

```
Port Configuration Mode
```

■ no green-ethernet acti-phy

This command disables power saving for ports with no link partner.

Format

```
no green-ethernet acti-phy
```

Mode

```
Port Configuration Mode
```

21.1.5. green-ethernet perfect-reach

This command enables power saving for ports which is connect to link partner with short cable.

Default

```
disable
```

Format

```
green-ethernet perfect-reach
```

Mode

```
Port Configuration Mode
```

■ no green-ethernet perfect-reach

This command disables power saving for ports which is connect to link partner with short cable.

Format

```
no green-ethernet perfect-reach
```

Mode

```
Port Configuration Mode
```

21.2. show

21.2.1. show green-ethernet eee

This command is used to show green Ethernet EEE status.

Format

```
show green-ethernet eee [ interface <port_type_list> ]
```

Mode

```
User EXEC Mode
```

21.2.2. show green-ethernet perfect-reach

This command is used to show green Ethernet perfect-reach status.

Format

```
show green-ethernet perfect-reach [ interface <port_type_list> ]
```

Mode

```
User EXEC Mode
```

21.2.3. show green-ethernet acti-phy

This command is used to show green Ethernet acti-phy status.

Format

```
show green-ethernet acti-phy [ interface <port_type_list> ]
```

Mode

```
User EXEC Mode
```

21.2.4. show green-ethernet

This command is used to show green Ethernet status.

Format

```
show green-ethernet [ interface <port_type_list> ]
```

Mode

```
User EXEC Mode
```

22. GVRP

GVRP stands for GARP VLAN Registration Protocol. It is a protocol for dynamically registering VLANs on ports, and is described in Article 11 of IEEE 802.1Q-2005. GVRP is an example of the use of GARP, so the abbreviation G is used in GVRP.

22.1. gvrp

This chapter allows you to configure global GVRP, which is typically applied to ports that enable GVRP.

22.1.1. gvrp (global)

This command is used to globally enable GVRP.

Default

```
disable
```

Format

```
gvrp
```

Mode

```
Global Configuration Mode
```

no gvrp

This command is used to globally disable GVRP.

Format

```
no gvrp
```

Mode

```
Global Configuration Mode
```

22.1.2. gvrp time

This command is used to configure the timer parameters for the GARP protocol, as specified in IEEE 802.1D-2004, Section 12.11. The Join timer, Leave timer, and LeaveAll timer are protocol parameters measured in centiseconds (i.e., 1/100 of a second). The range *<1-20>* represents the value for the Join timer, *<60-300>* represents the value for the Leave timer, and *<1000-5000>* represents the value for the LeaveAll timer.

Default

```
Join-time : 20
Leave-time : 60
LeaveAll-time : 1000
```

Format

```
gvrp time { [ join-time <1-20> ] [ leave-time <60-600> ] [ leave-all-time
<1000-5000> ] }
```

Mode

```
Global Configuration Mode
```

no gvrp time

This command is used to restore GARP protocol timer parameters to default.

Format

```
no gvrp time { [ join-time <1-20> ] [ leave-time <60-600> ] [ leave-all-time
<1000-5000> ] }
```

Mode

```
Global Configuration Mode
```

22.1.3. gvrp max-vlans

This command is used to configure the number of simultaneously VLANs that GVRP can control. *<1-4094>* represents the maximum number of VLANs.

Default

```
4094
```

Format

```
gvrp max-vlans <1-4094>
```

Mode

```
Global Configuration Mode
```

■ no gvrp max-vlans

This command is used to restore the maximum number of VLANs to default.

Format

```
no gvrp max-vlans <1-4094>
```

Mode

```
Global Configuration Mode
```

22.1.4. gvrp (port)

This command is used to enable GVRP on interface or interfaces.

Default

```
disable
```

Format

```
gvrp
```

Mode

```
Port Configuration Mode
```

■ no gvrp

This command is used to disable GVRP on interface or interfaces.

Format

```
no gvrp
```

Mode

```
Port Configuration Mode
```

23. http

This chapter allows you to configure HTTP settings and maintain the current port on the switch.

23.1. ip http

23.1.1. ip http

This command is Enable HTTP web server.

Default

```
enable
```

Format

```
ip http
```

Mode

```
Global Configuration Mode
```

■ no ip http

This command is Disable HTTP web server.

Format

```
no ip http
```

Mode

```
Global Configuration Mode
```

23.1.2. ip http port

This command is HTTP web server port. <*80,1024-65535*> HTTP Listen Port.

Default

```
80
```

Format

```
ip http port <80,1024-65535>
```

Mode

```
Global Configuration Mode
```

■ no ip http port

This command is Restore the HTTP default port number.

Format

```
no ip http port
```

Mode

```
Global Configuration Mode
```

23.2. show

23.2.1. show ip http

This command is used to display the secure HTTP web server status.

Format

```
show ip http
```

Mode

```
User EXEC Mode
```

24. HTTPS

This chapter allows you to configure HTTPS settings and maintain the current certificate on the switch.

24.1. ip http secure

24.1.1. ip http secure-server

This command is used to enable the HTTPS mode.

Default

```
disable
```

Format

```
ip http secure-server
```

Mode

```
Global Configuration Mode
```

■ no ip http secure-server

This command is used to disable the HTTPS mode.

Format

```
no ip http secure-server
```

Mode

```
Global Configuration Mode
```

24.1.2. ip http secure-port

This command configures the secure port for the HTTPS web server: *<443,1024-65535>* (HTTPS listening port).

Default

```
443
```

Format

```
ip http secure-port <443,1024-65535>
```

Mode

```
Global Configuration Mode
```

■ no ip http secure-port

Restore the HTTPS default port 443.

Format

```
no ip http secure-port
```

Mode

```
Global Configuration Mode
```

24.1.3. ip http secure-redirect

This command is used to enable automatically redirect the web browser to HTTPS mode.

Default

```
disable
```

Format

```
ip http secure-redirect
```

Mode

```
Global Configuration Mode
```

■ no ip http secure-redirect

This command is used to disable automatically redirect the web browser to HTTPS mode.

Format

```
no ip http secure-redirect
```

Mode

```
Global Configuration Mode
```

24.1.4. ip http secure-certificate

This command is used to manage the HTTPS certificate(PEM format). *<url_file>* represents the URL of the certificate PEM file. *<word64>* represents the pass phrase in this field if your uploading certificate is protected by a specific passphrase. "delete" represents delete the current certificate. Generate represents generate a new self-signed RSA certificate.

Default

```
none
```

Format

```
ip http secure-certificate { upload <url_file> [ pass-phrase <word64> ] | delete |
generate }
```

Mode

```
Global Configuration Mode
```

24.2. show

24.2.1. show ip https

This command is used to display the secure HTTPS web server status.

Format

```
show ip https
```

Mode

```
User EXEC Mode
```

25. IGMP

IGMP (Internet Group Management Protocol) is used to manage multicast group memberships between hosts and adjacent multicast routers. It enables the efficient management and distribution of multicast traffic in IP networks.

25.1. ip igmp

25.1.1. ip igmp

This command is used to enable IGMP functionality, including in global and VLAN modes.

Default

```
disable
```

Format

```
ip igmp
```

Mode

```
Global Configuration Mode/VLAN Interface Mode
```

■ no ip igmp

This command is used to disable IGMP functionality, including in global and VLAN modes.

Format

```
no ip igmp
```

Mode

```
Global Configuration Mode/VLAN Interface Mode
```

25.1.2. ip igmp version

This command is used to configuration Igmp version number.

Default

```
3
```

Format

```
ip igmp version <2-3>
```

Mode

```
VLAN Interface Mode
```

■ no ip igmp version

This command is used to configuration Igmp version number to default value.

Format

```
no ip igmp version
```

Mode

```
VLAN Interface Mode
```

25.1.3. ip igmp querier

This command is used to configuration query interval value or last member interval value or Max response time for query.

Default

```
query-interval: 125
last-member-interval: 10
max-response-time: 100
```

Format

```
ip igmp querier { query-interval <2-1800> | last-member-interval <1-255> | max-response-time <10-250> }
```

Mode

```
VLAN Interface Mode
```

■ no ip igmp querier

This command is used to configuration query interval value or last member interval value or Max response time for query to default value.

Format

```
no ip igmp querier { query-interval | last-member-interval | max-response-time }
```

Mode

```
VLAN Interface Mode
```

25.1.4. ip igmp-proxy

This command is used to enable IGMP proxy on the device.

Default

```
Disable
```

Format

```
ip igmp-proxy
```

Mode

```
Global Configuration Mode/VLAN Interface Mode
```

■ no igmp-proxy

This command is used to disable IGMP proxy on the device.

Format

```
no igmp-proxy
```

Mode

```
Global Configuration Mode/VLAN Interface Mode
```

25.2. show

25.2.1. show ip igmp

This command is used to show IGMP sources information, groups information, specific interface or interfaces or IGMP statistics.

Format

```
show ip igmp { sources | groups | interface vlan [ <vlan_id> ] | statistics }
```

Mode

```
User EXEC Mode
```

26. IP

Using an IP address (Internet Protocol Address) enables the management and communication of switches across different network layers, including routing capabilities, DNS proxy, ARP proxy, directed broadcast, and ICMP-related functions.

26.1. ip

26.1.1. ip domain name

This command is used to define the default domain name.

Default

```
none
```

Format

```
ip domain name { <domain_name> | dhcp [ ipv4 | ipv6 ] [ interface vlan <vlan_id> ] }
```

Mode

```
Global Configuration Mode
```

26.1.2. ip routing

This command is used to configure the IP stack should act as a Router. In Router mode traffic is routed between all interfaces.

Default

```
router
```

Format

```
ip routing
```

Mode

```
Global Configuration Mode
```

no ip routing

This command is used to configure the IP stack should act as a Host. In Host mode, IP traffic between interfaces will not be routed.

Format

```
no ip routing
```

Mode

```
Global Configuration Mode
```

26.1.3. ip route

This command is used to configure the address, mask length, gateway, and distance of IP routing.

Format

```
ip route <ipv4_subnet> <ipv4_ucast> [ distance <1-255> ]
```

Mode

```
Global Configuration Mode
```

■ no ip route

This command is used to delete the address, mask length, gateway, and distance of an IP route.

Format

```
no ip route <ipv4_subnet> <ipv4_ucast> [ distance <1-255> ]
```

Mode

```
Global Configuration Mode
```

26.1.4. ip route (Netmask)

This command is used to configure the address, mask, gateway, and distance of IP routing.

Format

```
ip route <ipv4_addr> <ipv4_netmask> { <ipv4_ucast> } [ distance <1-255> ]
```

Mode

```
Global Configuration Mode
```

■ no ip route

This command is used to delete the address, mask, gateway, and distance of an IP route.

Format

```
no ip route <ipv4_addr> <ipv4_netmask> { <ipv4_ucast> } [ distance <1-255> ]
```

Mode

```
Global Configuration Mode
```

26.1.5. ip route track (Netmask)

This command is used to configure the address, mask length, gateway, and name of the IP route track object.

Format

```
ip route track <ipv4_addr> <ipv4_netmask> { <ipv4_ucast> } <cword>
```

Mode

```
Global Configuration Mode
```

■ no ip route track

This command is used to delete the address, mask length, and gateway of the IP route track object.

Format

```
no ip route track <ipv4_addr> <ipv4_netmask> { <ipv4_ucast> }
```

Mode

```
Global Configuration Mode
```

26.1.6. ip route track

This command is used to configure the address, mask length, gateway, and name of the IP route track object.

Format

```
ip route track <ipv4_subnet> <ipv4_ucast> <cword>
```

Mode

```
Global Configuration Mode
```

no ip route track

This command is used to delete the address, mask length, and gateway of an IP route track.

Format

```
no ip route track <ipv4_subnet> <ipv4_ucast>
```

Mode

```
Global Configuration Mode
```

26.1.7. ip dns proxy

This command is used to enable the DNS proxy service.

Default

```
none
```

Format

```
ip dns proxy
```

Mode

```
Global Configuration Mode
```

no ip dns proxy

This command is used to disable the DNS proxy service.

Format

```
no ip dns proxy
```

Mode

```
Global Configuration Mode
```

26.1.8. ip address

This command is used to configure the IP addresses for interfaces, including the loopback interface.

Default

```
none
```

Format

```
ip address <ipv4_subnet>
```

Mode

```
VLAN Interface Mode
```

no ip address

This command is used to remove the IP addresses of interfaces, including loopback interfaces.

Format

```
no ip address
```

Mode

```
VLAN Interface Mode
```

26.1.9. ip proxy-arp

This command enables proxy ARP on a router interface. It is applicable to proxies between different vlans. Without proxy ARP, a device only responds to an ARP request if the target IP address is an address configured on the interface where the ARP request arrived. With proxy ARP, the device may also respond if the target IP address is reachable. The device only responds if all next hops in its route to the destination are through interfaces other than the interface that received the ARP request.

Default

```
disable
```

Format

```
ip proxy-arp
```

Mode

```
VLAN Interface Mode
```

no ip proxy-arp

This command disables proxy ARP on a router interface.

Format

```
no ip proxy-arp
```

Mode

```
VLAN Interface Mode
```

26.1.10. ip local-proxy-arp

This command enables local proxy ARP on a router interface. It is applicable to the isolation port proxy between the same VLAN. Without local proxy ARP, a device only responds to an ARP request if the target IP address is an address configured on the interface where the ARP request arrived. With local proxy ARP, the device may also respond if the target IP address is reachable. The device only responds if all next hops in its route to the destination are through interfaces other than the interface that received the ARP request.

Default

```
disable
```

Format

```
ip local-proxy-arp
```

Mode

```
VLAN Interface Mode
```

no ip local-proxy-arp

This command disables local proxy ARP on a router interface.

Format

```
no ip local-proxy-arp
```

Mode

```
VLAN Interface Mode
```

26.1.11. ip icmp echo-reply

This command enables sending icmp messages. Use no command to disable.

Default

```
disable
```

Format

```
ip icmp echo-reply
```

Mode

```
Global Configuration Mode
```

no ip icmp echo-reply

This command disables sending icmp messages.

Format

```
no ip icmp echo-reply
```

Mode

```
Global Configuration Mode
```

26.1.12. ip icmp unreachables

This command enables sending the icmp unreachable messages. Use no command to disable.

Default

```
disable
```

Format

```
ip icmp unreachables
```

Mode

```
VLAN Interface Mode
```

no ip icmp unreachables

This command disables sending the icmp unreachable messages.

Format

```
no ip icmp unreachables
```

Mode

```
VLAN Interface Mode
```

26.1.13. ip icmp rate-limit threshold

This command configures the packet rate, in pps, allowed sending icmp messages. *<1-500>* represents the threshold value.

Default

```
100
```

Format

```
ip icmp rate-limit threshold <1-500>
```

Mode

```
Global Configuration Mode
```

no ip icmp rate-limit threshold

This command resets the icmp packet rate to the default value.

Format

```
no ip icmp rate-limit threshold
```

Mode

```
Global Configuration Mode
```

26.1.14. ip icmp redirects

This command enables sending icmp redirects. Use no command to disable.

Default

```
disable
```

Format

```
ip icmp redirects
```

Mode

```
VLAN Interface Mode
```

■ no ip icmp redirects

This command disables sending icmp redirects.

Format

```
no ip icmp redirects
```

Mode

```
VLAN Interface Mode
```

26.1.15. ip directed-broadcast

This command enables net directed broadcasts of IP frames. Use no command to disable.

Default

```
disable
```

Format

```
ip directed-broadcast
```

Mode

```
VLAN Interface Mode
```

■ no ip directed-broadcast

This command disables net directed broadcasts of IP frames.

Format

```
no ip directed-broadcast
```

Mode

```
VLAN Interface Mode
```

26.1.16. ip address (DHCP)

This command can configure the IP address/prefix size, DHCP fallback address/prefix size, DHCP fallback timeout, default value is 60 seconds, value range is 0 to 4294967295 seconds, DHCP client identifier, etc.

Default

```
none
```

Format

```
ip address { { <ipv4_subnet> } | { dhcp [ fallback <ipv4_subnet> [ timeout <uint> ] ]
[ client-id { <port_type_id> | ascii <word31> | hex <word64> } ] [ hostname
<domain_name63> ] } }
```

Mode

```
VLAN Interface Mode
```

no ip address

This command is used to delete ip address configuration.

Format

```
no ip address
```

Mode

```
VLAN Interface Mode
```

26.2. interface

26.2.1. interface loopback

This command configures the loopback interface.

Default

```
none
```

Format

```
interface loopback <loopback-id>
```

Mode

```
Global Configuration Mode
```

no interface loopback

This command deletes the loopback interface.

Format

```
no interface loopback <loopback-id>
```

Mode

```
Global Configuration Mode
```

26.3. ping

1.1.3.ping ip

This command is used to issue ICMP (IPv4) PING packets to troubleshoot IP connectivity issues. *<domain_name>* or *<ipv4_addr>* represents the address of the destination host, either as a symbolic hostname or an IP Address. *<1-255>* represents the Time-To-Live (TTL) field value in the IPv4 header. *<1-60>* represents the number of PING requests sent. *<ipv4_addr>* represents send from interface with source address. *<port_type_id>* represents source interface. *<vlan_id>* represents source VLAN interface. *<loopback_id>* represents source loopback interface. *<2-1452>* represents the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP and ICMP headers). *<0-255>* represents the pattern used in the ICMP data payload.

Default

```
ttl : 64
repeat : 5
size : 56
data : 0
```

Format

```
ping [ ip ] { <domain_name> | <ipv4_addr> } [ ttl <1-255> ] [ repeat <1-60> ] [ { saddr <ipv4_addr> | sif { <port_type_id> | vlan <vlan_id> | loopback <loopback_id> } } ] [ size <2-1452> ] [ data <0-255> ] [ { verbose | quiet } ]
```

Mode

```
User EXEC Mode
```

26.3.1. ping ipv6

This command is used to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues. *<domain_name>* or *<ipv6_addr>* represents the address of the destination host, either as a symbolic hostname or an IP Address. *<1-60>* represents the number of PING requests sent. *<ipv6_addr>* represents send from interface with source address. *<port_type_id>* represents source interface. *<vlan_id>* represents source VLAN interface. *<2-1452>* represents the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP and ICMP headers). *<0-255>* represents the pattern used in the ICMP data payload.

Default

```
repeat : 5
size : 56
data : 0
```

Format

```
ping ipv6 { <domain_name> | <ipv6_addr> } [ repeat <1-60> ] [ saddr <ipv6_addr> ] [ sif { <port_type_id> | vlan <vlan_id> } ] [ size <2-1452> ] [ data <0-255> ] [ { verbose | quiet } ]
```

Mode

```
User EXEC Mode
```

26.3.2. ping sif loopback

The ping command uses the loopback address as the source interface to send packets to the destination address.

Default

```
none
```

Format

```
ping <ipv4_addr> sif loopback <loopback-id>
```

Mode

```
User EXEC Mode
```

26.4. traceroute

26.4.1. traceroute ip

This command is used to perform a traceroute test over IPv4 towards a remote host. Traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv4 network. *<domain_name>* or *<ipv4_addr>* represents the address of the destination host, either as a symbolic hostname or an IP Address. *<0-63>* represents the DSCP value in the IPv4 header. *<1-86400>* represents the number of seconds to wait for a reply to a sent request. *<ipv4_addr>* represents send from interface with source address. *<port_type_id>* represents source interface. *<vlan_id>* represents source VLAN interface. *<1-60>* represents the number of probes (packets) sent for each hop. *<1-30>* represents the value of the Time-To-Live (TTL) field in the IPv4 header in the first packet sent. *<1-255>* represents the maximum value of the Time-To-Live (TTL) field in the IPv4 header, if this value is reached before the specified remote host is reached the test stops.

Default

```
dscp : 0
timeout : 3
probes : 3
firstttl : 1
maxttl : 30
```

Format

```
traceroute ip { <domain_name> | <ipv4_addr> } [ dscp <0-63> ] [ timeout <1-86400> ] [ { saddr <ipv4_addr> | sif {<port_type_id> | vlan <vlan_id> } } ] [ probes <1-60> ] [ firstttl <1-30> ] [ maxttl <1-255> ] [ icmp ] [ numeric ]
```

Mode

```
User EXEC Mode
```

26.4.2. traceroute ipv6

This command is used to perform a traceroute test over IPv6 towards a remote host. Traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv6 network. *<domain_name>* or *<ipv6_addr>* represents the address of the destination host, either as a symbolic hostname or an IP Address. *<0-255>* represents the DSCP value in the IPv6 header. *<1-86400>* represents the number of seconds to wait for a reply to a sent request. *<ipv6_addr>* represents send from interface with source address. *<port_type_id>* represents source interface. *<vlan_id>* represents source VLAN interface. *<1-60>* represents the number of probes (packets) sent for each hop. *<1-255>* represents the maximum value of the Time-To-Live (TTL) field in the IPv6 header, if this value is reached before the specified remote host is reached the test stops.

Default

```
dscp : 0
timeout : 3
probes : 3
maxttl : 30
```

Format

```
traceroute ipv6 { <domain_name> | <ipv6_addr> } [ dscp <0-255> ] [ timeout <1-86400> ] [ saddr <ipv6_addr> ] [ sif { <port_type_id> | vlan <vlan_id> } ] [ probes <1-60> ] [ maxttl <1-255> ] [ numeric ]
```

Mode

```
User EXEC Mode
```

26.5. show

26.5.1. show ip domain

This command display the active domain name information.

Default

none

Format

show ip domain

Mode

User EXEC Mode

26.5.2. show interface loopback

This command queries the loopback interface configuration information.

Default

none

Format

show interface loopback [*<loopback-id>*]

Mode

User EXEC Mode

26.5.3. show running-config interface loopback

This command checks the global configuration of loopback.

Default

none

Format

show running-config interface loopback *<loopback-id>*

Mode

User EXEC Mode

26.5.4. show ipv6 route

This command is used to show ipv6 route information.

Format

show ipv6 route

Mode

User EXEC Mode

26.5.5. show ip route track

This command is used to display the information of the route track object.

Format

show ip route track

Mode

User EXEC Mode

26.5.6. show ip route

This command is used to show the routing table status.

Format

```
show ip route
```

Mode

```
User EXEC Mode
```

26.5.7. show ip interface

This command can query all IP interface information, including query for loopback interface information.

Default

```
none
```

Format

```
show ip interface
```

Mode

```
User EXEC Mode
```

26.5.8. show ip neighbor

This command is used to print ARP/neighbor table.

Format

```
show ip neighbor
```

Mode

```
User EXEC Mode
```

27. IP Source Guard

IP Source Guard is used to prevent IP address fraud and spoofing on the network by restricting each port on network devices to only use a specific one or set of IP addresses to send traffic, thereby enhancing network security.

27.1. ip

Note: When the global configuration mode and port configuration mode are enabled on a specified port, the IP source protection will be enabled on the specified port. Moreover, if the global configuration mode is enabled, all the configured ACE will be lost.

27.1.1. ip verify source (global)

This command is used to enable global configuration mode.

Default

```
disable
```

Format

```
ip verify source
```

Mode

```
Global Configuration Mode
```

■ no ip verify source

This command is used to disable global configuration mode.

Format

```
no ip verify source
```

Mode

```
Global Configuration Mode
```

27.1.2. ip verify source translate

This command is used to translate all dynamic entries to static entries.

Format

```
ip verify source translate
```

Mode

```
Global Configuration Mode
```

27.1.3. ip verify source (port)

This command is used to enable port configuration mode, specify to enable IP source protection on this port.

Default

```
disable
```

Format

```
ip verify source
```

Mode

```
Port Configuration Mode
```

no ip verify source

This command is used to disable port configuration mode.

Format

```
no ip verify source
```

Mode

```
Port Configuration Mode
```

27.1.4. ip verify source limit

This command is used to configure the number of client MACs allows on the port. <*0-2*> represents the maximum number of dynamic clients that can be learned on given port.

Default

```
unlimited
```

Format

```
ip verify source limit <0-2>
```

Mode

```
Port Configuration Mode
```

no ip verify source limit

This command is used to restore the number of client MACs allows on the port to unlimited.

Format

```
no ip verify source limit
```

Mode

```
Port Configuration Mode
```

27.1.5. ip source binding interface

This command is used to configure IP source binding entry interface. <*port_type_id*> represents port id to configure. <*vlan_id*> represents VLAN id to configure. <*ipv4_ucast*> represents IP Address to configure. <*mac_ucast*> represents MAC address to configure.

Default

```
none
```

Format

```
ip source binding interface <port_type_id> <vlan_id> <ipv4_ucast> <mac_ucast>
```

Mode

```
Global Configuration Mode
```

no ip source binding interface

This command is used to delete IP source binding entry interface. <*port_type_id*> represents port id. <*vlan_id*> represents VLAN id. <*ipv4_ucast*> represents IP Address. <*mac_ucast*> represents MAC address.

Format

```
no ip source binding interface <port_type_id> <vlan_id> <ipv4_ucast> <mac_ucast>
```

Mode

```
Global Configuration Mode
```

27.2. show

27.2.1. show ip verify source

This command is used to display IP verify source interface configuration. *<port_type_list>* represents port list.

Format

```
show ip verify source [ interface <port_type_list> ]
```

Mode

```
User EXEC Mode
```

27.2.2. show ip source binding

This command is used to display IP source binding interface configuration. *<port_type_list>* represents port list.

Format

```
show ip source binding [ dhcp-snooping | static ] [ interface <port_type_list> ]
```

Mode

```
User EXEC Mode
```

28. IPMC Profile

IPMC (Internet Protocol Multicast) Profile is used to manage and optimize multicast traffic on network devices. Multicast is a network transmission mechanism that allows a single data source to simultaneously send packets to multiple destinations.

28.1. ipmc

28.1.1. ipmc profile

This command is used to enable global IPMC Profie function.

Default

```
disabld
```

Format

```
ipmc profile
```

Mode

```
Global Configuration Mode
```

■ no ipmc profile

This command is used to disable the global IPMC configuration file function.

Format

```
no ipmc profile
```

Mode

```
Global Configuration Mode
```

28.1.2. ipmc profile profile-name

This command is used to specify the name of IPMC profile entry on which access control is enabled, and enters icmp profile configuration mode.

Default

```
none
```

Format

```
ipmc profile <profile-name>
```

Mode

```
Global Configuration Mode
```

■ no ipmc profile

This command is used to delete the name of IPMC or to delete all.

Format

```
no ipmc profile { [ <profile-name> | all ] }
```

Mode

```
Global Configuration Mode
```

28.1.3. ipmc range range-name

This command is used to define the expected address ranges. <*word1-16*> represents name of range, <*ipv4_mcast*> represents valid IPv4 multicast address, <*ipv6_mcast*> represents valid IPv6 multicast address.

Default

none

Format

ipmc range <*word1-16*> { <*ipv4_mcast*> [<*ipv4_mcast*>] | <*ipv6_mcast*> [<*ipv6_mcast*>] }

Mode

Global Configuration Mode

■ no ipmc range range-name

This command is used to delete the desired address ranges.

Format

no ipmc range range-name

Mode

Global Configuration Mode

28.2. description

28.2.1. description

This command is used to add additional notes for describing the specific profile.

Default

none

Format

description <*line64*>

Mode

IPMC Profile Mode

■ no description

This command is used to delete additionalnotesfor describing the specific profile.

Format

no description

Mode

IPMC Profile Mode

28.3. range

28.3.1. range range-name

This command is used to arrange and configure rules for the specific profile. Configuring deny matching addresses, permit matching addresses, log when matching, next *<word1-16>* represents to insert this rule a specific place in this profile's list, write the name of the range to insert it just before. If left out, this new rule will be added last.

Default

```
none
```

Format

```
range <word1-16> { [ deny | permit ] } [ log ] [ next <word1-16> ]
```

Mode

```
IPMC Profile Mode
```

no range range-name

This command is used to delete rules for the specific profile.

Format

```
no range <word1-16>
```

Mode

```
IPMC Profile Mode
```

28.4. show

28.4.1. show ipmc profile

This command is used to show ipmc profile configuration/status.

Format

```
show ipmc profile { [ profile-name | detail ] }
```

Mode

```
User EXEC Mode
```

29. IPMC

IPMC (Intelligent Platform Management Controller) is a hardware management controller used for monitoring and managing switches.

29.1. ip igmp

29.1.1. ip igmp

The command is used to set the IPv4 multicast address and to enable the flooding of unregistered IPv4 multicast traffic.

Default

```
ssm-range : 232.0.0.0/8
unknown-flooding : enable
```

Format

```
ip igmp { [ ssm-range <ipv4_mcast> <4-32> | unknown-flooding ] }
```

Mode

```
Global Configuration Mode
```

■ no ip igmp

The command is used to restore the default IPv4 multicast address and to disable the flooding of unregistered IPv4 multicast traffic.

Format

```
no ip igmp { [ ssm-range | unknown-flooding ] }
```

Mode

```
Global Configuration Mode
```

29.1.2. ip igmp snooping (global)

This command is used to enable the global igmp snooping function.

Default

```
enable
```

Format

```
ip igmp snooping
```

Mode

```
Global Configuration Mode
```

■ no ip igmp snooping

This command is used to disable the global igmp snooping function.

Format

```
no ip igmp snooping
```

Mode

```
Global Configuration Mode
```

29.1.3. ip igmp host-proxy

This command is used to enables IGMP host proxy or leave proxy.

Default

```
disable
```

Format

```
ip igmp host-proxy [ leave-proxy ]
```

Mode

```
Global Configuration Mode
```

■ no ip igmp host-proxy

This command is used to disable the designated (IP) VLAN interface MLD snooping.

Format

```
no ip igmp host-proxy [ leave-proxy ]
```

Mode

```
Global Configuration Mode
```

29.1.4. ip igmp snooping immediate-leave

This command is used to set up fast leave feature.

Default

```
disable
```

Format

```
ip igmp snooping immediate-leave
```

Mode

```
Port Configuration Mode
```

■ no ip igmp snooping immediate-leave

This command is used to delete fast leave feature.

Format

```
no ip igmp snooping immediate-leave
```

Mode

```
Port Configuration Mode
```

29.1.5. ip igmp snooping mrouter

This command is used to set up router port feature.

Default

```
disable
```

Format

```
ip igmp snooping mrouter
```

Mode

```
Port Configuration Mode
```

no ip igmp snooping mrouter

This command is used to delete router port feature.

Format

```
no ip igmp snooping mrouter
```

Mode

```
Port Configuration Mode
```

29.1.6. ip igmp snooping (vlanif)

This command is used to set up IGMP VLAN interface specific configurations.

Default

```
ip igmp snooping : disabled
compatibility : auto
last-member-query-interval : 10
Priority : 0
querier address : none
querier election : enabled
query-interval : 125
query-max-response-time : 100
robustness-variable : 2
unsolicited-report-interval : 1
```

Format

```
ip igmp snooping [ compatibility { auto | v1 | v2 | v3 } | last-member-query-interval
<0-31744> | priority <0-7> | querier address <ipv4_ucast> | querier election |
query-interval <1-31744> | query-max-response-time <0-31744> | robustness-variable
<2-255> | unsolicited-report-interval <1-31744> ]
```

Mode

```
VLAN Interface Mode
```

no ip igmp snooping

This command is used to delete IGMP VLAN interface specific configurations.

Format

```
no ip igmp snooping { [ compatibility | last-member-query-interval | priority | querier
address | querier election | query-interval | query-max-response-time |
robustness-variable | unsolicited-report-interval ] }
```

Mode

```
VLAN Interface Mode
```

29.1.7. ip igmp snooping filter

This command is used to set up filtering feature.

Default

```
none
```

Format

```
ip igmp snooping filter <word16>
```

Mode

```
Port Configuration Mode
```

no ip igmp snooping filter

This command is used to delete filtering feature.

Format

```
no ip igmp snooping filter
```

Mode

```
Port Configuration Mode
```

29.1.8. ip igmp snooping max-groups

This command is used to set up throttling feature.

Default

```
none
```

Format

```
ip igmp snooping max-groups <1-10>
```

Mode

```
Port Configuration Mode
```

no ip igmp snooping max-groups

This command is used to delete throttling feature.

Format

```
no ip igmp snooping max-groups
```

Mode

```
Port Configuration Mode
```

29.2. ipv6 mld

29.2.1. ipv6 mld

The command is used to set the IPv6 multicast address and enable flooding of unregistered IPv6 multicast traffic.

Default

```
ssm-range : ff3e::/96
unknown-flooding : enable
```

Format

```
ipv6 mld { [ ssm-range <ipv6_mcast> <8-128> | unknown-flooding ] }
```

Mode

```
Global Configuration Mode
```

no ipv6 mld

This command is used to delete unknown flooding or SSM range or IPv6 multicast data forwarding.

Format

```
no ipv6 mld { [ ssm-range | unknown-flooding ] }
```

Mode

```
Global Configuration Mode
```

29.2.2. ipv6 mld snooping (global)

This command is used to enable the global MLD snooping function.

Default

```
enable
```

Format

```
ipv6 mld snooping
```

Mode

```
Global Configuration Mode
```

■ no ipv6 mld snooping

This command is used to disable theglobal MLD snooping function.

Format

```
no ipv6 mld snooping
```

Mode

```
Global Configuration Mode
```

29.2.3. ipv6 mld host-proxy

This command is used to enables IGMP host proxy or leave proxy.

Default

```
disable
```

Format

```
ipv6 mld host-proxy [ leave-proxy ]
```

Mode

```
Global Configuration Mode
```

■ no ipv6 mld host-proxy

This command is used to disable the designated (IP) VLAN interface MLD snooping.

Format

```
no ipv6 mld host-proxy [ leave-proxy ]
```

Mode

```
Global Configuration Mode
```

29.2.4. ipv6 mld snooping immediate-leave

This command is used to set up fast leave feature.

Default

```
disable
```

Format

```
ipv6 mld snooping immediate-leave
```

Mode

```
Port Configuration Mode
```

no ipv6 mld snooping immediate-leave

This command is used to delete fast leave feature.

Format

```
no ipv6 mld snooping immediate-leave
```

Mode

```
Port Configuration Mode
```

29.2.5. ipv6 mld snooping mrouter

This command is used to set up router port feature.

Default

```
none
```

Format

```
ipv6 mld snooping mrouter
```

Mode

```
Port Configuration Mode
```

no ipv6 mld snooping mrouter

This command is used to delete router port feature.

Format

```
no ipv6 mld snooping mrouter
```

Mode

```
Port Configuration Mode
```

29.2.6. ipv6 mld snooping (vlanif)

This command is used to set up MLD VLAN interface specific configurations.

Default

```
ipv6 mld snooping : disable
compatibility : auto
last-member-query-interval : 10
priority : 0
querier election : enable
query-interval : 125
query-max-response-time : 100
robustness-variable : 2
unsolicited-report-interval : 1
```

Format

```
ipv6 mld snooping [ compatibility { auto | v1 | v2 } | last-member-query-interval
<0-31744> | priority <0-7> | querier election | query-interval <1-31744> |
query-max-response-time <0-31744> | robustness-variable <2-255> |
unsolicited-report-interval <1-31744> ]
```

Mode

```
VLAN Interface Mode
```

■ no ipv6 mld snooping

This command is used to delete MLD VLAN interface specific configurations.

Format

```
no ipv6 mld snooping { [ compatibility | last-member-query-interval | priority |
querier election | query-interval | query-max-response-time | robustness-variable |
unsolicited-report-interval ] }
```

Mode

```
VLAN Interface Mode
```

29.2.7. ipv6 mld snooping filter

This command is used to set up filtering feature.

Default

```
none
```

Format

```
ipv6 mld snooping filter <word16>
```

Mode

```
Port Configuration Mode
```

■ no ipv6 mld snooping filter

This command is used to delete filtering feature.

Format

```
no ipv6 mld snooping filter
```

Mode

```
Port Configuration Mode
```

29.2.8. ipv6 mld snooping max-groups

This command is used to set up throttling feature.

Default

```
none
```

Format

```
ipv6 mld snooping max-groups <1-10>
```

Mode

```
Port Configuration Mode
```

■ no ipv6 mld snooping max-groups

This command is used to delete throttling feature.

Format

```
no ipv6 mld snooping max-groups
```

Mode

```
Port Configuration Mode
```

29.3. show

29.3.1. show ip igmp snooping

This command is used to show igmp snooping configuration/status.

Format

```
show ip igmp snooping [ mrouter [ details ] | [ [ vlan <vlan_list> ] [ statistics
| { group-database [ interface <port_type_list> ] } ] [ details ] ] ]
```

Mode

```
User EXEC Mode
```

29.3.2. show ipv6 mld snooping

This command is used to show mld snooping configuration/status.

Format

```
show ipv6 mld snooping [ mrouter [ details ] | [ [ vlan <vlan_list> ] [ statistics
| { group-database [ interface <port_type_list> ] } ] [ details ] ] ]
```

Mode

```
User EXEC Mode
```

30. IPv6 Source Guard

IPv6 Source Guard is used to prevent IPv6 address fraud and spoofing on the network by restricting each port on network devices to only use a specific one or set of IPv6 addresses to send traffic, thereby enhancing network security.

30.1. ipv6

Note: When the global configuration mode and port configuration mode are enabled on a specified port, the IPv6 source protection will be enabled on the specified port. Moreover, if the global configuration mode is enabled, all the configured ACE will be lost.

30.1.1. ipv6 verify source (global)

This command is used to enable ipv6 source guard globally.

Default

```
disable
```

Format

```
ipv6 verify source
```

Mode

```
Global Configuration Mode
```

■ no ipv6 verify source

This command is used to disable ipv6 source guard globally.

Format

```
no ipv6 verify source
```

Mode

```
Global Configuration Mode
```

30.1.2. ipv6 verify source translate

This command is used to translate dynamic entries in binding table to static entries.

Format

```
ipv6 verify source translate
```

Mode

```
Global Configuration Mode
```

30.1.3. ipv6 verify source (port)

This command is used to enable ipv6 source guard on current port interface.

Default

```
disable
```

Format

```
ipv6 verify source
```

Mode

```
Port Configuration Mode
```

no ipv6 verify source

This command is used to disable ipv6 source guard on current port interface.

Format

```
no ipv6 verify source
```

Mode

```
Port Configuration Mode
```

30.1.4. ipv6 verify source limit

This command is used to configure the maximum number of dynamic clients on current port interface. *<0-2>* represents the number of max dynamic clients (0, 1 or 2).

Default

```
Unlimited
```

Format

```
ipv6 verify source limit <0-2>
```

Mode

```
Port Configuration Mode
```

no ipv6 verify source limit

This command is used to restore the maximum number of dynamic clients on current port interface to unlimited.

Format

```
no ipv6 verify source limit
```

Mode

```
Port Configuration Mode
```

30.1.5. ipv6 source binding interface

This command is used to creates a new static entry in binding table. No form of the command deletes a static entry from the table. *<port_type_id>* represents port id to configure. *<vlan_id>* represents VLAN id to configure. *<ipv6_ucast>* represents IPv6 address to configure, format xxxx::yyyy. *<mac_ucast>* represents MAC address to configure.

Default

```
none
```

Format

```
ipv6 source binding interface <port_type_id> [ vlan <vlan_id> ] <ipv6_ucast>
<mac_ucast>
```

Mode

```
Global Configuration Mode
```

no ipv6 source binding interface

This command is used to delete IPv6 source binding entry interface. *<port_type_id>* represents port id. *<vlan_id>* represents VLAN id. *<ipv6_ucast>* represents IPv6 address, format xxxx::yyyy. *<mac_ucast>* represents MAC address.

Format

```
no ipv6 source binding interface <port_type_id> [ vlan <vlan_id> ] <ipv6_ucast>
<mac_ucast>
```

Mode

```
Global Configuration Mode
```

30.2. show

30.2.1. show ipv6 verify source

This command is used to display global and per port status of IPv6 source guard. *<0-2>* represents port list.

Format

```
show ipv6 verify source [ interface <port_type_list> ]
```

Mode

```
User EXEC Mode
```

30.2.2. show ipv6 source binding

This command is used to display entries, all, static or dynamic, in binding table per port. *<port_type_list>* represents port list.

Format

```
show ipv6 source binding [ dhcpv6-snooping | static ] [ interface <port_type_list> ]
```

Mode

```
User EXEC Mode
```

31. IRDP

This chapter provides a detailed explanation of ICMP Router Discovery Protocol (IRDP) commands. The commands are divided by functionality into the following different groups:

- Show commands are used to display switch settings, statistics and other information.
- Configuration Commands are used to configure features and options of the switch. Each configuration command can be viewed in the show running-config or the show irdp command.

31.1. ip irdp

31.1.1. ip irdp

This command is used to activate the irdp on the specified interface. The switch defaults to send advertisement to the broadcast address 255.255.255.255.

Default

```
none
```

Format

```
ip irdp
```

Mode

```
VLAN Interface Mode
```

no ip irdp

This command is used to deactivate the irdp on the specified interface and to remove the relevant configuration of the irdp for this interface.

Format

```
no ip irdp
```

Mode

```
VLAN Interface Mode
```

31.1.2. ip irdp enable

This command is used to enable the irdp on the specified interface.

Default

```
none
```

Format

```
ip irdp enable
```

Mode

```
VLAN Interface Mode
```

ip irdp disable

This command is used to disable the irdp on the specified interface.

Format

```
no ip irdp
```

Mode

```
VLAN Interface Mode
```

31.1.3. ip irdp broadcast / multicast

This command is used to specify the destination to which the device sends advertisements. Broadcast: specifies the interface to send advertisement to the broadcast address 255.255.255.255; Multicast: specifies the interface to send advertisement to the multicast address 224.0.0.1.

Default

```
none
```

Format

```
ip irdp broadcast/multicast
```

Mode

```
VLAN Interface Mode
```

31.1.4. ip irdp preference

This command is used to specify the key figure that an end device uses to decide which gateway to the destination network to use when multiple routers in the subnet identify themselves through IRDP. The higher the priority, the more likely it is that end devices will use the switch as a gateway.The range of *<value>* is 0 to 2147483647.

Default

```
0
```

Format

```
ip irdp preference <value>
```

Mode

```
VLAN Interface Mode
```

31.1.5. ip irdp holdtime

This command is used to specify the validity period for the advertisements in seconds. The prerequisite is that the value is greater than or equal to the value specified in the maxadvertinterval column. The range of *<value>* is 4 to 9000.

Default

```
1800
```

Format

```
ip irdp holdtime <value>
```

Mode

```
VLAN Interface Mode
```

■ no ip irdp holdtime

This command is used to restore the default value of the validity time.

Format

```
no ip irdp holdtime
```

Mode

```
VLAN Interface Mode
```

31.1.6. ip irdp maxadvertinterval

This command is used to specify the maximum period in seconds after which the device sends another advertisement. The prerequisite is that the value is greater than or equal to the value specified in the minadvertinterval column.The range of <*value*> is 4 to 1800.

Default

600

Format

ip irdp maxadvertinterval <*value*>

Mode

VLAN Interface Mode

■ no ip irdp maxadvertinterval

This command is used to restore the default value of the maximum period.

Format

no ip irdp maxadvertinterval

Mode

VLAN Interface Mode

31.1.7. ip irdp minadvertinterval

This command is used to specify the minimum period in seconds after which the device sends another advertisement.The range of <*value*> is 3 to 1800.

Default

450

Format

ip irdp minadvertinterval <*value*>

Mode

VLAN Interface Mode

■ no ip irdp minadvertinterval

This command is used to restore the default value of the minimum period.

Format

no ip irdp minadvertinterval

Mode

VLAN Interface Mode

31.1.8. ip irdp address

This command is used to specify the configuration of the proxy addresses and proxy address priorities.

Default

none

Format

ip irdp address <*address*> *preference* <*value*>

Mode

VLAN Interface Mode

no ip irdp address

The no ip irdp address used to remove all proxy addresses .The no ip irdp address <*address*> used to remove the specified proxy address.

Format

```
no ip irdp address <address>
```

Mode

```
VLAN Interface Mode
```

31.2. show

31.2.1. show ip irdp

This command is used to view the irdp statistics of a specific physical port on a switch. The parameter <*intf-id*> is for the specific physical port, and the interface <intf-id> is an optional parameter. If the optional parameter exists, the irdp information of a specific physical interface is displayed. If the optional parameter does not exist, the irdp information of all interfaces is displayed.

Format

```
show ip irdp [ interface <intf-id> ]
```

Mode

```
User EXEC Mode
```

32. Link OAM

The Ethernet OAM (IEEE 802.3ah) protocol for installing, monitoring, and troubleshooting Metro Ethernet networks and Ethernet WANs relies on an optional sub layer in the data link layer of the OSI model. Normal link operation does not require Ethernet OAM (IEEE 802.3ah). You can implement Ethernet OAM(IEEE 802.3ah) on any full-duplex point-to-point or emulated point-to-point Ethernet link for a network or part of a network (specified interfaces).

32.1. link-oam

32.1.1. link-oam remote-loopback

This command is used to turn on or turn off Link OAM remote loopback on an interface.

Default

```
stop
```

Format

```
link-oam remote-loopback { start | stop } interface <port_type_list>
```

Mode

```
User EXEC Mode
```

32.1.2. link-oam

This command is used to enable Link OAM on an interface.

Default

```
link oam is disabled
```

Format

```
link-oam
```

Mode

```
Port Configuration Mode
```

■ no link-oam

This command is used to disable Link OAM on an interface.

Format

```
no link-oam
```

Mode

```
Port Configuration Mode
```

32.1.3. link-oam mode

This command is used to set Link OAM mode Active or Passive on an interface.

Default

```
passive
```

Format

```
link-oam mode { active | passive }
```

Mode

```
Port Configuration Mode
```

■ no link-oam mode

This command is used to set Link OAM mode to default.

Format

```
no link-oam mode
```

Mode

```
Port Configuration Mode
```

32.1.4. link-oam remote-loopback supported

This command is used to enable Link OAM remote loopback on the interface.

Default

```
none
```

Format

```
link-oam remote-loopback supported
```

Mode

```
Port Configuration Mode
```

■ no link-oam remote-loopback supported

This command is used to disable Link OAM remote loopback on the interface.

Format

```
no link-oam remote-loopback supported
```

Mode

```
Port Configuration Mod
```

32.1.5. link-oam mib-retrieval supported

This command is used to set Link OAM Mib retrieval support.

Default

```
disable
```

Format

```
link-oam mib-retrieval supported
```

Mode

```
Port Configuration Mode
```

■ no link-oam mib-retrieval supported

This command is used to set Link OAM Mib retrieval support to disabled.

Format

```
no link-oam mib-retrieval supported
```

Mode

```
Port Configuration Mode
```

32.1.6. link-oam link-monitor supported

This command is used to enable link monitoring support on interface.

Default

```
enable
```

Format

```
link-oam link-monitor supported
```

Mode

```
Port Configuration Mode
```

no link-oam link-monitor supported

This command is used to disable link monitoring support on interface.

Format

```
no link-oam link-monitor supported
```

Mode

```
Port Configuration Mod
```

32.1.7. link-oam link-monitor frame

This command is used to configure frame error event window and threshold that trigger an error-frame link event. “windows” Set the a window of time during which error frames are counted.*<1-60>* Duration of the monitoring period in terms of seconds. “threshold” Set a threshold in number of frames. *<0-4294967295>* Number of permissible errors frames in the period defined by the error window.

Default

```
default for window is 1 second,Default for threshold 0 frames
```

Format

```
link-oam link-monitor frame { [ window <1-60> ] [ threshold <0-4294967295> ] }
```

Mode

```
Port Configuration Mode
```

no link-oam link-monitor frame

This command is used to configure default window and threshold that trigger an error-frame link event.

Format

```
no link-oam link-monitor frame
```

Mode

```
Port Configuration Mode
```

32.1.8. link-oam link-monitor symbol-period

This command is used to configure window and thresholds for an error-symbol period that triggers an error-symbol period link event. “windows” Duration of the monitoring in terms of seconds.*<1-60>* Set window size in terms of seconds. “threshold” Number of permissible error symbols in the period defined by the error window. *<0-4294967295>* Threshold in number of symbols.

Default

```
default for error window 1 second,for threshold 0 symbols
```

Format

```
link-oam link-monitor symbol-period { [ window <1-60> ] [ threshold <0-4294967295> ] }
```

Mode

```
Port Configuration Mode
```

■ no link-oam link-monitor symbol-period

This command is used to configure default window and thresholds for an error-symbol period that triggers an error-symbol period link event.

Format

```
no link-oam link-monitor symbol-period
```

Mode

```
Port Configuration Mode
```

32.1.9. link-oam link-monitor frame-seconds

This command is used to configure frame-seconds summary window and thresholds for triggering an error-frame-seconds event. “windows” Configure window value.*<10-900>* Duration of the monitoring period in terms of seconds. “threshold” Configure threshold. *<1-900>* Number of permissible errors frames in the period defined by the error window.

Default

```
default window 60 seconds,Default threshold 1
```

Format

```
link-oam link-monitor frame-seconds { [ window <10-900> ] [ threshold <1-900> ] }
```

Mode

```
Port Configuration Mode
```

■ no link-oam link-monitor frame-seconds

This command is used to cancels the frame second summary window and window thresholds that trigger error frame second events.

Format

```
no link-oam link-monitor frame-seconds
```

Mode

```
Port Configuration Mode
```

32.2. show

32.2.1. show link-oam

This command is used to show Link OAM configuration, statistics, and status.

Default

```
none
```

Format

```
show link-oam { [ status ] [ link-monitor ] [ statistics ] } [ interface
<port_type_list> ]
```

Mode

```
User EXEC Mode
```

32.3. clear

32.3.1. clear link-oam statistics

This command is used to clear Link OAM statistics on interface.

Default

```
clear on all ports
```

Format

```
clear link-oam statistics [ interface <port_type_list> ]
```

Mode

```
User EXEC Mode
```

33. Link Aggregation Control Protocol (LACP)

Link Aggregation Control Protocol (LACP) is a network protocol implemented according to the IEEE 802.3 ad standard, designed to enhance link reliability and bandwidth by bundling multiple physical links into a single logical link. LACP is a type of dynamic link aggregation protocol that can automatically negotiate the establishment of aggregated connections across multiple ports, as well as automatically configure and maintain these connections. Through LACP, load balancing and redundant connections can be achieved, improving network transmission efficiency and fault tolerance.

33.1. lacp

33.1.1. lacp failover

This command is used to enable revertive of the aggregation group. This parameter only applies to LACP-enabled groups. It determines if the group will perform automatic link (re-)calculation when links with higher priority becomes available. "revertive" represents automatically revert to the primary path upon recovery, "non-revertive" represents do not automatically revert to the primary path upon recovery.

Default

```
disable
```

Format

```
lacp failover { revertive | non-revertive }
```

Mode

```
LLAG Mode
```

■ no lacp failover

This command is used to disable revertive of an aggregation group.

Format

```
no lacp failover [ revertive | non-revertive ]
```

Mode

```
LLAG Mode
```

33.1.2. lacp max-bundle

This command is used to configure max-bundle of an aggregation group. This parameter only applies to LACP-enabled groups. It determines the maximum number of active bundled LACP ports allowed in an aggregation. *<uint>* represents number of ports.

Default

```
the maximum is 16, and the default value varies depending on the device form factor
```

Format

```
lacp max-bundle <uint>
```

Mode

```
LLAG Mode
```

■ no lacp max-bundle

This command is used to reset max-bundle to default. *<uint>* represents number of ports.

Format

```
no lacp max-bundle [ <uint> ]
```

Mode

```
LLAG Mode
```

33.1.3. lacp system-priority

This command is used to configure the LACP system priority. The system priority can be configured through the user interface. The lower the value, the higher the system priority. *<1-65535>* represents priority value.

Default

```
32768
```

Format

```
lacp system-priority <1-65535>
```

Mode

```
Global Configuration Mode
```

■ no lacp system-priority

This command is used to reset system priority to default. *<1-65535>* represents priority value.

Format

```
no lacp system-priority <1-65535>
```

Mode

```
Global Configuration Mode
```

33.1.4. lacp

This command is used to enable LACP on an interface.

Default

```
enable
```

Format

```
lacp
```

Mode

```
Port Configuration Mode
```

■ no lacp

This command is used to disable LACP on an interface.

Format

```
no lacp
```

Mode

```
Port Configuration Mode
```

33.1.5. lacp timeout

This command is used to configure the LACP timeout. The Timeout controls the period between BPDU transmissions. "fast" will transmit LACP packets each second, while slow will wait for 30 seconds before sending a LACP packet.

Default

```
fast
```

Format

```
lacp timeout { fast | slow }
```

Mode

```
Port Configuration Mode
```

no lacp timeout

This command is used to reset the LACP timeout to fast.

Format

```
no lacp timeout { fast | slow }
```

Mode

```
Port Configuration Mode
```

33.1.6. lacp port-priority

This command is used to configure LACP priority of the port. If the number of LACP bundles is n, and there are n+1 ports participating in the negotiation, you can set the priority levels to allow the higher priority ports to become members of the aggregation group. Lower number means a higher priority. <*1-65535*> represents priority value.

Default

```
32768
```

Format

```
lacp port-priority <1-65535>
```

Mode

```
Port Configuration Mode
```

no lacp port-priority

This command is used to reset LACP priority of the port to default. <*1-65535*> represents priority value.

Format

```
no lacp port-priority <1-65535>
```

Mode

```
Port Configuration Mode
```

33.2. show

33.2.1. show lacp

This command is used to show LACP configuration/status. Use internal keyword to view Internal LACP configuration. Use neighbor keyword to view Neighbor LACP status. Use statistics keyword to view Internal LACP statistics. Use system-id keyword to view LACP system status.

Format

```
show lacp { internal | statistics | system-id | neighbor } [ details ]
```

Mode

```
User EXEC Mode
```

33.3. clear

33.3.1. clear lacp statistics

This command is used to clear all LACP statistics.

Format

```
clear lacp statistics
```

Mode

```
User EXEC Mode
```

34. LLDP

LLDP (Link Layer Discovery Protocol) is a Layer 2 Discovery protocol defined in IEEE 802.1ab. LLDP provides a standard method for link layer discovery, allowing the essential capabilities, management addresses, device identifiers, interface identifiers, and other information of the local device to be encapsulated into LLDP messages and transmitted to neighboring nodes. Upon receiving this information, the neighboring nodes store it in the form of a standard MIB (Management Information Base), which can be queried by an NMS (Network Management System) to assess the status of link communications.

34.1. lldp

34.1.1. lldp transmit

This command is used to enable transmission of LLDP frames.

Default

```
enable
```

Format

```
lldp transmit
```

Mode

```
Port Configuration Mode
```

■ no lldp transmit

This command is used to disable transmission of LLDP frames.

Format

```
no lldp transmit
```

Mode

```
Port Configuration Mode
```

34.1.2. lldp receive

This command is used to enable decoding of received LLDP frames.

Default

```
disable
```

Format

```
lldp receive
```

Mode

```
Port Configuration Mode
```

■ no lldp receive

This command is used to disable decoding of received LLDP frames.

Format

```
no lldp receive
```

Mode

```
Port Configuration Mode
```

34.1.3. lldp tlv-select

This command is used to enable transmission of optional system TLV. The transmission functions include the transmission of management address, port description, system capabilities, system description, and system name.

Default

```
enable
```

Format

```
lldp tlv-select { management-address | port-description | system-capabilities |
system-description | system-name }
```

Mode

```
Port Configuration Mode
```

■ no lldp tlv-select

This command is used to disable transmission of optional system TLV.

Format

```
no lldp tlv-select { management-address | port-description | system-capabilities |
system-description | system-name }
```

Mode

```
Port Configuration Mode
```

34.1.4. lldp cdp-aware

This command is used to configure if the interface shall be CDP aware (CDP discovery information is added to the LLDP neighbor table).

Default

```
none
```

Format

```
lldp cdp-aware
```

Mode

```
Port Configuration Mode
```

■ no lldp cdp-aware

This command is used to disable the CDP aware function of an interface.

Format

```
no lldp cdp-aware
```

Mode

```
Port Configuration Mode
```

34.1.5. lldp holdtime

This command is used to set LLDP Tx interval (The time between each LLDP frame transmitted in seconds).

Default

```
4
```

Format

```
lldp holdtime <2-10>
```

Mode

```
Global Configuration Mode
```

no lldp holdtime

This command is used to delete LLDP Tx interval.

Format

```
no lldp holdtime
```

Mode

```
Global Configuration Mode
```

34.1.6. lldp transmission-delay

This command is used to set LLDP transmission-delay. LLDP transmission delay (the amount of time that the transmission of LLDP frames will delayed after LLDP configuration has changed) in seconds.

Default

```
2
```

Format

```
lldp transmission-delay <1-8192>
```

Mode

```
Global Configuration Mode
```

no lldp transmission-delay

This command is used to delete LLDP transmission-delay.

Format

```
no lldp transmission-delay
```

Mode

```
Global Configuration Mode
```

34.1.7. lldp reinit

This command is used to set LLDP Tx re-initialization delay in seconds.

Default

```
2
```

Format

```
lldp reinit <1-10>
```

Mode

```
Global Configuration Mode
```

no lldp reinit

This command is used to delete LLDP Tx re-initialization delay in seconds.

Format

```
no lldp reinit
```

Mode

```
Global Configuration Mode
```

34.1.8. lldp timer

This command is used to sets LLDP TX interval (The time between each LLDP frame transmitted in seconds).

Default

30

Format

lldp timer *<5-32768>*

Mode

Global Configuration Mode

■ no lldp timer

This command is used to set LLDP TX interval to default.

Format

no lldp timer

Mode

Global Configuration Mode

34.1.9. lldp trap

This command is used to sent SNMP trap shall be emitted when the LLDP neighbor table changes for the interface.

Default

disable

Format

lldp trap

Mode

Port Configuration Mode

■ no lldp trap

This command is used to disable the sending of SNMP traps.

Format

no lldp trap

Mode

Port Configuration Mode

34.2. lldp med

34.2.1. lldp med fast

This command is used to specifies the fast start repeat count for LLDP-MED.

Default

4

Format

lldp med fast *<1-10>*

Mode

Global Configuration Mode

no lldp med fast

This command is used to specifies the fast start repeat count for LLDP-MED.

Format

```
no lldp med fast
```

Mode

```
Global Configuration Mode
```

34.2.2. lldp med datum

This command is used to specifies the geodetic system type. The optional parameters represent the Mean lower low water datum 1983, North American vertical datum 1983, and World Geodetic System 1984.

Default

```
wgs84
```

Format

```
lldp med datum { nad83-mllw | nad83-navd88 | wgs84 }
```

Mode

```
Global Configuration Mode
```

no lldp med datum

This command is used to delete the geodetic system type.

Format

```
no lldp med datum
```

Mode

```
Global Configuration Mode
```

34.2.3. lldp med location-tlv

This command is used to assign the geographic coordinate value for the device. Also, the ELIN identification could be specified. "elin-addr <*dword25*>" represents emergency call service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling. Emergency Location Identification Number, (e.g. E911 and others), such as defined by TIA or NENA. "latitude { north | south } <*word8*>" represents setting latitude direction to north or south latitude degrees. "longitude { east | west } <*word9*>" represents setting longitude direction to west or east longitude degrees. "altitude { meters | floors } <*word11*>" represents specify the altitude in meters or floors altitude value, valid range -2097151.9 to 2097151.9.

Default

```
none
```

Format

```
lldp med location-tlv { elin-addr <dword25> | latitude { north | south } <word8> |
longitude { east | west } <word9> | altitude { meters | floors } <word11> }
```

Mode

```
Global Configuration Mode
```

no lldp med location-tlv

This command is used to delete the geographic coordinate value for the device.

Format

```
no lldp med location-tlv { elin-addr |latitude | longitude | altitude }
```

Mode

```
Global Configuration Mode
```

34.2.4. lldp med location-tlv civil-addr

This command is used to specifies civic location information. The optional parameters represent the two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US. National subdivisions (state, canton, region, province, prefecture), county, parish, gun (Japan), district. City division, borough, city district, ward, chou (Japan). Neighborhood, block. Street - Example: Oxford Street. Leading street direction - Example: N. Trailing street suffix - Example: SW. Street suffix - Example: Ave, Platz. House number - Example: 21. House number suffix - Example: A, 1/2. Landmark or vanity address - Example: Columbia University. Additional location info - Example: South Wing. Name (residence and office occupant) - Example: John Doe. Postal/zip code - Example: 2791. Building (structure) - Example: Low Library. Unit (Apartment, suite) - Example: Apt 42. Floor - Example: 4. Room number - Example: 450F. Place type - Example: Office. Postal community name - Example: Leonia. Post office box (P.O. BOX) - Example: 12345. Additional code - Example: 1320300003. Value for the corresponding selected civic address.

Default

none

Format

lldp med location-tlv civic-addr { { country *<line2>* } | { state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code } *<line250>* }

Mode

Global Configuration Mode

no lldp med civic-addr

This command is used to delete civic location information.

Format

no lldp med location-tlv civic-addr { country | state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code }

Mode

Global Configuration Mode

34.2.5. lldp med media-vlan-policy

This command is used to create a network policy that can be assigned to an interface for a specific kind of application. *<0-31>* represents policy id for the policy which is created. The optional parameters represent create a voice policy. Create a voice signaling policy. Create a guest voice signaling policy. Create a guest voice policy. Create a soft phone voice policy. Create a video conferencing policy. Create a streaming video policy. Create a video signaling policy. The policy uses untagged frames. The policy uses tagged frames, *<vlan_id>* represents the VLAN the policy uses tagged frames. Layer 2 priority. If not given then L2 priority value is set to 0, *<0-7>* represents Priority 0-7. Differentiated Services Code Point. If not given then DSCP value is set to 0, *<0-63>* represents DSCP value 0-63.

Default

none

Format

lldp med media-vlan-policy *<0-31>* { voice | voice-signaling | guest-voice-signaling | guest-voice | softphone-voice | video-conferencing | streaming-video | video-signaling } { untagged | tagged *<vlan_id>* [l2-priority *<0-7>*] } [dscp *<0-63>*]

Mode

Global Configuration Mode

no lldp med media-vlan-policy

This command is used to delete a network policy.

Format

```
no lldp med media-vlan-policy policy-id
```

Mode

```
Global Configuration Mode
```

34.2.6. lldp med type

This command is used to select either Network Connectivity Device or an Endpoint Device as the interface role.

Default

```
none
```

Format

```
lldp med type { [ connectivity | end-point ] }
```

Mode

```
Port Configuration Mode
```

no lldp med type

This command is used to delete a network policy.

Format

```
no lldp med type
```

Mode

```
Port Configuration Mode
```

34.2.7. lldp med transmit-tlv

This command is used to specify the optional TLVs to be transmitted. "capabilities" represents enable transmission of the optional capabilities TLV, "location" represents enable transmission of the optional location TLV, "network-policy" represents enable transmission of the optional network-policy TLV, "poe" represents runtime.

Default

```
none
```

Format

```
lldp med transmit-tlv [ capabilities ] [ location ] [ network-policy ] [ poe ]
```

Mode

```
Port Configuration Mode
```

no lldp med transmit-tlv

This command is used to delete the optional TLVs to be transmitted.

Format

```
no lldp med transmit-tlv [ capabilities ] [ location ] [ network-policy ] [ poe ]
```

Mode

```
Port Configuration Mode
```

34.2.8. lldp med media-vlan policy-list

This command is used to specify the media policy that an interface will apply. <*range_list*> represents policies to assign to the interface.

Default

none

Format

lldp med media-vlan policy-list <*range_list*>

Mode

Port Configuration Mode

no lldp med media-vlan policy-list

This command is used to delete the media policy.

Format

no lldp med media-vlan policy-list [<*range_list*>]

Mode

Port Configuration Mode

34.3. show

34.3.1. show lldp

This command is used to show lldp configuration/status. "eee" represents display LLDP local and neighbor EEE information, "neighbors" represents display LLDP neighbors information, "preempt" represents display LLDP local and neighbor preempt information, "statistics" represents display LLDP statistics information, "interface <*port_type_list*>" represents interface to display, "brief" represents brief LLDP neighbors information.

Format

show lldp { [eee | neighbors | preempt | statistics] [interface <*port_type_list*>] [brief] }

Mode

User EXEC Mode

34.3.2. show lldp med

This command is used to show lldp med configuration/status. "media-vlan-policy" represents display media VLAN policies, <*0~31*> represents list of policies. "remote-device" display remote device LLDP-MED neighbors information, "interface <*port_type_list*>" represents interface to display.

Format

show lldp med { [media-vlan-policy [<*0~31*>] | remote-device [interface <*port_type_list*>]] }

Mode

User EXEC Mode

35. Loop Protection

Loop Protection is a network feature used to detect and prevent the infinite looping of network data packets caused by loops. When there is a loop in the network, packets can circulate endlessly within the loop, leading to network congestion and degraded performance. Loop Protection addresses this issue by detecting duplicate packets on the loop path and preventing them from further propagation. When a loop path is detected, Loop Protection actively discards the duplicate packets, thereby avoiding the adverse effects of network loops. This helps improve network reliability and performance and protects the network from the disruptions caused by loop issues.

35.1. loop-protect

35.1.1. loop-protect (global)

This command is used to add globally enable the loop protections.
Loop-protect: globally enable the loop protections.
Transmit-time: interval of each loop protection to send PDUs to each port. The range is 1-10s.
Shutdown-time: The period for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds. A value of zero will keep a port disabled.

Default

```
none
```

Format

```
loop-protect [ transmit-time | shutdown-time ]
```

Mode

```
Global Configuration Mode
```

no loop-protect

This command is used to delete loop-protect settings.

Format

```
no loop-protect [ transmit-time | shutdown-time ]
```

Mode

```
Global Configuration Mode
```

35.1.2. loop-protect (port)

This command is used to add loop protection on the port. loop-protect: in the mode of port configuration,enable loop protection on the port. "action" represents optional values are log, shutdown port, log and shutdown port. "tx-mode" represents control whether the port is automatically generate loop protection PDU, or just passively looking for loop protection PDU.

Default

```
none
```

Format

```
loop-protect [ action | tx-mode ]
```

Mode

```
Port Configuration Mode
```

no loop-protect

This command is used to delete loop-protect settings.

Format

```
no loop-protect [ action | tx-mode ]
```

Mode

```
Port Configuration Mode
```

35.2. show

35.2.1. show loop-protect

This command is used to show loop-protect configuration/status.

Format

```
show loop-protect [ interface <port_type_list> ]
```

Mode

```
User EXEC Mode
```

36. MAC

Switches forward and filter network packets based on MAC addresses. When a packet arrives at a switch, it learns the source MAC address and associates it with the corresponding port, thus building a MAC address table. Later, when data needs to be sent to a specific device, the switch looks up the MAC address table, finds the corresponding port, and sends the packet only to the port where the destination device is located. This effectively prevents redundant packet transmission in the network. This MAC-based forwarding method allows for more efficient transmission of data within a local area network, reducing network congestion and conflicts, and improving network performance and security.

36.1. mac address-table

36.1.1. mac address-table learning

This command is used to configure the port-based MAC learning mode to learning, "secure" represents port secure mode.

Default

```
enable
```

Format

```
mac address-table learning [ secure ]
```

Mode

```
Port Configuration Mode
```

no mac address-table learning

This command is used to delete the MAC learning mode.

Format

```
no mac address-table learning [ secure ]
```

Mode

```
Port Configuration Mode
```

36.1.2. mac address-table learning vlan

This command is used to configure the VLAN-based MAC learning mode to learning.

Default

```
enable
```

Format

```
mac address-table learning vlan <vlan_list>
```

Mode

```
Global Configuration Mode
```

no mac address-table learning

This command is used to delete the MAC learning mode.

Format

```
no mac address-table learning vlan <vlan_list>
```

Mode

```
Global Configuration Mode
```

36.1.3. mac address-table aging-time

This command is used to configure the mac address aging time, *<0,10-1000000>* represents aging time in seconds.

Default

300s

Format

mac address-table aging-time *<0,10-1000000>*

Mode

Global Configuration Mode

■ no mac address-table aging-time

This command is used to delete the mac address aging time.

Format

no mac address-table aging-time *<0,10-1000000>*

Mode

Global Configuration Mode

36.1.4. mac address-table static

This command is used to adding a static MAC address entry. <*mac_addr*> represents a 48-bit MAC address: xx:xx:xx:xx:xx:xx, <*vlan_id*> represents VLAN IDs 1-4095, and <*port_type_list*> represents the IDs of the ports.

Default

none

Format

mac address-table static *<mac_addr>* vlan *<vlan_id>* interface *<port_type_list>*

Mode

Global Configuration Mode

■ no mac address-table static

This command is used to delete a static MAC address entry.

Format

no mac address-table static *<mac_addr>* vlan *<vlan_id>* interface *<port_type_list>*

Mode

Global Configuration Mode

36.2. show

36.2.1. show mac address-table

This command is used to display the MAC table. It can be filtered and displayed based on criteria such as address, aging time, configuration, count, interface, learning, static, vlan.

Format

show mac address-table [conf | static | aging-time | { { learning | count } [interface <*port_type_list*> | vlan <*vlan_id*>] } | { address <*mac_addr*> [vlan <*vlan_id*>] } | vlan <*vlan_id*> | interface <*port_type_list*>]

Mode

User EXEC Mode

37. Mirroring

Mirroring is divided into local and remote mirroring, allowing administrators to replicate the traffic from one or more switch ports to another specific monitoring port. Through this method, administrators can monitor the replicated traffic in real time, including network communications, packet transfers, and protocol analysis.

37.1. monitor

37.1.1. monitor session

This command is used to configure the relevant information of the mirroring port. You can configure the target interface, or the reflector port under the remote vlan, and also configure the source interface to monitor bidirectional data, only listening to the sending or only listening to the receiving data. You can also configure the remote vlan and cpu of the source interface to monitor bidirectional data, only listening to the sending and only listening to the receiving data. The option reset-after-restart is to enable the mirroring function, but it will be reset after restart.

Default

```
none
```

Format

```
monitor session <uint> [ destination { interface <port_type_list> | remote vlan <vlan_id> reflector-port <port_type_id> } | source { interface <port_type_list> [ both | rx | tx ] | remote vlan <vlan_id> | vlan <vlan_list> | cpu [ both | rx | tx ] } | reset-after-restart ]
```

Mode

```
Global Configuration Mode
```

no monitor session

This command is used to delete or disable the mirroring configuration.

Format

```
no monitor session <uint> [ destination { interface <port_type_list> | remote } | source { interface <port_type_list> [ both | rx | tx ] | remote | vlan <vlan_list> | cpu [ both | rx | tx ] } ]
```

Mode

```
Global Configuration Mode
```

37.2. show

37.2.1. show monitor

This command is used to show mirroring configuration.

Format

```
show monitor [ session { <uint> | all | remote } ]
```

Mode

```
User EXEC Mode
```

38. MRP

MRP (Multiple Registration Protocol) is a function used in Ethernet networks to provide faster network convergence in the event of link or node failures. Based on the principles of the IEEE 802.1Q standard, MRP aims to provide a method for nodes to register and receive updates about the network status and to quickly update their forwarding tables based on changes in network topology. It is designed to complement Rapid Spanning Tree Protocol (RSTP) or Multiple Spanning Tree Protocol (MSTP) to achieve faster convergence in certain network topologies.

38.1. role

38.1.1. role

This command is used to set the role of this node for this ring instance.

Default

```
none
```

Format

```
role { mrc | mrm | mra }
```

Mode

```
MRP Configuration Mode
```

■ no role

This command is used to set the role of this node to be the default role.

Format

```
no role
```

Mode

```
MRP Configuration Mode
```

38.2. name

38.2.1. name

This command is used to set a domain name for this media-redundancy instance for easy identification.

Default

```
none
```

Format

```
name <string1-240>
```

Mode

```
MRP Configuration Mode
```

■ no name

This command is used to clear the domain name of this media-redundancy instance.

Format

```
no name
```

Mode

```
MRP Configuration Mode
```

38.3. uuid

38.3.1. uuid

This command is used to set a UUID for this media-redundancy instance. Also used in PDUs.

Default

```
none
```

Format

```
uuid <string36-36>
```

Mode

```
MRP Configuration Mode
```

no uuid

This command is used to restore the default UUID.

Format

```
no uuid
```

Mode

```
MRP Configuration Mode
```

38.4. oui

38.4.1. oui

This command is used to set the OUI used in MRP_Option TLVs.

Default

```
none
```

Format

```
oui { default | siemens | custom <oui> }
```

Mode

```
MRP Configuration Mode
```

no oui

This command is used to set the OUI used in MRP_Option TLVs to default (the switch's own OUI).

Format

```
no oui
```

Mode

```
MRP Configuration Mode
```

38.5. port1

38.5.1. port1 interface

This command is used to assign an interface to ring port1.

Default

```
none
```

Format

```
port1 interface <port_type_id>
```

Mode

```
MRP Configuration Mode
```

■ no port1 interface

This command is used to unassign port1's interface.

Format

```
no port1 interface
```

Mode

```
MRP Configuration Mode
```

38.5.2. port1 sf-trigger

This command is used to choose whether port1's interface link state or a MEP installed on port1's interface is used as signal-fail trigger.

Default

```
none
```

Format

```
port1 sf-trigger { link | { mep domain <kword1-15> service <kword1-15> mep-id
<1-8191> } }
```

Mode

```
MRP Configuration Mode
```

■ no port1 sf-trigger

This command is used to set port1's signal fail trigger to default (link).

Format

```
no port1 sf-trigger
```

Mode

```
MRP Configuration Mode
```

38.6. port2

38.6.1. port2 interface

This command is used to assign an interface to ring port2.

Default

```
none
```

Format

```
port2 interface <port_type_id>
```

Mode

```
MRP Configuration Mode
```

■ no port2 interface

This command is used to unassign port2's interface.

Format

```
no port2 interface
```

Mode

```
MRP Configuration Mode
```

38.6.2. port2 sf-trigger

This command is used to choose whether port2's interface link state or a MEP installed on port2's interface is used as signal-fail trigger.

Default

```
none
```

Format

```
port2 sf-trigger { link | { mep domain <kword1-15> service <kword1-15> mep-id
<1-8191> } }
```

Mode

```
MRP Configuration Mode
```

■ no port2 sf-trigger

This command is used to set port2's signal fail trigger to default (link).

Format

```
no port2 sf-trigger
```

Mode

```
MRP Configuration Mode
```

38.7. control-vlan

38.7.1. control-vlan

This command is used to set the media-redundancy instance's VLAN used in MRP PDUs transmitted on both ring ports. Use no-form to force untagged.

Default

```
none
```

Format

```
control-vlan <vlan_id>
```

Mode

```
MRP Configuration Mode
```

■ no control-vlan

This command is used to use untagged MRP PDUs on the ring ports.

Format

```
no control-vlan
```

Mode

```
MRP Configuration Mode
```

38.8. recovery-profile

38.8.1. recovery-profile

This command is used to select a recovery profile, adhering to the timing parameters of Table 59 and 60 of IEC 62439-2:2016.

Default

```
none
```

Format

```
recovery-profile { 10ms | 30ms | 200ms | 500ms }
```

Mode

```
MRP Configuration Mode
```

■ no recovery-profile

This command is used to select the default recovery profile.

Format

```
no recovery-profile
```

Mode

```
MRP Configuration Mode
```

38.9. mrm

38.9.1. mrm priority

This command is used to select the MRM/MRA priority.

Default

```
none
```

Format

```
mrm priority <uint16>
```

Mode

```
MRP Configuration Mode
```

no mrm priority

This command is used to set the MRM/MRA priority to its default.

Format

```
no mrm priority
```

Mode

```
MRP Configuration Mode
```

38.9.2. mrm react-on-link-change

This command is used to indicates whether the MRM reacts on MRP_LinkDown PDUs. Corresponds to the standard's MRP_REACT_ON_LINK_CHANGE.

Default

```
none
```

Format

```
mrm react-on-link-change
```

Mode

```
MRP Configuration Mode
```

38.10. interconnection

38.10.1. interconnection role

This command is used to set the interconnection role of this node for this ring instance.

Default

```
none
```

Format

```
interconnection role { mic | mim | none }
```

Mode

```
MRP Configuration Mode
```

no interconnection role

This command is used to disable interconnection functionality on this node. Corresponds to “interconnection role none”.

Format

```
no interconnection role
```

Mode

```
MRP Configuration Mode
```

38.10.2. interconnection mode

This command is used to set the interconnection mode of this node for this ring instance.

Default

```
none
```

Format

```
interconnection mode { link-check | ring-check }
```

Mode

```
MRP Configuration Mode
```

no interconnection mode

This command is used to set the interconnection mode to its default.

Format

```
no interconnection mode
```

Mode

```
MRP Configuration Mode
```

38.10.3. interconnection id

This command is used to set an ID for this interconnection domain.

Default

```
none
```

Format

```
interconnection id <uint16>
```

Mode

```
MRP Configuration Mode
```

no interconnection id

This command is used to use a default ID for this interconnection domain.

Format

```
no interconnection id
```

Mode

```
MRP Configuration Mode
```

38.10.4. interconnection name

This command is used to set a domain name for this media-redundancy interconnection instance for easy identification.

Default

```
none
```

Format

```
interconnection name <string1-240>
```

Mode

```
MRP Configuration Mode
```

■ no interconnection name

This command is used to clear the interconnection name of this media-redundancy instance.

Format

```
no interconnection name
```

Mode

```
MRP Configuration Mode
```

38.10.5. interconnection interface

This command is used to assign an interface to the interconnection port.

Default

```
none
```

Format

```
interconnection interface <port_type_id>
```

Mode

```
MRP Configuration Mode
```

■ no interconnection interface

This command is used to unassign interconnection interface.

Format

```
no interconnection interface
```

Mode

```
MRP Configuration Mode
```

38.10.6. interconnection sf-trigger

This command is used to choose whether the interconnection port's link state or a MEP installed on the interconnection port is used as signal-fail trigger.

Default

```
none
```

Format

```
interconnection sf-trigger { link | { mep domain <kword1-15> service <kword1-15>
mep-id <1-8191> } }
```

Mode

```
MRP Configuration Mode
```

no interconnection sf-trigger

This command is used to set the interconnection port's signal fail trigger to default (link).

Format

```
no interconnection sf-trigger
```

Mode

```
MRP Configuration Mode
```

38.10.7. interconnection control-vlan

This command is used to set the media-redundancy instance's VLAN used in MRP PDUs transmitted on the interconnection port. Use no-form to force untagged.

Default

```
none
```

Format

```
interconnection control-vlan <vlan_id>
```

Mode

```
MRP Configuration Mode
```

no interconnection control-vlan

This command is used to use untagged MRP PDUs on the interconnection port.

Format

```
no interconnection control-vlan
```

Mode

```
MRP Configuration Mode
```

38.10.8. interconnection recovery-profile

This command is used to select an interconnection recovery profile, adhering to the timing parameters of Table 61 and 62 of IEC 62439-2:2016.

Default

```
none
```

Format

```
interconnection recovery-profile { 200ms | 500ms }
```

Mode

```
MRP Configuration Mode
```

no interconnection recovery-profile

This command is used to select the default recovery profile for the interconnection.

Format

```
no interconnection recovery-profile
```

Mode

```
MRP Configuration Mode
```

38.11. admin-state

38.11.1. admin-state

This command is used to enable or disable this media-redundancy instance.

Default

```
none
```

Format

```
admin-state { enable | disable }
```

Mode

```
MRP Configuration Mode
```

38.12. mrp

38.12.1. mrp timers

This command is used to configure MRP protocol timer parameters. IEEE 802.1Q-2014, clause 10.7. Join-time, Leave-time and LeaveAll-time are protocol parameters in units of centi-seconds, (i.e., in 1/100 seconds). <*1-20*> represents Join-time value. <*60-600*> represents Leave-time value. <*1000-5000*> represents LeaveAll-time value.

Default

```
join-time : 20
leave-time : 60
leaveAll-time : 1000
```

Format

```
mrp timers { [ join-time <1-20> ] [ leave-time <60-600> ] [ leave-all-time
<1000-5000> ] }
```

Mode

```
Port Configuration Mode
```

38.12.2. mrp timers default

This command is used to set all MRP timers to their default values.

Format

```
mrp timers default
```

Mode

```
Port Configuration Mode
```

38.12.3. mrp periodic

This command is used to enable MRP Periodic Transmission on the port.

Default

```
disable
```

Format

```
mrp periodic
```

Mode

```
Port Configuration Mode
```

no mrp periodic

This command is used to disable MRP Periodic Transmission on the port.

Format

```
no mrp periodic
```

Mode

```
Port Configuration Mode
```

38.13. show

38.13.1. show media-redundancy

This command is used to show the state or counters of one or more media-redundancy instances.

Default

```
none
```

Format

```
show media-redundancy [ <range_list> ] { status | statistics } [ details ]
```

Mode

```
User EXEC Mode
```

38.14. clear

38.14.1. clear media-redundancy statistics

This command is used to clear the counters of one or more media-redundancy instances.

Default

```
none
```

Format

```
clear media-redundancy [ <range_list> ] statistics
```

Mode

```
User EXEC Mode
```

39. MSTP

The Multiple Spanning Tree Protocol (MSTP) is used to create a loop-free logical topology among Ethernet switches in a Local Area Network (LAN). Its primary purpose is to prevent problems such as broadcast storms and potential instability in the MAC address table that can arise from having redundant paths configured in the network. In typical LAN design, redundant paths are implemented to provide fault tolerance and prevent single points of failure.

39.1. spanning-tree

39.1.1. spanning-tree mode

This command is used to add bridge basic settings. "stp" represents 802.1D Spanning Tree. "rstp" represents Rapid Spanning Tree (802.1w). "mstp" represents Multiple Spanning Tree (802.1s).

Default

```
mode : mstp
```

Format

```
spanning-tree mode { [ stp | rstp | mstp ] }
```

Mode

```
Global Configuration Mode
```

no spanning-tree mode

This command is used to delete bridge settings.

Format

```
no spanning-tree mode { [ stp | rstp | mstp ] }
```

Mode

```
Global Configuration Mode
```

39.1.2. spanning-tree edge

This command is used to add bridge advanced settings. "bpdu-filter" represents enable BPDU filter (stop BPDU tx/rx). "bpdu-guard" represents enable BPDU guard.

Default

```
disable
```

Format

```
spanning-tree edge { [ bpdu-filter | bpdu-guard ] }
```

Mode

```
Global Configuration Mode
```

no spanning-tree edge

This command is used to delete bridge settings.

Format

```
no spanning-tree edge { [ bpdu-filter | bpdu-guard ] }
```

Mode

```
Global Configuration Mode
```

39.1.3. spanning-tree recovery interval

This commond is used to set the port error recovery and port error recovery timout.<*30-86400*> Range in seconds.

Default

```
disable
```

Format

```
spanning-tree recovery interval <30-86400>
```

Mode

```
Global Configuration Mode
```

■ no spanning-tree recovery interval

This command is used to delete the port error recovery and port error recovery timout.

Format

```
no spanning-tree recovery interval
```

Mode

```
Global Configuration Mode
```

39.1.4. spanning-tree mst name (revision)

This command is used to add MSTI Mapping setings. By default, all VLAN Ids are mapped to the Common and Internal Spanning Tree (CIST). If the protocol version is set to MSTP, then a VLAN ID can be mapped to one out of 8 spanning trees, where CIST is one. The 7 others are called MSTI1、…、MSTI7. A MSTI configuration also has a name and revision. All these values have to be identical on the switches in the network. Otherwise the configuration will not take effect. <*word32*> Name of the bridge. <*0-65535*> Revision number.

Default

```
none
```

Format

```
spanning-tree mst name <word32> revision <0-65535>
```

Mode

```
Global Configuration Mode
```

■ no spanning-tree mst

This command is used to delete MSTI Mapping settings.

Format

```
no spanning-tree mst name <word32>
```

Mode

```
Global Configuration Mode
```

39.1.5. spanning-tree mst name (priority)

This command is used to increase the priority of an MSTI. Each MSTI and CIST can be assigned a priority. The smaller the value, the higher the priority. A Bridge Identifier is constructed per CIST, MSTI1、...、MSTI7, the bridge priority number. This is concatenated with the MAC address of the switch. In this way the bridge Identifier is unique. A low bridge Identifier indicates a higher priority. A high priority means that the switch tends to be the root of the spanning tree. If two switches have the same bridge priority, then for example, setting MSTI1 priority higher, or setting MSTI2 lower, makes one switch tends the root. <*0-7*> instance (CIST=0, MSTI1=1...).<*0-61440*> represents the STP bridge priority. Supported values are 0 / 4096 / 8192 / 12288 / 16384 / 20480 / 24576 / 28672 / 32768 / 36864 / 40960 / 45056 / 49152 / 53248 / 57344 / 61440 i.e divisible by 4096. Default value is 32768.

Default

```
32768
```

Format

```
spanning-tree mst name <0-7> priority <0-61440>
```

Mode

```
Global Configuration Mode
```

■ no spanning-tree mst

This command is used to delete MSTI Mapping settings.

Format

```
no spanning-tree mst name <ConfigurationName> priority <priority>
```

Mode

```
Global Configuration Mode
```

39.1.6. spanning-tree

This command is used to enable for taking part in the spanning tree protocol with the following command.

Default

```
enable
```

Format

```
spanning-tree
```

Mode

```
Port Configuration Mode
```

■ no spanning-tree

This command is used to disable for taking part in the spanning tree protocol with the following command.

Format

```
no spanning-tree
```

Mode

```
Port Configuration Mode
```

39.1.7. spanning-tree mst

This command is used to set the path cost and priority.

Default

```
cost: Disabled
port-priority: 128
```

Format

```
spanning-tree mst <0-7> { [ cost <Cost> | port-priority <Priority> ] }
```

Mode

```
Port Configuration Mode
```

■ no spanning-tree mst

This command is used to delete the path cost and priority.

Format

```
no spanning-tree mst { [ cost | port-priority ] }
```

Mode

```
Port Configuration Mode
```

39.1.8. spanning-tree (edge)

This commond controls how a port is declared to be an edge port or not. An edge port is a port which is not connected to a bridge. If auto edge is enabled, then the port determines whether it is an edge port by registering if BPDUs are received on that port. The admin edge determines what the port should start as, being edge or not, until auto edge if enabled, then change.

Default

```
edge: Non-Edge
auto-edge: Enabled
```

Format

```
spanning-tree { [ edge | auto-edge ] }
```

Mode

```
Port Configuration Mode
```

■ no spanning-tree

This command is used to delete the setting.

Format

```
no spanning-tree { [ edge | auto-edge ] }
```

Mode

```
Port Configuration Mode
```

39.1.9. spanning-tree (restricted)

If restricted role is enabled it causes the port not to be selected as root port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an alternate port after the root port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network to influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.
If restricted TCN is enabled it causes the port not to propagate received topology change notifications and topology changes to other ports. If set, it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

Default

```
restricted-role: Disabled
restricted-tcn: Disabled
```

Format

```
spanning-tree { [ restricted-role | restricted-tcn ] }
```

Mode

```
Port Configuration Mode
```

no spanning-tree

This command is used to delete the setting.

Format

```
no spanning-tree { [ restricted-role | restricted-tcn ] }
```

Mode

```
Port Configuration Mode
```

39.1.10. spanning-tree bpdu-guard

If enabled it causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port edge status does not affect this setting.

Default

```
disable
```

Format

```
spanning-tree bpdu-guard
```

Mode

```
Port Configuration Mode
```

no spanning-tree bpdu-guard

This command is used to delete the setting.

Format

```
no spanning-tree bpdu-guard
```

Mode

```
Port Configuration Mode
```

39.1.11. spanning-tree link-type

This command is used set the link to point-to-point. "auto" represents auto detect. "point-to-point" represents forced to point-to-point. "shared " represents forced to shared.

Default

```
auto
```

Format

```
spanning-tree link-type { [ auto | point-to-point | shared ] }
```

Mode

```
Port Configuration Mode
```

■ no spanning-tree link-type

This command is used to delete the setting.

Format

```
no spanning-tree link-type
```

Mode

```
Port Configuration Mode
```

39.1.12. spanning-tree transmit hold-count

This command is used to set the maximum number of BPDUs (Bridge Protocol Data Units) transmitted per second. The valid range is 1-10.

Default

```
6
```

Format

```
spanning-tree transmit hold-count <1-10>
```

Mode

```
Global Configuration Mode
```

■ no spanning-tree transmit hold-count

This command is used to reset the maximum number of BPDUs (Bridge Protocol Data Units) transmitted per second to the default value.

Format

```
no spanning-tree transmit hold-count
```

Mode

```
Global Configuration Mode
```

39.1.13. spanning-tree mst hello-time

This command is used to set the MSTP bridge hello time. The valid range is 1-10.

Default

```
2
```

Format

```
spanning-tree mst hello-time <1-10>
```

Mode

```
Global Configuration Mode
```

no spanning-tree mst hello-time

This command is used to reset the MSTP bridge hello time to the default value.

Format

```
no spanning-tree mst hello-time
```

Mode

```
Global Configuration Mode
```

39.1.14. spanning-tree mst max-hops

This command is used to set the MSTP bridge max hop count. The valid range is 6-40.

Default

```
20
```

Format

```
spanning-tree mst max-hops <6-40>
```

Mode

```
Global Configuration Mode
```

no spanning-tree mst max-hops

This command is used to reset the MSTP bridge max hop count to the default value.

Format

```
no spanning-tree mst max-hops
```

Mode

```
Global Configuration Mode
```

39.1.15. spanning-tree mst max-age

This command is used to set the max bridge age before timeout. The max age valid range is 6-40, forward-time <*4-30*> represents forward delay time.

Default

```
max-age: 20
forward-time: 15
```

Format

```
spanning-tree mst max-age <6-40> [ forward-time <4-30> ]
```

Mode

```
Global Configuration Mode
```

no spanning-tree mst max-age

This command is used to reset the max bridge age before timeout to the default value.

Format

```
no spanning-tree mst max-age
```

Mode

```
Global Configuration Mode
```

39.1.16. spanning-tree edge bpdu-filter

This command is used to enable BPDU filter (stop BPDU tx/rx).

Default

```
disable
```

Format

```
spanning-tree edge bpdu-filter
```

Mode

```
Global Configuration Mode
```

■ no spanning-tree edge bpdu-filter

This command is used to disable BPDU filter (stop BPDU tx/rx).

Format

```
no spanning-tree edge bpdu-filter
```

Mode

```
Global Configuration Mode
```

39.1.17. spanning-tree edge bpdu-guard

This command is used to enable edge BPDU guard.

Default

```
disable
```

Format

```
spanning-tree edge bpdu-guard
```

Mode

```
Global Configuration Mode
```

■ no spanning-tree edge bpdu-guard

This command is used to disable edge BPDU guard.

Format

```
no spanning-tree edge bpdu-guard
```

Mode

```
Global Configuration Mode
```

39.1.18. spanning-tree mst priority

This command is used to set the priority of the instance, *<0-7>* represents instance (CIST=0, MSTI1=1...), *<0-61440>* represents the priority of the instance.

Default

```
32768
```

Format

```
spanning-tree mst <0-7> priority <0-61440>
```

Mode

```
Global Configuration Mode
```

no spanning-tree mst priority

This command is used to delete instance.

Format

```
no spanning-tree mst <0-7> priority
```

Mode

```
Global Configuration Mode
```

39.1.19. spanning-tree mst vlan

The following command line is used to set up Multiple Spanning Tree instances and the mapping relationship with VLANs. *<0-7>* represents instance (CIST=0, MSTI1=1...), *<vlan_list>* represents the range of VLANs.

Default

```
all VLANs are mapped to the CIST
```

Format

```
spanning-tree mst <0-7> vlan <vlan_list>
```

Mode

```
Global Configuration Mode
```

no spanning-tree mst vlan

This command is used to restore the mapping of VLANs to the CIST under Multiple Spanning Tree instances.

Format

```
no spanning-tree mst <0-7> vlan
```

Mode

```
Global Configuration Mode
```

39.1.20. spanning-tree mst te vlan

The following command is used to set the VLAN list of traffic engineering. *<vlan_list>* represents the range of VLANs.

Default

```
0
```

Format

```
spanning-tree mst te vlan <vlan_list>
```

Mode

```
Global Configuration Mode
```

no spanning-tree mst te vlan

This command is used to delete the VLAN list of traffic engineering.

Format

```
no spanning-tree mst te vlan
```

Mode

```
Global Configuration Mode
```

39.2. show

39.2.1. show spanning-tree

This command is used to show spanning-tree configuration/status. "active" represents STP active interfaces. "detailed" represents STP statistics. "interface" represents choose port. "mst" represents multiple STP. "summary" represents STP summary.

Format

```
Show spanning-tree { [ active | detailed | interface | mst | summary ] }
```

Mode

```
User EXEC Mode
```

40. MVR

MVR (Multicast VLAN Registration) is primarily used to efficiently manage and transmit multicast traffic. MVR allows a single VLAN (known as the multicast VLAN) to receive all multicast streams and distribute them to multiple different client VLANs.

40.1. mvr

40.1.1. mvr

This command is used to enable global MVR administrative control.

Default

```
disable
```

Format

```
mvr
```

Mode

```
Global Configuration Mode
```

■ no mvr

This command is used to disable global MVR administrative control.

Format

```
no mvr
```

Mode

```
Global Configuration Mode
```

40.1.2. mvr vlan

This command is used to create MVR VLAN interface. <*v_vlan_list*> MVR multicast VLAN list.“name” MVR multicast name. <*mvr_name*> MVR multicast VLAN name.

Default

```
none
```

Format

```
mvr vlan <v_vlan_list> { [ name <mvr_name> ] }
```

Mode

```
Global Configuration Mode
```

■ no mvr vlan

This command is used to delete MVR VLAN interface.

Format

```
no mvr vlan <v_vlan_list>
```

Mode

```
Global Configuration Mode
```

40.1.3. mvr name

This command is used to set MVR name. *<mvr_name>* MVR multicast VLAN name. *<profile_name>* Specify an existing profile name.

Default

none

Format

mvr name *<mvr_name>* channel *<profile_name>*

Mode

Global Configuration Mode

no mvr name

This command is used to delete MVR Name.

Format

no mvr name *<mvr_name>* channel

Mode

Global Configuration Mode

40.1.4. mvr vlan (parametes)

This command is used to set up MVR VLAN interface parameters for tuning MVR operations. "frame priority" represents control the transmitted frames' priority (PCP value). "frame tagged" represents controls whether the transmitted frames are tagged or not. "igmp-address" represents MVR address configuration used as Source IP in IGMP messages. "last-member-query-interval" represents last Member Query Interval in tenths of seconds. "mode" represents MVR mode of operation, include dynamic and compatible.

Default

none

Format

mvr vlan *<vlan_list>* { [frame priority *<0-7>* | frame tagged | igmp-address *<ipv4_ucast>* | last-member-query-interval *<0-31744>* | mode { [dynamic | compatible] }] }

Mode

Global Configuration Mode

no mvr vlan

This command is used to delete MVR VLAN interface parameters.

Format

no mvr vlan *<vlan_list>*

Mode

Global Configuration Mode

40.1.5. mvr vlan type

This command is used to specify the MVR port role of the designated port.

Default

none

Format

mvr vlan *<v_vlan_list>* type { [source | receiver] }

Mode

Port Configuration Mode

no mvr vlan type

This command is used to delete the MVR port role of the designated port.

Format

```
no mvr vlan <v_vlan_list> type
```

Mode

```
Port Configuration Mode
```

40.1.6. mvr immediate-leave

This command is used to enable the immediate leave capability of the designated port.

Default

```
disable
```

Format

```
mvr immediate-leave
```

Mode

```
Port Configuration Mode
```

no mvr immediate-leave

This command is used to disable the immediate leave capability of the designated port.

Format

```
no mvr immediate-leave
```

Mode

```
Port Configuration Mode
```

40.2. show

40.2.1. show mvr

This command is used to show mvr configuration/status.

Format

```
show mvr { [ group-database | name | statistics | vlan ] }
```

Mode

```
User EXEC Mode
```

41. MVRP

MVRP (Multiple VLAN Registration Protocol) is a protocol for dynamically registering and deregistering VLAN identifiers across bridged local area networks. It uses the MRP (Multiple Registration Protocol) framework to define its operations, which is why it is also referred to as an MRP application. The standard was initially defined by IEEE 802.1ak, and its most recent incorporation is in IEEE 802.1Q-2014.

41.1. mvrp

41.1.1. mvrp

This command is used to enable the MVRP feature globally or on a specific interface.

Default

```
disable
```

Format

```
mvrp
```

Mode

```
Global Configuration Mode/Port Configuration Mode
```

no mvrp

This command is used to disable the MVRP function globally or on a specific interface.

Format

```
no mvrp
```

Mode

```
Global Configuration Mode/Port Configuration Mode
```

41.1.2. mvrp managed vlan

This command is used to configure the list of MVRP-managed VLANs. The optional parameters respectively represent the all VLANs, no VLANs, add VLANs to the current list, remove VLANs from the current list, and all VLANs except the following. <*vlan_list*> represents VLAN IDs of the managed VLANs of MVRP.

Default

```
none
```

Format

```
mvrp managed vlan { all | none | [ add | remove | except ] <vlan_list> }
```

Mode

```
Global Configuration Mode
```

41.2. show

41.2.1. show mrp status

This command is used to view MRP statistics for each interface. <*port_type_list*> represents Interface specification.

Format

```
show mrp status [ interface <port_type_list> ] [ all | mvrp ]
```

Mode

```
User EXEC Mode
```

42. Network Access Server (NAS)

NAS (Network Access Server) is a computer server that enables independent service provider (ISP) to provide Internet access services, located at the interface of PSTN (PSTN / ISDN) and IP networks. The user dials through subscriber line or trunk to get access to the network access server by the switch. A client connects to the NAS. And the NAS will connect another resource to ask whether the client's supplied credentials are valid. Then it will be allowed or disallowed to access to the protected resource based on the answer.

42.1. dot1x

42.1.1. dot1x system-auth-control

This command is used to enable the global NAS on the switchstack.

Default

```
disable
```

Format

```
dot1x system-auth-control
```

Mode

```
Global Configuration Mode
```

■ no dot1x system-auth-control

This command is used to disable the global NAS. If globally disabled, all ports are allowed forwarding of frames.

Format

```
no dot1x system-auth-control
```

Mode

```
Global Configuration Mode
```

42.1.2. dot1x re-authentication

This command is used to after first authentication is approved, the client will be authenticated every a certain time to ensure the legality of the client. In this case, the re-authentication function needs to be enabled. After the re-authentication function is enabled, 802.1x will periodically send the authentication request to the host.

Default

```
disable
```

Format

```
dot1x re-authentication
```

Mode

```
Global Configuration Mode
```

■ no dot1x re-authentication

This command is used to disable re-authentication function.

Format

```
no dot1x re-authentication
```

Mode

```
Global Configuration Mode
```

42.1.3. dot1x authentication timer re-authenticate

This command is used to determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled. *<1-3600>* represents the period between re-authentication attempts in seconds.

Default

```
3600
```

Format

```
dot1x authentication timer re-authenticate <1-3600>
```

Mode

```
Global Configuration Mode
```

■ no dot1x authentication timer re-authenticate

This command is used to restore the default timer reauthentication to 3600 seconds.

Format

```
no dot1x authentication timer re-authenticate
```

Mode

```
Global Configuration Mode
```

42.1.4. dot1x timeout tx-period

This command is used to during the 802.1x authentication process, it will send data message to the client host. You can regulate the data sending to ensure the response of the client host via controlling 802.1x transmission frequency. *<1-65535>* represents the time between EAPOL retransmissions.

Default

```
30
```

Format

```
dot1x timeout tx-period <1-65535>
```

Mode

```
Global Configuration Mode
```

■ no dot1x timeout tx-period

This command is used to restore the default time between EAPOL retransmissions to 30 seconds.

Format

```
no dot1x timeout tx-period
```

Mode

```
Global Configuration Mode
```

42.1.5. dot1x authentication timer inactivity

This command is used to port security module needs to be periodically check the MAC address table, and delete the MAC address not in use. This configuration is suitable for Single-802.1x, Multi-802.1x and mac-based authentication. *<10-1000000>* represents the time in seconds between check for activity on successfully authenticated MAC addresses.

Default

```
300
```

Format

```
dot1x authentication timer inactivity <10-1000000>
```

Mode

```
Global Configuration Mode
```

no dot1x authentication timer inactivity

This command is used to restore the default time in seconds between check for activity on successfully authenticated MAC addresses to 300 seconds.

Format

```
no dot1x authentication timer inactivity
```

Mode

```
Global Configuration Mode
```

42.1.6. dot1x timeout quiet-period

The hold time indicates the time in unauthorized state ranges from 10~1000000 seconds. This configuration is suitable for Single-802.1x, Multi-802.1x and mac-based authentication. <*10-1000000*> represents the time in seconds before a MAC-address that failed authentication gets a new authentication chance.

Default

```
10
```

Format

```
dot1x timeout quiet-period <10-1000000>
```

Mode

```
Global Configuration Mode
```

no dot1x timeout quiet-period

This command is used to restore the default time in seconds before a MAC-address that failed authentication gets a new authentication chance to 10 seconds.

Format

```
no dot1x timeout quiet-period
```

Mode

```
Global Configuration Mode
```

42.1.7. dot1x feature

This command is used to globally enables a dot1x feature functionality. You can globally enables state of guest-VLAN, RADIUS-assigned QoS and RADIUS-assigned VLAN.“guest-vlan” Globally enables/disables state of guest-VLAN.“radius-qos” Globally enables/disables state of RADIUS-assigned QoS. “radius-vlan” Globally enables/disables state of RADIUS-assigned VLAN.

Default

```
disable
```

Format

```
dot1x feature { [ guest-vlan ] [ radius-qos ] [ radius-vlan ] }
```

Mode

```
Global Configuration Mode
```

no dot1x feature

This command is used to globally disables a dot1x feature functionality. You can globally disables state of guest-VLAN, RADIUS-assigned QoS and RADIUS-assigned VLAN.

Format

```
no dot1x feature { [ guest-vlan ] [ radius-qos ] [ radius-vlan ] }
```

Mode

```
Global Configuration Mode
```

42.1.8. dot1x guest-vlan (value)

This command is used to configure the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. *<1-4095>* represents Guest VLAN ID used when entering the Guest VLAN.

Default

```
1
```

Format

```
dot1x guest-vlan <1-4095>
```

Mode

```
Global Configuration Mode
```

■ no dot1x guest-vlan

This command is used to restore the default Guest VLAN ID to 1.

Format

```
no dot1x guest-vlan
```

Mode

```
Global Configuration Mode
```

42.1.9. dot1x max-reauth-req

This command is used to configure the number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. *<1-255>* represents the number of times.

Default

```
2
```

Format

```
dot1x max-reauth-req <1-255>
```

Mode

```
Global Configuration Mode
```

■ no dot1x max-reauth-req

This command is used to restore the default number of times to 2.

Format

```
no dot1x max-reauth-req
```

Mode

```
Global Configuration Mode
```

42.1.10. dot1x guest-vlan supplicant

The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled, the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port.

Default

```
disable
```

Format

```
dot1x guest-vlan supplicant
```

Mode

```
Global Configuration Mode
```

no dot1x guest-vlan supplicant

This command is used to disable guest-vlan supplicant.

Format

```
no dot1x guest-vlan supplicant
```

Mode

```
Global Configuration Mode
```

42.1.11. dot1x port-control

This command is used to set the port security state. Valid states include force-authorized, force-unauthorized, auto, single, multi and mac-based. The optional parameters respectively represent port access is allowed, port access is not allowed, port-based 802.1X Authentication, single Host 802.1X Authentication, multiple Host 802.1X Authentication, Mac-based authentication.

Default

```
force-authorized
```

Format

```
dot1x port-control { force-authorized | force-unauthorized | auto | single | multi
| mac-based }
```

Mode

```
Port Configuration Mode
```

no dot1x port-control

This command is used to restore the default port security state to force-authorized.

Format

```
no dot1x port-control
```

Mode

```
Port Configuration Mode
```

42.1.12. dot1x radius-qos

This command is used to enables per-port state of RADIUS-assigned QoS. This option is only available for single-client modes, i.e. Port-based 802.1x and Single 802.1x.

Default

```
disable
```

Format

```
dot1x radius-qos
```

Mode

```
Port Configuration Mode
```

no dot1x radius-qos

This command is used to disables per-port state of RADIUS-assigned QoS.

Format

```
no dot1x radius-qos
```

Mode

```
Port Configuration Mode
```

42.1.13. dot1x radius-vlan

This command is used to enable per-port state of RADIUS-assigned VLAN. This option is only available for single-client modes, i.e. Port-based 802.1x and Single 802.1x.

Default

```
disable
```

Format

```
dot1x radius-vlan
```

Mode

```
Port Configuration Mode
```

■ no dot1x radius-vlan

This command is used to disable per-port state of RADIUS-assigned VLAN.

Format

```
no dot1x radius-vlan
```

Mode

```
Port Configuration Mode
```

42.1.14. dot1x guest-vlan

This command is used to enable guest VLAN. This option is only available for EAPOL-based modes, i.e. Port-based 802.1x, Single 802.1x and guest VLAN.

Default

```
disable
```

Format

```
dot1x guest-vlan
```

Mode

```
Port Configuration Mode
```

■ no dot1x guest-vlan

This command is used to disable guest VLAN.

Format

```
no dot1x guest-vlan
```

Mode

```
Port Configuration Mode
```

42.1.15. dot1x re-authenticate

This command is used to refresh (restart) 802.1x authentication process.

Format

```
dot1x re-authenticate
```

Mode

```
Port Configuration Mode
```

42.1.16. dot1x initialize

This command is used to force a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress. *<port_type_list>* represents port interface.

Format

```
dot1x initialize [ interface <port_type_list> ]
```

Mode

```
User EXEC Mode
```

42.2. show

42.2.1. show dot1x status

This command is used to shows dot1x status, such as admin state, port state and last source. *<port_type_list>* represents port interface.

Format

```
show dot1x status [ interface <port_type_list> ] [ brief ]
```

Mode

```
User EXEC Mode
```

42.2.2. show dot1x statistics

This command is used to shows statistics for either EAPoL or RADIUS. *<port_type_list>* represents port interface.

Format

```
show dot1x statistics { eapol | radius | all } [ interface <port_type_list> ]
```

Mode

```
User EXEC Mode
```

42.3. clear

42.3.1. clear dot1x statistics

This command is used to clears the statistics counters. *<port_type_list>* represents port interface.

Format

```
clear dot1x statistics [ interface <port_type_list> ]
```

Mode

```
User EXEC Mode
```

43. NTP

The Network Time Protocol (NTP) is a protocol used for synchronizing the clocks of computer systems, ensuring precision and consistency in system time. The NTP functionality of a switch allows it to synchronize its time with one or more NTP servers over the network, ensuring that all devices in the network have accurate time settings. This enhances the accuracy and reliability of log recording, scheduled tasks, and other time-sensitive operations.

43.1. ntp

43.1.1. ntp

This command is used to enable the NTP.

Default

```
disabled
```

Format

```
ntp
```

Mode

```
Global Configuration Mode
```

■ no ntp

This command is used to disable the NTP.

Format

```
no ntp
```

Mode

```
Global Configuration Mode
```

43.1.2. ntp server

This command is used to configure the NTP servers.<*1-5*> index number.

Default

```
none
```

Format

```
ntp server <1-5> ip-address { <ipv4_ucast> | <ipv6_ucast> | <domain_name> }
```

Mode

```
Global Configuration Mode
```

■ no ntp server

This command is used to negate the NTP servers.

Format

```
no ntp server <1-5>
```

Mode

```
Global Configuration Mode
```

43.2. show

43.2.1. show ntp status

This command is used to show the NTP status.

Format

```
show ntp status
```

Mode

```
User EXEC Mode
```

44. SNTP

The Simple Network Time Protocol (SNTP), adapted from NTP, is mainly used to synchronize the clocks of computers on the Internet. It is defined in RFC2030.

44.1. sntp

44.1.1. sntp server

This command is used to enable the SNTP.

Default

```
disabled
```

Format

```
sntp server
```

Mode

```
Global Configuration Mode
```

■ no sntp server

This command is used to disable the NTP.

Format

```
no sntp server
```

Mode

```
Global Configuration Mode
```

44.1.2. sntp client

This command is used to enable the SNTP (Simple Network Time Protocol) client.

Default

```
disabled
```

Format

```
sntp
```

Mode

```
Global Configuration Mode
```

■ no sntp client

This command is used to disable SNTP.

Format

```
no sntp client
```

Mode

```
Global Configuration Mode
```

44.1.3. sntp client server

This command is used to disable SNTP.

Format

```
sntp server <1-5> ip-address { <ipv4_ucast> | <ipv6_ucast> | <domain_name> }
```

Mode

```
Global Configuration Mode
```

■ no sntp server

This command is used to disable the SNTP server.

Format

```
no sntp server <1-5>
```

Mode

```
Global Configuration Mode
```

44.1.4. sntp client request-interval

This command is used to configure the SNTP time interval.

Default

```
10
```

Format

```
sntp client request-interval <10-16284>
```

Mode

```
Global Configuration Mode
```

■ no sntp client request-interval

This command is used to restore the default value of the Sntp interval.

Format

```
no sntp client request-interval
```

Mode

```
Global Configuration Mode
```

44.2. show

44.2.1. show sntp status

This command is used to display the status of SNTP.

Format

```
show sntp status
```

Mode

```
Global Configuration Mode
```

45. OSPF

OSPF is used for distributing routing information within a single Autonomous System (AS). OSPF is a link-state routing protocol primarily used in IP networks. It employs a flooding algorithm to rapidly propagate routing information and calculates the shortest path to each segment of the network.

45.1. router

45.1.1. router ospf

This command is used to enable OSPF router mode. And enter OSPF router configuration view.

Default

```
disable
```

Format

```
router ospf
```

Mode

```
Global Configuration Mode
```

■ no router ospf

This command is used to disable OSPF router mode.

Format

```
no router ospf
```

Mode

```
Global Configuration Mode
```

45.2. router-id

45.2.1. router-id

This command is used to configure the OSPF Router ID in IPv4 address format(A.B.C.D). When the router's OSPF Router ID is changed, if there is one or more fully adjacent neighbors in current OSPF area, the new router ID will take effect after restart OSPF process. Notice that the router ID should be unique in the Autonomous System and value “0.0.0.0” is invalid since it is reserved for the default algorithm. <*ipv4_addr*> represents IPv4 address, the allowed range is from 0.0.0.1 to 255.255.255.254.

Default

```
the largest IP address assigned to the router
```

Format

```
router-id <ipv4_addr>
```

Mode

```
OSPF Router Mode
```

■ no router-id

This command is used to restore the OSPF Router ID to default.

Format

```
no router-id
```

Mode

```
OSPF Router Mode
```

45.3. passive-interface

45.3.1. passive-interface default

This command is used to configure all interfaces as passive-interface by default. When an interface is configured as a passive-interface, the OSPF routing updates sending is suppressed, therefore the interface does not establish adjacencies (No OSPF Hellos). The subnet of all interfaces (both passive and active) is advertised by the OSPF router.

Default

```
disable
```

Format

```
passive-interface default
```

Mode

```
OSPF Router Mode
```

■ no passive-interface default

This command is used to disable all interfaces as passive-interface by default.

Format

```
no passive-interface default
```

Mode

```
OSPF Router Mode
```

45.4. default-metric

45.4.1. default-metric

This command is used to configure user specified default metric value for the OSPF routing protocol. *<0-16777214>* represents user specified default metric value.

Default

```
0
```

Format

```
default-metric <0-16777214>
```

Mode

```
OSPF Router Mode
```

■ no default-metric

This command is used to restore user specified default metric value to default.

Format

```
no default-metric
```

Mode

```
OSPF Router Mode
```

45.5. redistribute

45.5.1. redistribute

This command is used to configure the OSPF redistributed metric type for the static routes, connected interfaces or RIP routes. Use keywords metric to configure the specified metric for OSPF redistribution, default is auto. *<0-16777214>* represents user specified metric value.

Default

```
none
```

Format

```
redistribute { static | connected | rip } [ metric <0-16777214> ] [ metric-type { 1 | 2 } ]
```

Mode

```
OSPF Router Mode
```

no redistribute

This command is used to restore the OSPF redistributed metric type for the static routes, connected interfaces or RIP routes.

Format

```
no redistribute { static | connected | rip }
```

Mode

```
OSPF Router Mode
```

45.6. max-metric

45.6.1. max-metric router-lsa

This command is used to enable OSPF to advertise a maximum metric during startup or shutdown for a configured period of time, or OSPF stub router mode administratively applied for an indefinite period. *<5-86400>* represents user specified time interval (seconds) to advertise itself as stub area. *<5-100>* represents user specified time interval (seconds) to wait till shutdown completed.

Default

```
disable
```

Format

```
max-metric router-lsa { [ on-startup <5-86400> ] [ on-shutdown <5-100> ] [ administrative ] }
```

Mode

```
OSPF Router Mode
```

no max-metric router-lsa

This command is used to disable OSPF to advertise a maximum metric during startup or shutdown for a configured period of time, or OSPF stub router mode administratively applied for an indefinite period.

Format

```
no max-metric router-lsa [ on-startup ] [ on-shutdown ] [ administrative ]
```

Mode

```
OSPF Router Mode
```

45.7. default-information

45.7.1. default-information originate

This command is used to configure the OSPF redistributed metric type for a default route. *<0-16777214>* represents user specified metric value for a default route.

Default

```
none
```

Format

```
default-information originate [ always ] [ metric <0-16777214> ] [ metric-type { 1 | 2 } ]
```

Mode

```
OSPF Router Mode
```

no default-information originate

This command is used to restore the OSPF redistributed metric type for a default route.

Format

```
no default-information originate
```

Mode

```
OSPF Router Mode
```

45.8. distance

45.8.1. distance

This command is used to configure the OSPF administrative distance. *<1-255>* represents administrative distance value.

Default

```
110
```

Format

```
distance <1-255>
```

Mode

```
OSPF Router Mode
```

no distance

This command is used to restore the OSPF administrative distance to default.

Format

```
no distance
```

Mode

```
OSPF Router Mode
```

45.9. network

45.9.1. network

This command is used to configure OSPF network area. *<ipv4_addr>* represents IPv4 network address. *<ipv4_mask>* represents the the IPv4 network mask. *<area_id>* represents OSPF area ID.

Default

none

Format

network *<ipv4_addr>* *<ipv4_mask>* area *<area_id>*

Mode

OSPF Router Mode

■ no network

This command is used to delete OSPF network area.

Format

no network *<ipv4_addr>* *<ipv4_addr>* [area *<area_id>*]

Mode

OSPF Router Mode

45.10. passive-interface

45.10.1. passive-interface vlan

This command is used to enable OSPF router interface as OSPF passive-interface. *<vlan_list>* represents the interface.

Default

disable

Format

passive-interface vlan *<vlan_list>*

Mode

OSPF Router Mode

■ no passive-interface vlan

This command is used to disable OSPF router interface as OSPF passive-interface.

Format

no passive-interface vlan *<vlan_list>*

Mode

OSPF Router Mode

45.11. area

45.11.1. area stub

This command is used to configure the area as a stub area. *<area_id>* represents OSPF area ID.

Default

none

Format

area *<area_id>* stub [no-summary]

Mode

OSPF Router Mode

no area stub

This command is used to delete the area as a stub area.

Format

no area *<area_id>* stub [no-summary]

Mode

OSPF Router Mode

45.11.2. area nssa

This command is used to configure the area as a nssa. *<area_id>* represents OSPF area ID. "translate" represents translate LSA. "type7" represents from Type 7 to Type 5. "candidate" represents configure NSSA-ABR for translate election (default). "never" represents configure NSSA-ABR to never translate. "always" represents configure NSSA-ABR to never translate. "no-summary" represents don’t inject inter-area routes into nssa.

Default

none

Format

area *<area_id>* nssa [translate type7 { candidate | never | always } | no-summary]

Mode

OSPF Router Mode

no area nssa

This command is used to delete the area as a nssa.

Format

no area *<area_id>* nssa [translate type7 { candidate | never | always } | no-summary]

Mode

OSPF Router Mode

45.11.3. area authentication

This command is used to configure the area authentication. *<area_id>* represents OSPF area ID.

Default

none

Format

area *<area_id>* authentication [message-digest]

Mode

OSPF Router Mode

■ no area authentication

This command is used to delete the area authentication.

Format

```
no area <area_id> authentication
```

Mode

```
OSPF Router Mode
```

45.11.4. area range

This command is used to configure the OSPF area range. *<area_id>* represents OSPF area ID. *<ipv4_addr>* represents IPv4 network address. *<ipv4_netmask>* represents IPv4 network mask. *<0-16777215>* represents user specified cost (or metric) for this summary route.

Default

```
none
```

Format

```
area <area_id> range <ipv4_addr> <ipv4_netmask> [ advertise [ cost <0-16777215> ]
| not-advertise | cost <0-16777215> ]
```

Mode

```
OSPF Router Mode
```

■ no area range

This command is used to delete the OSPF area range.

Format

```
no area <area_id> range <ipv4_addr> <ipv4_netmask> [ advertise | not-advertise | cost ]
```

Mode

```
OSPF Router Mode
```

45.12. ip ospf

45.12.1. ip ospf

This command is used to configure the OSPF interface. *<0-255>* represents user specified router priority for the interface. "cost *<1-65535>*" represents user specified cost for this interface. "hello-interval *<1-65535>*" represents set the hello interval value for the specific interface. *<3-65535>* represents the time interval (in seconds) between link-state advertisement(LSA) retransmissions for adjacencies. "dead-interval <1-65535>" represents the neighbor dead interval. *<1-10>* represents how many Hello packets will be sent per second.

Default

```
priority: 1
cost: 1
hello-interval: 10
retransmit-interval: 5
dead-interval: 40
hello-multiplier: disabled
```

Format

```
ip ospf { priority <0-255> | cost <1-65535> | hello-interval <1-65535> |
retransmit-interval <3-65535> | dead-interval { <1-65535> | minimal hello-multiplier
<1-10> } }
```

Mode

```
VLAN Interface Mode
```

no ip ospf

This command is used to restore the OSPF interface configuration.

Format

```
no ip ospf { priority | cost | dead-interval | hello-interval | retransmit-interval }
```

Mode

```
VLAN Interface Mode
```

45.12.2. ip ospf authentication

This command is used to configure the authentication type. "null" represents use null authentication. "message-digest" represents use message digest (MD5) authentication.

Default

```
null
```

Format

```
ip ospf authentication [ null | message-digest ]
```

Mode

```
VLAN Interface Mode
```

no ip ospf authentication

This command is used to restore the authentication type to default.

Format

```
no ip ospf authentication
```

Mode

```
VLAN Interface Mode
```

45.12.3. ip ospf authentication-key

This command is used to configure simple password authentication. <*word1-8*> represents the unencrypted (Plain Text) user password. <*word128*> represents the encrypted(hidden) user password.

Default

```
none
```

Format

```
ip ospf authentication-key { unencrypted <word1-8> | encrypted <word128> }
```

Mode

```
VLAN Interface Mode
```

no ip ospf authentication-key

This command is used to restore simple password authentication to default.

Format

```
no ip ospf authentication-key
```

Mode

```
VLAN Interface Mode
```

45.12.4. ip ospf message-digest-key

This command is used to configure message digest key authentication. <*1-255*> represents message digest key ID. <*word1-16*> represents the unencrypted (Plain Text) user password. <*word128*> represents the encrypted (hidden) user password.

Default

none

Format

ip ospf message-digest-key <*1-255*> md5 { unencrypted <*word1-16*> | encrypted <*word128*> }

Mode

VLAN Interface Mode

■ no ip ospf message-digest-key

This command is used to restore message digest key authentication to default.

Format

no ip ospf message-digest-key <*1-255*>

Mode

VLAN Interface Mode

45.13. area virtual-link

45.13.1. area virtual-link

This command is used to configure a virtual link. <*area_id*> represents the OSPF area ID. <*ipv4_addr*> represents router ID of the remote ABR. "hello-interval <*1-65535*>" represents the time interval (in seconds) between hello packets. <*3-65535*> represents the time interval (in seconds) between link-state advertisement(LSA) retransmissions for adjacencies. "dead-interval <*1-65535*>" represents the number of seconds to wait until the neighbor is declared to be dead.

Default

none

Format

area <*area_id*> virtual-link <*ipv4_addr*> [hello-interval <*1-65535*>] [retransmit-interval <*3-65535*>] [dead-interval <*1-65535*>]

Mode

OSPF Router Mode

■ no area virtual-link

This command is used to restore a virtual link to default.

Format

no area <*area_id*> virtual-link <*ipv4_addr*> [hello-interval [<*1-65535*>]] [retransmit-interval [<*1-65535*>]] [dead-interval [<*1-65535*>]]

Mode

OSPF Router Mode

45.13.2. area virtual-link authentication

This command is used to enable authentication. <*area_id*> represents the OSPF area ID. <*ipv4_addr*> represents router ID of the remote ABR.

Default

disable

Format

area <*area_id*> virtual-link <*ipv4_addr*> authentication [null | message-digest]

Mode

OSPF Router Mode

■ no area virtual-link authentication

This command is used to disable authentication.

Format

no area <*area_id*> virtual-link <*ipv4_addr*> authentication

Mode

OSPF Router Mode

45.13.3. area virtual-link authentication-key

This command is used to configure simple password authentication. <*area_id*> represents the OSPF area ID. <*ipv4_addr*> represents router ID of the remote ABR. <*word1-8*> represents the unencrypted (Plain Text) user password. <*word128*> represents the encrypted (hidden) user password.

Default

none

Format

area <*area_id*> virtual-link <*ipv4_addr*> authentication-key { unencrypted <*word1-8*> | encrypted <*word128*> }

Mode

OSPF Router Mode

■ no area virtual-link authentication-key

This command is used to restore simple password authentication.

Format

no area <*area_id*> virtual-link <*ipv4_addr*> authentication-key

Mode

OSPF Router Mode

45.13.4. area virtual-link message-digest-key

This command is used to configure message digest key authentication. <*area_id*> represents the OSPF area ID. <*ipv4_addr*> represents router ID of the remote ABR. <*1-255*> represents message digest key ID. <*word1-16*> represents the unencrypted (Plain Text) user password. <*word128*> represents the encrypted (hidden) user password.

Default

none

Format

area <*area_id*> virtual-link <*ipv4_addr*> message-digest-key <*1-255*> md5 { unencrypted <*word1-16*> | encrypted <*word128*> }

Mode

OSPF Router Mode

no area virtual-link message-digest-key

This command is used to restore message digest key authentication.

Format

```
no area <area_id> virtual-link <ipv4_addr> message-digest-key <1-255>
```

Mode

```
OSPF Router Mode
```

45.14. show

45.14.1. show ip ospf

This command is used to display OSPF configuration.

Format

```
show ip ospf
```

Mode

```
User EXEC Mode
```

45.14.2. show ip ospf route

This command is used to display OSPF routing information.

Format

```
show ip ospf route
```

Mode

```
User EXEC Mode
```

45.14.3. show ip ospf interface

This command is used to display OSPF interface configuration. *<vlan_list>* represents VLAN interface. *<vlink_list>* represents virtual link interface. *<loopback_id>* represents loopback interface.

Format

```
show ip ospf interface [ vlan <vlan_list> | vlink <vlink_list> | loopback
<loopback_id> ]
```

Mode

```
User EXEC Mode
```

45.14.4. show ip ospf neighbor

This command is used to display OSPF neighbor information.

Format

```
show ip ospf neighbor [ detail ]
```

Mode

```
User EXEC Mode
```

45.14.5. show ip ospf database

This command is used to display OSPF database information. link-state-id <*ipv4_addr*> represents link state ID (as an IPv4 address format). adv-router <*ipv4_addr*> represents advertising router ID (as an IPv4 address format).

Format

```
show ip ospf database [ {router | network | summary | asbr-summary | external |
nssa-external } [ link-state-id <ipv4_addr> ] ] [ adv-router <ipv4_addr> |
self-originate ]
```

Mode

```
User EXEC Mode
```

45.15. clear

45.15.1. clear ip ospf process

This command is used to reset the current OSPF process.

Format

```
clear ip ospf process
```

Mode

```
User EXEC Mode
```

46. OSPFv3

OSPFv3 is a version of the OSPF protocol designed to support the IPv6 address family while also retaining compatibility with IPv4. Compared to OSPFv2, OSPFv3 has been expanded and improved to accommodate the requirements of IPv6 networks.

46.1. router

46.1.1. router ospf6

This command is used to enable OSPF6 router mode. And enter OSPF6 router configuration view.

Default

```
disable
```

Format

```
router ospf6
```

Mode

```
Global Configuration Mode
```

■ no router ospf6

This command is used to disable OSPF6 router mode.

Format

```
no router ospf6
```

Mode

```
Global Configuration Mode
```

46.2. router-id

46.2.1. router-id

This command is used to configure the OSPF6 Router ID in IPv4 address format(A.B.C.D). When the router's OSPF6 Router ID is changed, if there is one or more fully adjacent neighbors in current OSPF6 area, the new router ID will take effect after restart OSPF6 process. Notice that the router ID should be unique in the Autonomous System and value '0.0.0.0' is invalid since it is reserved for the default algorithm. *<ipv4_addr>* represents IPv4 address, the allowed range is from 0.0.0.1 to 255.255.255.254.

Default

```
the largest IP address assigned to the router
```

Format

```
router-id <ipv4_addr>
```

Mode

```
OSPFv3 Router Mode
```

■ no router-id

This command is used to restore the OSPF6 Router ID to default.

Format

```
no router-id
```

Mode

```
OSPFv3 Router Mode
```

46.3. redistribute

46.3.1. redistribute

This command is used to enable the OSPF6 redistributed for the static routes or connected interfaces.

Default

```
disable
```

Format

```
redistribute { static | connected }
```

Mode

```
OSPFv3 Router Mode
```

no redistribute

This command is used to disable the OSPF6 redistributed for the static routes or connected interfaces.

Format

```
no redistribute { static | connected }
```

Mode

```
OSPFv3 Router Mode
```

46.4. distance

46.4.1. distance

This command is used to configure the OSPF6 administrative distance. *<1-255>* represents administrative distance value.

Default

```
110
```

Format

```
distance <1-255>
```

Mode

```
OSPFv3 Router Mode
```

no distance

This command is used to restore the OSPF6 administrative distance to default.

Format

```
no distance
```

Mode

```
OSPFv3 Router Mode
```

46.5. interface

46.5.1. interface vlan area

This command is used to configure the OSPF6 router interface area. <*vlan_list*> represents list of VLAN interface numbers. <*area_id*> represents area ID of the interface.

Default

```
disable
```

Format

```
interface vlan <vlan_list> area <area_id>
```

Mode

```
OSPFv3 Router Mode
```

■ no interface vlan area

This command is used to restore the OSPF6 router interface area.

Format

```
no interface vlan <vlan_list> area <area_id>
```

Mode

```
OSPFv3 Router Mode
```

46.5.2. interface vlan

This command is used to enable the OSPF6 router interface. <*vlan_list*> represents list of VLAN interface numbers.

Default

```
disable
```

Format

```
interface vlan <vlan_list>
```

Mode

```
OSPFv3 Router Mode
```

■ no interface vlan

This command is used to disable the OSPF6 router interface.

Format

```
no interface vlan <vlan_list>
```

Mode

```
OSPFv3 Router Mode
```

46.6. area

46.6.1. area stub

This command is used to configure the OSPF6 stub area. *<area_id>* represents the OSPF6 area ID.

Default

none

Format

area *<area_id>* stub [no-summary]

Mode

OSPFv3 Router Mode

no area stub

This command is used to delete the OSPF6 stub area.

Format

no area *<area_id>* stub [no-summary]

Mode

OSPFv3 Router Mode

46.6.2. area range

This command is used to configure the OSPF6 area range. *<area_id>* represents the OSPF6 area ID. *<ipv6_subnet>* represents IPv6 network address. *<0-16777215>* represents user specified cost (or metric) for this summary route.

Default

none

Format

area *<area_id>* range *<ipv6_subnet>* [advertise [cost *<0-16777215>*] | not-advertise | cost *<0-16777215>*]

Mode

OSPFv3 Router Mode

no area range

This command is used to restore the OSPF6 area range.

Format

no area *<area_id>* range *<ipv6_subnet>* [advertise | not-advertise | cost]

Mode

OSPFv3 Router Mode

46.7. ipv6

46.7.1. ipv6 ospf

This command is used to configure the OSPF6 interface. Priority *<0-255>* represents user specified router priority for the interface. cost *<1-65535>* represents user specified cost for this interface. hello-interval *<1-65535>* represents how many Hello packets will be sent per second. retransmit-interval *<3-65535>* represents the time interval (in seconds) between link-state advertisement(LSA) retransmissions for adjacencies. transmit-delay *<1-3600>* represents user transmit-delay value for the specified interface. dead-interval *<1-65535>* represents the time interval (in seconds) between hello packets.

Default

```
priority: 1
cost: 1
hello-interval: 10
retransmit-interval: 5
dead-interval: 40
```

Format

```
ipv6 ospf { passive | priority <0-255> | cost <1-65535> | hello-interval <1-65535>
| retransmit-interval <3-65535> | transmit-delay <1-3600> | dead-interval { <1-65535> } }
```

Mode

```
VLAN Interface Mode
```

■ no ipv6 ospf

This command is used to restore the OSPF6 interface configuration.

Format

```
no ipv6 ospf { priority | cost | dead-interval | hello-interval | retransmit-interval
| transmit-delay | passive }
```

Mode

```
VLAN Interface Mode
```

46.8. show

46.8.1. show ipv6 ospf

This command is used to display OSPF6 configuration.

Format

```
show ipv6 ospf
```

Mode

```
User EXEC Mode
```

46.8.2. show ipv6 ospf interface

This command is used to display OSPF6 interface configuration. <*vlan_list*> represents VLAN interface.

Format

```
show ipv6 ospf interface [ vlan <vlan_list> ]
```

Mode

```
User EXEC Mode
```

46.8.3. show ipv6 ospf neighbor

This command is used to display OSPF6 neighbor information.

Format

```
show ipv6 ospf neighbor [ detail ]
```

Mode

```
User EXEC Mode
```

46.8.4. show ipv6 ospf database

This command is used to display OSPF6 database information. Link-state-id <*ipv4_addr*> represents link state ID (as an IPv4 address format). Adv-router <*ipv4_addr*> represents advertising router ID (as an IPv4 address format).

Format

```
show ipv6 ospf database [ { router | network | inter-prefix | inter-router | external | link | intra-prefix } [ link-state-id <ipv4_addr> ] ] [ adv-router <ipv4_addr> | self-originate ]
```

Mode

```
User EXEC Mode
```

46.8.5. show ipv6 ospf route

This command is used to display OSPF6 routing information.

Format

```
show ipv6 ospf route
```

Mode

```
User EXEC Mode
```

46.9. clear

46.9.1. clear ipv6 ospf process

This command is used to reset the current OSPF6 process.

Format

```
clear ipv6 ospf process
```

Mode

```
User EXEC Mode
```

47. PIM

PIM is a multicast routing protocol used on switches and routers responsible for managing and transmitting multicast data streams, such as video or streaming media, within IP networks. The PIM protocol operates independently of the underlying unicast routing protocols, meaning it does not rely on specific unicast routing protocols such as OSPF or BGP to propagate multicast routing information.

47.1. ip

47.1.1. ip pim sm

This command is used to enable global pim sm. PIM SM refers to the Protocol Independent Multicast Sparse Mode. It is a multicast routing protocol used to efficiently transport multicast traffic in computer networks.

Default

```
disable
```

Format

```
ip pim sm
```

Mode

```
Global Configuration Mode
```

■ no ip pim sm

This command is used to disable global pim sm.

Format

```
no ip pim sm
```

Mode

```
Global Configuration Mode
```

47.1.2. ip pim ssm prefix-list

This command is used to specify a prefix list for filtering Multicast routes in Protocol Independent Multicast (PIM) Source Specific Multicast (SSM) mode.

Default

```
none
```

Format

```
ip pim ssm prefix-list <word-31>
```

Mode

```
Global Configuration Mode
```

■ no ip pim ssm prefix-list

This command is used to delete a specified prefix list.

Format

```
no ip pim ssm prefix-list <word-31>
```

Mode

```
Global Configuration Mode
```

47.1.3. ip pim

This command is used to configure PIM interface parameters. It enables PIM functionality on the interface and specifies the hello message interval. Hello messages are control messages used by the PIM protocol to discover and maintain multicast neighbor relationships. It also specifies the time interval between sending two Join/Prune messages. Join/Prune messages are control messages used by the PIM protocol to manage multicast group membership. Lastly, it specifies the designated router (DR) priority for the PIM device. Devices with higher priority will be selected as the DR.

Default

```
hello: 30
join-prune-interval: 60
dr-priority: 1
```

Format

```
ip pim { [ hello <1-180> ] [ join-prune-interval <60-600> ] [ dr-priority <1-4294967295> ] }
```

Mode

```
VLAN Interface Mode
```

no ip pim

This command is used to disable the pim function on an interface, restore the default interval of hello messages and join-prune-interval messages, and restore the default dr Priority.

Format

```
no ip pim { [ hello ] [ join-prune-interval ] [ dr-priority ] }
```

Mode

```
VLAN Interface Mode
```

47.1.4. ip pim sm rp

This command is used to specify the pim sm static RP as the central node of the multicast group so that the device can communicate with it during the multicast transmission.

Default

```
none
```

Format

```
ip pim sm rp <address> <group_address/masklength>
```

Mode

```
Global Configuration Mode
```

no ip pim sm rp

This command is used to delete a static RP.

Format

```
no ip pim sm rp <address> <group_address/masklength>
```

Mode

```
Global Configuration Mode
```

47.1.5. ip multicast-routing

This command is used to enable global multicast services. Multicast Routing is a technique used to transport multicast traffic from a source point to multiple destinations in a computer network. Unlike Unicast and Broadcast, multicast only sends packets to specific multicast group members that need to be received.

Default

```
disable
```

Format

```
ip multicast-routing
```

Mode

```
Global Configuration Mode
```

no ip multicast-routing

This command is used to disable global multicast services.

Format

```
no ip multicast-routing
```

Mode

```
Global Configuration Mode
```

47.2. show

47.2.1. show ip pim interface

This command is used to display detailed information about the interface on which PIM is enabled. The information includes the name, status, number of neighbors, and status of the interface.

Format

```
show ip pim interface
```

Mode

```
User EXEC Mode
```

47.2.2. show ip pim neighbor

This command is used to display the PIM neighbor information on the device. This command displays detailed information about all established PIM neighbors, including IP addresses, interfaces, and DRS. This command can be used to verify the establishment and status of PIM neighbors and help diagnose and troubleshoot problems related to PIM neighbors.

Format

```
show ip pim neighbor
```

Mode

```
User EXEC Mode
```

47.2.3. show ip mroute

This command is used to display the IP multicast routing table on the device. This command lists the source and group information of the learned multicast traffic on the device. It displays the details of multicast routes such as source IP addresses, group IP addresses, and outgoing interfaces. This command helps you view the multicast routes and traffic distribution configured on the device and traverse the multicast path of the device.

Format

```
show ip mroute
```

Mode

```
User EXEC Mode
```

48. PoE

PoE (Power over Ethernet) technology refers to the existing Ethernet cabling infrastructure that supplies power along with data transmission without any modifications. This ensures that the Ethernet cable can transmit data signals to Ethernet terminal devices while simultaneously providing DC power to such devices.

48.1. PoE

48.1.1. poe terminal-description

This command is used to set textual description for each PoE-PD device connected to the port.

Default

```
none
```

Format

```
poe terminal-description <line32>
```

Mode

```
Port Configuration Mode
```

■ no poe terminal-description

This command is used to delete the text description for each PoE-PD device connected to the port.

Format

```
no poe terminal-description
```

Mode

```
Port Configuration Mode
```

48.1.2. poe mode

This command is used to configure of PoE mode, divided into standard and plus modes.

Default

```
disable
```

Format

```
poe mode { standard | plus }
```

Mode

```
Port Configuration Mode
```

■ no poe mode

This command is used to disable PoE mode.

Format

```
no poe mode
```

Mode

```
Port Configuration Mode
```

48.1.3. poe priority

This command is used to configure PoE priority, the priority is divided into low, high, and critical.

Default

```
low
```

Format

```
poe priority { low | high | critical }
```

Mode

```
Port Configuration Mode
```

no poe priority

This command is used to set PoE priority to default.

Format

```
no poe priority
```

Mode

```
Port Configuration Mode
```

48.1.4. poe lldp

This command is used to enable PoE lldp functionality.

Default

```
enable
```

Format

```
poe lldp
```

Mode

```
Port Configuration Mode
```

no poe lldp

This command is used to disable PoE lldp functionality.

Format

```
no poe lldp
```

Mode

```
Port Configuration Mode
```

48.1.5. poe capacitor-detect

This command is used to enable PoE capacitor-detect.

Default

```
disable
```

Format

```
poe capacitor-detect
```

Mode

```
Global Configuration Mode
```

no poe capacitor-detect

This command is used to disable PoE capacitor-detect.

Format

```
no poe capacitor-detect
```

Mode

```
Global Configuration Mode
```

48.2. show

48.2.1. show poe system

This command is used to show poe system information.

Format

```
show poe system
```

Mode

```
User EXEC Mode
```

48.2.2. show poe

This command is used to show PoE status.

Format

```
show poe [ interface <port_type_list> ]
```

Mode

```
User EXEC Mode
```

49. Port

Ports on a switch primarily play critical roles in functions such as data transmission, auto-negotiation, VLAN segmentation, security configurations, and MAC address learning.

49.1. media-type

49.1.1. media-type

This command use media-type to configure the interface media type.

Default

```
none
```

Format

```
media-type { rj45 | sfp | dual | dac-1m | dac-2m | dac-3m | dac-5m }
```

Mode

```
Port Configuration Mode
```

■ no media-type

This command use media-type to configure the interface media type to default.

Format

```
no media-type
```

Mode

```
Port Configuration Mode
```

49.2. fec

49.2.1. fec

This command is used to force a particular FEC mode.

Default

```
none
```

Format

```
fec { auto | r-fec | rs-fec | none }
```

Mode

```
Port Configuration Mode
```

■ no fec

This command use this command to default the FEC mode (corresponds to 'fec auto').

Format

```
no fec
```

Mode

```
Port Configuration Mode
```

49.3. clause-73

49.3.1. clause-73 parallel-detect

This command is used to enable Clause-73 (KR) parallel-detect.

Default

```
enable
```

Format

```
clause-73 parallel-detect
```

Mode

```
Port Configuration Mode
```

■ no clause-73 parallel-detect

This command is used to disable Clause-73 (KR) parallel-detect.

Format

```
no clause-73 parallel-detect
```

Mode

```
Port Configuration Mode
```

49.4. speed

49.4.1. speed

This command is used to configure interface speed. If you use 10, 100, 1000 or one of the other keywords with the auto keyword the port will only advertise the specified speeds.

Default

```
none
```

Format

```
speed { 10 | 100 | 1000 | 2500 | 5g | 10g | 25g | force-clause-73 | auto { [ 10 ] [ 100 ] [ 1000 ] [ 2500 ] [ 5g ] [ 10g ] { [ no-hdx ] | [ no-fdx ] } } }
```

Mode

```
Port Configuration Mode
```

■ no speed

This command use "no speed" to configure interface to default speed.

Format

```
no speed
```

Mode

```
Port Configuration Mode
```

49.5. duplex

49.5.1. duplex

This command use duplex to configure interface duplex mode when speed is a forced speed.

Default

```
none
```

Format

```
duplex { half | full | { auto [ half | full ] } }
```

Mode

```
Port Configuration Mode
```

■ no duplex

This command use "no duplex" to set duplex to default.

Format

```
no duplex
```

Mode

```
Port Configuration Mode
```

49.6. flowcontrol

49.6.1. flowcontrol

This command use flowcontrol to configure flow control for the interface.

Default

```
none
```

Format

```
flowcontrol { on | off }
```

Mode

```
Port Configuration Mode
```

■ no flowcontrol

This command use no flowcontrol to set flow control to default.

Format

```
no flowcontrol
```

Mode

```
Port Configuration Mode
```

49.7. priority-flowcontrol

49.7.1. priority-flowcontrol prio

This command use priority flowcontrol (802.1Qbb) to configure flow control per priority.

Default

```
none
```

Format

```
priority-flowcontrol prio <0~7>
```

Mode

```
Port Configuration Mode
```

■ no priority-flowcontrol prio

This command use priority flowcontrol (802.1Qbb) to configure flow control per priority to default.

Format

```
no priority-flowcontrol prio [ <0~7> ]
```

Mode

```
Port Configuration Mode
```

49.8. mtu

49.8.1. mtu

This command use mtu to specify maximum frame size (1518-max-for-platform bytes).

Default

```
none
```

Format

```
mtu <1518-Maximum_frame_size>
```

Mode

```
Port Configuration Mode
```

■ no mtu

This command use no mtu to set maximum frame size to default.

Format

```
no mtu
```

Mode

```
Port Configuration Mode
```

49.9. port-monitor

49.9.1. port-monitor

This command is used to enable/disable the Port Monitor function globally.

Default

```
disable
```

Format

```
port-monitor
```

Mode

```
Port Configuration Mode
```

■ no port-monitor

This command is used to disable the Port Monitor function globally.

Format

```
no port-monitor
```

Mode

```
Port Configuration Mode
```

49.9.2. port-monitor condition speed-duplex mode

This command is used to enable/disable the monitoring of the link speed and duplex mode on the port.

Default

```
none
```

Format

```
port-monitor condition speed-duplex mode
```

Mode

```
Port Configuration Mode
```

■ no port-monitor condition speed-duplex mode

This command is used to disable the monitoring of the link speed and duplex mode on the port.

Format

```
no port-monitor condition speed-duplex mode
```

Mode

```
Port Configuration Mode
```

49.9.3. port-monitor condition speed-duplex speed

This command is used to enable/disable the port monitor to accept a data rate combination on the port.

Default

```
port static capability
```

Format

```
port-monitor condition speed-duplex speed { [ hdx-10 ] [ fdx-10 ] [ hdx-100 ] [ fdx-100 ]
[ fdx-1000 ] [ fdx-2500 ] [ fdx-5000 ] [ fdx-10000 ] }
```

Mode

```
Port Configuration Mode
```

no port-monitor condition speed-duplex speed

This command is used to disable the port monitor to accept a data rate combination on the port.

Format

```
no port-monitor condition speed-duplex speed
```

Mode

```
Port Configuration Mode
```

49.9.4. port-monitor action

This command is used to specify the action that the device carries out if the Port Monitor function detects that the parameters have been exceeded.

Default

```
none
```

Format

```
port-monitor action { trap-only | port-disable }
```

Mode

```
Port Configuration Mode
```

49.10. show

49.10.1. show port-monitor speed-duplex

This command is used to show the current Ports Monitor speed-duplex configurations.

Format

```
show port-monitor speed-duplex
```

Mode

```
User EXEC Mode
```

49.10.2. show port-monitor brief

This command is used to show all Ports Monitor brief information.

Format

```
show port-monitor brief
```

Mode

```
User EXEC Mode
```

49.10.3. show port-monitor interface

This command is used to show all the interface Ports Monitor information.

Format

```
show port-monitor interface <port_type_list>
```

Mode

```
User EXEC Mode
```

49.10.4. show interface status

This command is used to display status for the interface.

Format

```
show interface <port_type_list> status [ err-disable ] [ details [ clause-73 ] ]
```

Mode

```
User EXEC Mode
```

49.10.5. show interface statistics

This command is used to show statistics for the interface.

Format

```
show interface <port_type_list> statistics [ { packets | bytes | errors | discards
| dot3br | { priority [ <0~7> ] } | link-state-changes } ] [ { up | down } ]
```

Mode

```
User EXEC Mode
```

49.11. clear

49.11.1. clear statistics

This command is used to clear the statistics for the interface.

Format

```
clear statistics [ interface ] <port_type_list>
```

Mode

```
User EXEC Mode
```

50. Privilege Level

By setting privilege levels, it is possible to control the access permissions of users at different levels to various modules.

50.1. web

50.1.1. web privilege group

This command configures module privilege level. “group” represents web group name defined by system, such as DHCP, IP. “configRoPriv” represents configuring read-only privilege level, ranging from 0 to 15. “configRwPriv” represents configuring read-and-write privilege level, ranging from 0 to 15. “statusRoPriv” represents status/statistic read-only privilege level, ranging from 0 to 15. “statusRwPriv” represents status/statistic read-and-write privilege level, ranging from 0 to 15.Privilege levels are related to user levels; when a user's level is higher than the privilege level, then that user can configure/view that module.

Default

module: System、Ports

- configRoPriv 5
- configRwPriv 10
- statusRoPriv 1
- statusRwPriv 10

module: Debug、Miscellaneous

- configRoPriv 15
- configRwPriv 15
- statusRoPriv 15
- statusRwPriv 15

module: Security(access)

- configRoPriv 10
- configRwPriv 10
- statusRoPriv 5
- statusRwPriv 10

module: Others

- configRoPriv 5
- configRwPriv 10
- statusRoPriv 5
- statusRwPriv 10

Format

web privilege group *<cword>* level { [configRoPriv *<0-15>*] [configRwPriv *<0-15>*] [statusRoPriv *<0-15>*] [statusRwPriv *<0-15>*] }

Mode

Global Configuration Mode

no web privilege

This command restores the default module privilege level.

Format

```
no web privilege group [ <cword> ] level
```

Mode

```
Global Configuration Mode
```

50.2. show

50.2.1. show web privilege

This command is used to view the configured module privilege levels. The parameter <*cword*> is the web group name defined by system.

Format

```
show web privilege group [ <cword> ] level
```

Mode

```
User EXEC Mode
```

51. Private VLAN

Private VLANs partition a physical VLAN into multiple virtual VLANs, allowing for the isolation of different groups of users on the same physical network, primarily to enhance security and manage network traffic capabilities.

51.1. pvlan

51.1.1. pvlan

This command is used to add a port to a PVLAN.

Default

```
none
```

Format

```
pvlan <range_list>
```

Mode

```
Port Configuration Mode
```

■ no pvlan

This command is used to remove a port to a PVLAN.

Format

```
no pvlan <range_list>
```

Mode

```
Port Configuration Mode
```

51.1.2. pvlan isolation

This command is used to add the port into an isolation group.

Default

```
none
```

Format

```
pvlan isolation
```

Mode

```
Port Configuration Mode
```

■ no pvlan isolation

This command is used to remove the port out of an isolation group.

Format

```
no pvlan isolation
```

Mode

```
Port Configuration Mode
```

51.2. show

51.2.1. show pvlan

This command is used to show pvlan configuration/status.

Format

```
show pvlan { [ <range_list> | isolation ] }
```

Mode

```
User EXEC Mode
```

52. Port Security

Port security allows network administrators to limit the number of MAC addresses that a switch port can learn, thereby providing control over network access. This section can cover topics such as MAC address limitation, aging time configuration, and setting the maximum number of violation addresses.

52.1. port-security

52.1.1. port-security aging

This command is used to enable port security aging.

Default

```
disable
```

Format

```
port-security aging
```

Mode

```
Global Configuration Mode
```

■ no port-security aging

This command is used to disable port security aging.

Format

```
no port-security aging
```

Mode

```
Global Configuration Mode
```

52.1.2. port-security aging time

This command is used to configure the aging time for dynamic MAC addresses in port security.<*uint*> represents aging period in seconds, the aging period can be set to a number between 10 and 10000000 seconds with a default of 3600 seconds.

Default

```
3600
```

Format

```
port-security aging time <uint>
```

Mode

```
Global Configuration Mode
```

■ no port-security aging time

This command is used to restore the default aging time to 3600 seconds.

Format

```
no port-security aging time
```

Mode

```
Global Configuration Mode
```

52.1.3. port-security hold time

This command is used to configure the violating MAC addresses are held non-forwarding for this amount of seconds. <*uint*> represents hold time in seconds, valid range is between 10 and 10000000 seconds with a default of 300 seconds.

Default

```
300
```

Format

```
port-security hold time <uint>
```

Mode

```
Global Configuration Mode
```

■ no port-security hold time

This command is used to restore the default hold time to 300 seconds.

Format

```
no port-security hold time
```

Mode

```
Global Configuration Mode
```

52.1.4. port-security

This command is used to enable port security per interface.

Default

```
disable
```

Format

```
port-security
```

Mode

```
Port Configuration Mode
```

■ no port-security

This command is used to disable port security per interface.

Format

```
no port-security
```

Mode

```
Port Configuration Mode
```

52.1.5. port-security maximum

This command is used to configure the maximum number of MAC addresses that can be learned on this set of interfaces. <*uint*> represents the maximum number of MAC addresses that can be secured on this port, this number cannot exceed 1023, default is 4.

Default

```
4
```

Format

```
port-security maximum <uint>
```

Mode

```
Port Configuration Mode
```

no port-security maximum

This command is used to restore the default maximum number of MAC addresses that can be secured on this port to 4.

Format

```
no port-security maximum
```

Mode

```
Port Configuration Mode
```

52.1.6. port-security violation

This command is used to configure the action taken if limit is exceeded. The optional parameters respectively represent don't do anything, keep recording violating MAC addresses, shutdown the port.

Default

```
protect
```

Format

```
port-security violation { protect | restrict | shutdown }
```

Mode

```
Port Configuration Mode
```

no port-security violation

This command is used to restore the default action taken to protect.

Format

```
no port-security violation
```

Mode

```
Port Configuration Mode
```

52.1.7. port-security maximum-violation

This command is used to configure the maximum number of violating MAC addresses (used when violation is restrict). <*uint*> represents the maximum number of MAC addresses that can be marked as violating on this port, this number cannot exceed 1023, default is 4.

Default

```
4
```

Format

```
port-security maximum-violation <uint>
```

Mode

```
Port Configuration Mode
```

no port-security maximum-violation

This command is used to restore the default maximum number of MAC addresses that can be marked as violating on this port to 4.

Format

```
no port-security maximum-violation
```

Mode

```
Port Configuration Mode
```

52.1.8. port-security mac-address sticky

This command is used to enable sticky learning of MAC addresses on this port. When the port is in sticky mode, all MAC addresses that would otherwise have been learned as dynamic are learned as sticky.

Default

```
disable
```

Format

```
port-security mac-address sticky
```

Mode

```
Port Configuration Mode
```

■ no port-security mac-address sticky

This command is used to disable sticky learning of MAC addresses on this port.

Format

```
no port-security mac-address sticky
```

Mode

```
Port Configuration Mode
```

52.1.9. port-security mac-address

This command is used to add a static (or sticky, though not recommended) MAC address on interface. <*mac_ucast*> represents unicast MAC address. <*vlan_id*> represents VLAN ID.

Default

```
none
```

Format

```
port-security mac-address { [ sticky ] [ <mac_ucast> [ vlan <vlan_id> ] ] }*1
```

Mode

```
Port Configuration Mode
```

■ no port-security mac-address

This command is used to delete a static (or sticky, though not recommended) MAC address on interface. <*mac_ucast*> represents unicast MAC address. <*vlan_id*> represents VLAN ID.

Format

```
no port-security mac-address { [ sticky ] [ <mac_ucast> [ vlan <vlan_id> ] ] }*1
```

Mode

```
Port Configuration Mode
```

52.2. show

52.2.1. show port-security

This command is used to display the port security overview status. *<port_type_list>* represents port.

Format

```
show port-security [ interface <port_type_list> ]
```

Mode

```
User EXEC Mode
```

52.2.2. show port-security address

This command is used to display MAC addresses learned by port security. <*port_type_list*> represents port.

Format

```
show port-security address [ interface <port_type_list> ]
```

Mode

```
User EXEC Mode
```

52.3. clear

52.3.1. clear port-security dynamic

This command is used to remove specific MAC addresses, all on one or more ports or all on a given VLAN. <*mac_addr*> represents MAC address to clear. <*vlan_id*> represents VLAN on which to delete all MAC addresses. <*port_type_list*> represents port.

Format

```
clear port-security dynamic [ { address <mac_addr> [ vlan <vlan_id> ] } | { interface
<port_type_list> [ vlan <vlan_id> ] } | vlan <vlan_id> ]
```

Mode

```
User EXEC Mode
```

53. PTP

PTP (Precision Time Protocol), standardized as IEEE 1588, is used for transmitting precise time synchronization information across local area networks.

53.1. ptp

53.1.1. ptp ext

This command is used to update the 1PPS and External clock output configuration and the preferred clock rate adjustment option. The optional parameters respectively represent enable 1PPS output. Enable external clock frequency output, <1-25000000> External Clock output frequency in Hz. Select Local Time Counter (LTC) frequency control. Select SyncE DPLL frequency control, if allowed by SyncE. Select an oscillator independent of SyncE for frequency control, if supported by the hardware. Select second DPLL for PTP, Both DPLL have the same (SyncE recovered) clock. AUTO Select clock control, based on PTP profile and available hardware resources.

Default

```
disable
```

Format

```
ptp ext [ output ] [ ext <1-25000000> ] [ ltc | single | independent | common | auto ]
```

Mode

```
Global Configuration Mode
```

no ptp ext

This command is used to configure the 1PPS and External clock output configuration and the preferred clock rate adjustment option to default.

Format

```
no ptp ext
```

Mode

```
Global Configuration Mode
```

53.1.2. ptp adj-method

This command is used to update the preferred clock rate adjustment option. The optional parameters respectively represent select Local Time Counter (LTC) frequency control, select SyncE DPLL frequency control, if allowed by SyncE, select an oscillator independent of SyncE for frequency control, if supported by the hardware, select second DPLL for PTP, Both DPLL have the same (SyncE recovered) clock, AUTO Select clock control, based on PTP profile and available hardware resources.

Default

```
auto
```

Format

```
ptp adj-method { ltc | single | independent | common | auto }
```

Mode

```
Global Configuration Mode
```

no ptp ext

This command is used to configure the preferred clock rate adjustment option to default.

Format

```
no ptp adj-method
```

Mode

```
Global Configuration Mode
```

53.1.3. ptp mode

This command is used to create a PTP clock instance. The range *<0-3>* indicates the clock instance, with optional parameters representing the following types: ordinary/boundary clock (boundary), end-to-end transparent clock (e2etransparent), peer-to-peer transparent clock (p2ptransparent), master-only clock (master), slave-only clock (slave), boundary clock frontend (bcfrontend), AED grandmaster clock (aedgm), and internal clock (internal). Additionally, the following parameters can be configured:
Clock Synchronization Steps: twostep: Two-step clock synchronization
Interface Transmission Types: ethernet: Ethernet ethernet-mixed: Mixed Ethernet ip4multi: IPv4 multicast ip4mixed: Mixed IPv4 ip4unicast: Unicast IPv4 ip6mixed: Mixed IPv6 ethip4ip6-combo: Ethernet IPv4 and IPv6 combo
VLAN Identifier: Specify VLAN ID
Profile Type: profile { ieee1588 | g8265.1 | g8275.1 | g8275.2 | 802.1as | 802.1as-aed }: Specify the profile type to use, including IEEE 1588, G8265.1, G8275.1, G8275.2, 802.1AS, and 802.1AS AED profiles
Clock Domain: clock-domain *<0-6>*: Defines the hardware clock domain used by this instance. Instances with different hardware clock domains can maintain different times.
Priority: dscp *<0-63>*: Configure the DSCP value to specify priority pcp *<0-7>*: Configure the PCP value (0 to 7) for VLAN frame priority marking.
These parameters allow for fine-tuned configuration of PTP clock instances to meet the needs of various network environments and application scenarios.

Default

```
none
```

Format

```
ptp <0-3> mode { boundary | e2etransparent | p2ptransparent | master | slave |
bcfrontend | aedgm | internal } [ onestep | twostep ] [ ethernet | ethernet-mixed | ip4multi
| ip4mixed | ip4unicast | oam | onepps | ip6mixed | ethip4ip6-combo ] [ oneway | twoway ]
[ id <clock_id> ] [ vid <vlan_id> [ <0-7> ] ] [ mep <1-100> ] [ profile { ieee1588 |
g8265.1 | g8275.1 | g8275.2 | 802.1as | 802.1as-aed} ] [ clock-domain <0-6> ] [ dscp
<0-63> ]
```

Mode

```
Global Configuration Mode
```

no ptp mode

This command is used to delete a PTP clock instance.

Format

```
no ptp <0-3> mode { boundary | e2etransparent | p2ptransparent | master | slave |
bcfrontend | aedgm | internal }
```

Mode

```
Global Configuration Mode
```

53.1.4. ptp priority1

This command is used to set the PTP clock priority1 value in a specific PTP instance, with a range of 0 to 255. This value is primarily used for the selection of the grandmaster clock in the PTP protocol; the smaller the value, the higher the priority of the device.

Default

128

Format

ptp *<0-3>* priority1 *<0-255>*

Mode

Global Configuration Mode

■ no ptp priority1

This command is used to restore the PTP clock priority1 value to its default setting.

Format

no ptp *<0-3>* priority1

Mode

Global Configuration Mode

53.1.5. ptp priority2

This command is used to set the PTP clock priority2 value in a specific PTP instance, with a range of 0 to 255. This value is primarily used for the selection of the grandmaster clock in the PTP protocol; the smaller the value, the higher the priority of the device.

Default

128

Format

ptp *<0-3>* priority2 *<0-255>*

Mode

Global Configuration Mode

■ no ptp priority2

This command is used to restore the PTP clock priority1 value to its default setting.

Format

no ptp *<0-3>* priority2

Mode

Global Configuration Mode

53.1.6. ptp domain

This command is used to set the PTP domain value in a specific PTP instance, with a range of 0 to 127. This value is primarily used to set the domain value in the PTP protocol, thereby dividing different PTP domains for clock synchronization and management.

Default

none

Format

ptp *<0-3>* domain *<0-127>*

Mode

Global Configuration Mode

no ptp domain

This command is used to restore the PTP domain value in a PTP instance to its default setting.

Format

```
no ptp <0-3> domain
```

Mode

```
Global Configuration Mode
```

53.1.7. ptp time-property

This command is used to set parameters related to time properties in the PTP protocol to ensure accurate time synchronization and related characteristics of the system. The specific meanings are as follows:
utc-offset <*-32768-32767*>: Sets the UTC offset value, ranging from -32768 to 32767. This parameter represents the offset between PTP time and UTC time (in seconds).
valid: Marks whether the UTC offset is valid. If this option is set, it indicates that the current UTC offset configuration is valid.
leap-59 | leap-61: Specifies the type of leap second adjustment: leap-59: Decrease by one second (indicating a negative leap second). leap-61: Increase by one second (indicating a positive leap second).
time-traceable: Indicates whether the time is traceable. If set, it means the system time is traceable, i.e., the system time source is verified and can be traced via the PTP protocol.
freq-traceable: Indicates whether the frequency is traceable. If set, it means the system's frequency information is traceable. ptptimescale: Indicates whether the PTP timescale is used. When this parameter is set, it enables the PTP timescale.
time-source <*0-255*>: Configures the time source, ranging from 0 to 255. This value represents the source of time information, with different time source types defined by the PTP protocol standard.
leap-pending <*word10*> { leap-59 | leap-61 }: Indicates upcoming leap second adjustments and specifies the type of leap second:
leap-pending <*word10*>: Indicates the pending status of a leap second adjustment. leap-59: An upcoming decrease by one second (negative leap second).
leap-61: An upcoming increase by one second (positive leap second).
By setting the above parameters, you can effectively manage and configure the time properties in the PTP protocol, ensuring the system time synchronization and consistency with other devices, and meeting the needs of different network environments and application scenarios.

Default

```
utc-offset: 0
Valid: No
leap-59: No
leap-61: No
time-traceable: No
freq-traceable: No
```

Format

```
ptp <0-3> time-property [ utc-offset <-32768-32767> ] [ valid ] [ leap-59 | leap-61 ]
[ time-traceable ] [ freq-traceable ] [ ptptimescale ] [ time-source <0-255> ]
[ leap-pending <word10> { leap-59 | leap-61 } ]
```

Mode

```
Global Configuration Mode
```

53.1.8. ptp servo ap

This command is used to set the value of the P parameter in the base convergence algorithm for a specific PTP instance. This parameter is primarily used to adjust the performance of the servo convergence algorithm to enhance the accuracy and stability of clock synchronization.

Default

2

Format

ptp *<0-3>* servo ap *<1-1000>*

Mode

Global Configuration Mode

■ no ptp servo ap

This command is used to restore the P parameter in the base convergence algorithm of a PTP instance to its default value.

Format

no ptp *<0-3>* servo ap

Mode

Global Configuration Mode

53.1.9. ptp servo ai

This command is used to set the value of the I parameter in the base convergence algorithm for a specific PTP instance. This parameter is primarily used to adjust the performance of the servo convergence algorithm to enhance the accuracy and stability of clock synchronization.

Default

20

Format

ptp *<0-3>* servo ai *<1-10000>*

Mode

Global Configuration Mode

■ no ptp servo ai

This command is used to restore the I parameter in the base convergence algorithm of a PTP instance to its default value.

Format

no ptp *<0-3>* servo ai

Mode

Global Configuration Mode

53.1.10. ptp servo ad

This command is used to set the value of the D parameter in the base convergence algorithm for a specific PTP instance. This parameter is primarily used to adjust the performance of the servo convergence algorithm to enhance the accuracy and stability of clock synchronization.

Default

30

Format

ptp *<0-3>* servo ad *<1-10000>*

Mode

Global Configuration Mode

no ptp servo ad

This command is used to restore the I parameter in the base convergence algorithm of a PTP instance to its default value.

Format

```
no ptp <0-3> servo ad
```

Mode

```
Global Configuration Mode
```

53.1.11. ptp servo gain

This command is used to set the value of the gain parameter in the base convergence algorithm for a specific PTP instance. This parameter is primarily used to adjust the performance of the servo convergence algorithm to enhance the accuracy and stability of clock synchronization.

Default

```
1
```

Format

```
ptp <0-3> servo gain <1-10000>
```

Mode

```
Global Configuration Mode
```

no servo gain

This command is used to restore the gain parameter in the base convergence algorithm of a PTP instance to its default value.

Format

```
no ptp <0-3> servo gain
```

Mode

```
Global Configuration Mode
```

53.1.12. ptp afi-announce

This command is used to configure a specific PTP instance on platforms that support AFI (Advanced Filtering and Insertion) to enable the sending of announce messages through the AFI mechanism. Using this command can enhance the efficiency and performance of the PTP protocol.

Default

```
enable
```

Format

```
ptp <0-3> afi-announce
```

Mode

```
Global Configuration Mode
```

no ptp afi-announce

This command is used to disable the sending of announce messages through the AFI mechanism.

Format

```
no ptp <0-3> afi-announce
```

Mode

```
Global Configuration Mode
```

53.1.13. ptp afi-sync

This command is used to configure a specific PTP instance on platforms that support AFI (Advanced Filtering and Insertion) to enable the sending of sync messages through the AFI mechanism. Using this command can enhance the efficiency and performance of the PTP protocol.

Default

```
enable
```

Format

```
ptp <0-3> afi-sync
```

Mode

```
Global Configuration Mode
```

■ no ptp afi-sync

This command is used to disable the sending of sync messages through the AFI mechanism.

Format

```
no ptp <0-3> afi-sync
```

Mode

```
Global Configuration Mode
```

53.1.14. ptp path-trace-enable

This command is used to enable the path trace feature for a PTP instance. Once this feature is enabled, the Path Trace TLV (Type-Length-Value) parameter will be included in the Announce messages of the IEEE 1588 protocol.

Default

```
disable
```

Format

```
ptp <0-3> path-trace-enable
```

Mode

```
Global Configuration Mode
```

■ no ptp path-trace-enable

This command is used to disable the path trace feature in a PTP instance.

Format

```
no ptp <0-3> path-trace-enable
```

Mode

```
Global Configuration Mode
```

53.1.15. ptp vlan-override

The function of this command is to modify the handling of PTP packets at startup so that VLAN tags are ignored when receiving and sending.

Default

```
disable
```

Format

```
ptp <0-3> vlan-override { enable | disable }
```

Mode

```
Global Configuration Mode
```

53.1.16. ptp

This command is used to configure a specific PTP instance based on ports, ensuring that its PTP messages operate under the specified ports.

Default

none

Format

ptp *<0-3>* [internal]

Mode

Global Configuration Mode

■ no ptp

This command indicates that the PTP messages under this PTP instance will no longer operate on the specified ports.

Format

no ptp *<0-3>*

Mode

Global Configuration Mode

53.1.17. ptp announce

This command is used to configure the transmission frequency and timeout period of announce messages in a PTP instance based on port configuration.

Default

interval 1

timeout 3

Format

ptp *<0-3>* announce { [interval { *<-3-4>* | stop | default }] [timeout *<1-10>*] }*1

Mode

Port Configuration Mode

■ no ptp announce

This command is used to restore the transmission frequency and timeout period of announce messages in a PTP instance based on port configuration.

Format

no ptp *<0-3>* announce { interval | timeout }

Mode

Port Configuration Mode

53.1.18. ptp sync-interval

This command is used to configure the transmission frequency of sync messages in a PTP instance based on port configuration.

Default

0, with a value of 0 indicating sending once per second.

Format

ptp *<0-3>* sync-interval { *<int>* | stop | default }

Mode

Port Configuration Mode

■ no ptp sync-interval

This command is used to restore the transmission frequency of sync messages to the default value in a PTP instance based on port configuration.

Format

```
no ptp <0-3> sync-interval
```

Mode

```
Port Configuration Mode
```

53.1.19. ptp delay-mechanism

This command is used in Port Configuration Mode to configure the delay measurement method between ports in a PTP clock instance. In the PTP protocol, different delay measurement mechanisms are used to calculate and compensate for transmission delays to achieve precise time synchronization.

Default

```
p2p
```

Format

```
ptp <0-3> delay-mechanism { e2e | p2p | common-p2p }
```

Mode

```
Port Configuration Mode
```

■ no ptp delay-mechanism

This command is used to restore the delay measurement method between ports in a PTP clock instance to the default setting based on port configuration.

Format

```
no ptp <0-3> delay-mechanism
```

Mode

```
Port Configuration Mode
```

53.1.20. ptp delay-asymmetry

This command is used in Port Configuration Mode to set path delay asymmetry in the IEEE 1588 Precision Time Protocol (PTP). The purpose of this command is to compensate for path delay asymmetry in the network to improve clock synchronization accuracy.
Positive Value: Used when the receive path delay is greater than the transmit path delay. It represents the amount of delay that needs to be compensated.
Negative Value: Used when the transmit path delay is greater than the receive path delay. It represents the amount of delay that needs to be compensated.

Default

```
0
```

Format

```
ptp <0-3> delay-asymmetry <-100000-100000>
```

Mode

```
Port Configuration Mode
```

■ no ptp delay-asymmetry

This command is used to restore the delay asymmetry value between ports in a PTP clock instance to the default setting based on port configuration.

Format

```
no ptp <0-3> delay-asymmetry
```

Mode

```
Port Configuration Mode
```

53.1.21. ptp ingress-latency

This command is used in Port Configuration Mode to configure the device's ingress delay. Ingress delay refers to the time delay between when a data packet is received at the network interface and when the device actually processes the packet internally.

Default

0

Format

ptp *<0-3>* ingress-latency *<-100000-100000>*

Mode

Port Configuration Mode

■ no ptp ingress-latency

This command is used to restore the ingress delay value between ports in a PTP clock instance to the default setting based on port configuration.

Format

no ptp *<0-3>* ingress-latency

Mode

Port Configuration Mode

53.1.22. ptp egress-latency

This command is used in Port Configuration Mode to configure the device's egress delay. Egress delay refers to the time delay from when a data packet is fully processed internally and ready to be sent to the network interface, to when the packet is actually transmitted from the network interface.

Default

0

Format

ptp *<0-3>* egress-latency *<-100000-100000>*

Mode

Port Configuration Mode

■ no ptp egress-latency

This command is used to restore the egress delay value between ports in a PTP clock instance to the default setting based on port configuration.

Format

no ptp *<0-3>* egress-latency

Mode

Port Configuration Mode

53.1.23. ptp master-only

This command is used in Port Configuration Mode to set the IEEE 1588 BMC (Best Master Clock) algorithm's masterOnly attribute. This attribute specifies whether the device can operate only as a master clock, not participating in slave clock election and synchronization.

Default

0

Format

ptp *<0-3>* master-only

Mode

Port Configuration Mode

■ no ptp master-only

This command is used in Port Configuration Mode to clear the masterOnly attribute of the 1588 BMC (Best Master Clock) algorithm. With this command, the device can participate in clock election and synchronization as either a master or a slave clock.

Format

```
no ptp <0-3> master-only
```

Mode

```
Port Configuration Mode
```

53.1.24. ptp mcast-dest

This command is used in Port Configuration Mode to set the multicast destination address for PTP, where ptp <*0-3*> mcast-dest default is used to set the default multicast destination address for the specified PTP port or instance.
Layer 2 multicast destination address: 0x01, 0x1b, 0x19, 0x00, 0x00, 0x00.
Layer 3 multicast IP address: 224.0.1.129.
ptp <*0-3*> mcast-dest link-local is used to set the link-local multicast destination address for the specified PTP port or instance.
Layer 2 multicast destination address: 0x01, 0x80, 0xC2, 0x00, 0x00, 0x0E.
Layer 3 multicast IP address: 224.0.0.107.

Default

```
default
```

Format

```
ptp <0-3> mcast-dest { default | link-local }
```

Mode

```
Port Configuration Mode
```

53.1.25. ptp mgtSettableLogSyncInterval

This command is used in port configuration mode to configure the frequency of sending sync messages in gPTP (Precision Time Protocol) clock instances. The command takes effect only when ptp usemgtSettableLogSyncInterval is set to 1. With this command, you can adjust the interval for sending sync messages to ensure the precision of time synchronization and optimize network bandwidth utilization.

Default

```
-3
```

Format

```
ptp <0-3> mgtSettableLogSyncInterval { <-7-4> | stop | default }
```

Mode

```
Port Configuration Mode
```

53.1.26. ptp usemgtSettableLogSyncInterval

This command is used in Port Configuration Mode to determine whether to enable the ptp mgtSettableLogSyncInterval command to configure the transmission frequency of sync messages in a gPTP (Generalized Precision Time Protocol) instance. By doing so, you can control the sync message transmission interval, thereby affecting the precision of time synchronization and network bandwidth utilization.

Default

```
0
```

Format

```
ptp <0-3> usemgtSettableLogSyncInterval <0-1>
```

Mode

```
Port Configuration Mode
```

53.1.27. ptp mgtSettableLogAnnounceInterval

This command is used in Port Configuration Mode to configure the transmission frequency of Announce messages in a gPTP (Generalized Precision Time Protocol) clock instance. This command takes effect only when ptp useMgmtSettableLogAnnounceInterval is set to 1. By using this command, you can adjust the Announce message transmission interval to ensure precise time synchronization and optimize network bandwidth utilization.

Default

0

Format

ptp *<0-3>* mgtSettableLogAnnounceInterval { *<-3-4>* | stop | default }

Mode

Port Configuration Mode

53.1.28. ptp usemgtSettableLogAnnounceInterval

This command is used in Port Configuration Mode to determine whether to enable the ptp mgtSettableLogAnnounceInterval command to configure the transmission frequency of Announce messages in a gPTP (Generalized Precision Time Protocol) instance. By doing so, you can control the Announce message transmission interval, thereby affecting the precision of time synchronization and network bandwidth utilization.

Default

0

Format

ptp *<0-3>* usemgtSettableLogSyncInterval *<0-1>*

Mode

Port Configuration Mode

53.1.29. ptp mgtSettableLogPdelayReqInterval

This command is used in Port Configuration Mode to configure the transmission frequency of peer_delay_request messages in a gPTP (Generalized Precision Time Protocol) clock instance. This command takes effect only when ptp useMgmtSettableLogPdelayReqInterval is set to 1. By using this command, you can adjust the peer_delay_request message transmission interval to ensure precise time synchronization and optimize network bandwidth utilization.

Default

0

Format

ptp *<0-3>* mgtSettableLogPdelayReqInterval { *<-7-5>* | stop | default }

Mode

Port Configuration Mode

53.1.30. ptp usemgtSettableLogPdelayReqInterval

This command is used in Port Configuration Mode to determine whether to enable the ptp mgtSettableLogPdelayReqInterval command to configure the transmission frequency of peer_delay_request messages in a gPTP (Generalized Precision Time Protocol) instance. By doing so, you can control the peer_delay_request message transmission interval, thereby affecting the precision of time synchronization and network bandwidth utilization.

Default

0

Format

ptp *<0-3>* usemgtSettableLogPdelayReqInterval *<0-1>*

Mode

Port Configuration Mode

53.1.31. ptp mgtSettableLogGptpCapableMessageInterval

This command is used in Port Configuration Mode to configure the transmission frequency of signaling messages in a PTP instance.

Default

```
0
```

Format

```
ptp <0-3> mgtSettableLogGptpCapableMessageInterval { <-7-4> | stop | default }
```

Mode

```
Port Configuration Mode
```

53.1.32. ptp useMgtSettableLogGptpCapableMessageInterval

This command is used to enable or disable the configuration parameter ptp mgtSettableLogGptpCapableMessageInterval.

Default

```
0
```

Format

```
ptp <0-3> useMgtSettableLogGptpCapableMessageInterval <0-1>
```

Mode

```
Port Configuration Mode
```

53.1.33. ptp two-step

This command is used to enable the Two-Step Clock mode. In Two-Step Clock mode, the time synchronization process is divided into two steps: first, a Sync Message is sent, followed by a Follow-Up Message that conveys the precise timestamp information. This method can improve the accuracy of time synchronization.

Default

```
none
```

Format

```
ptp <0-3> two-step [ true ]
```

Mode

```
Port Configuration Mode
```

■ no ptp two-step

This command is used in Port Configuration Mode to restore the Two-Step Clock mode to Default. After restoring to Default, the Two-Step Clock mode type configured for the PTP clock will take precedence. This command allows you to clear the port-level Two-Step Clock configuration, ensuring it follows the settings of the global PTP clock configuration.

Format

```
no ptp <0-3> two-step
```

Mode

```
Port Configuration Mode
```

53.1.34. ptp two-step false

This command is used to enable the One-Step Clock mode. In One-Step Clock mode, the time synchronization process is completed by sending a single Sync Message that contains the precise timestamp information. This method simplifies the time synchronization process and can reduce protocol overhead in certain scenarios.

Default

```
none
```

Format

```
ptp <0-3> two-step false
```

Mode

```
Port Configuration Mode
```

■ no ptp two-step

This command is used in Port Configuration Mode to restore the Two-Step Clock mode to Default. After restoring to Default, the Two-Step Clock mode type configured for the PTP clock will take precedence. This command allows you to clear the port-level Two-Step Clock configuration, ensuring it follows the settings of the global PTP clock configuration.

Format

```
no ptp <0-3> two-step
```

Mode

```
Port Configuration Mode
```

53.1.35. ptp 802.1as

This command is used to specify the version of the 802.1AS protocol being used. When configuring gPTP (Generalized Precision Time Protocol), select the appropriate version as needed. This ensures that the device operates with the specified version of the 802.1AS protocol to meet the time synchronization requirements of different network environments and needs.

Default

```
2020
```

Format

```
ptp <0-3> 802.1as { 2020 | 2011 }
```

Mode

```
Port Configuration Mode
```

53.1.36. ptp delay-thresh

This command is used to configure the measurement threshold for PeerMeanPathDelay in gPTP (Generalized Precision Time Protocol). If the measured PeerMeanPathDelay value exceeds the specified threshold and surpasses the maximum allowable fault count set by the ptp *<0-3>* allow-faults *<1-255>* command, the device will not trigger the gPTP clock synchronization process. This prevents unstable time synchronization states.

Default

```
800
```

Format

```
ptp <0-3> delay-thresh <0-4000000000>
```

Mode

```
Port Configuration Mode
```

■ no ptp delay-thresh

This command is used to restore the delay-thresh parameter of a specific gPTP instance to its default value.

Format

```
no ptp <0-3> delay-thresh
```

Mode

```
Port Configuration Mode
```

53.1.37. ptp allow-faults

This command is used to set the maximum number of consecutive faults allowed in the gPTP clock synchronization process. If the specified maximum allowable fault count is exceeded, the device will not trigger gPTP clock synchronization, thereby preventing inaccurate time synchronization states.

Default

```
9
```

Format

```
ptp <0-3> allow-faults <1-255>
```

Mode

```
Port Configuration Mode
```

■ no allow-faults

This command is used to restore the allow-faults parameter of a gPTP instance to its default value.

Format

```
no ptp <0-3> allow-faults
```

Mode

```
Port Configuration Mode
```

53.1.38. ptp sync-rx-to

This command is used to set the syncReceiptTimeout value for a gPTP protocol port, which represents the timeout duration in terms of the number of syncTimeIntervals. In the gPTP protocol, syncTimeInterval is a key parameter used to determine the interval at which Sync messages are sent. This time interval can be set using the ptp mgtSettableLogAnnounceInterval command.

Default

```
3
```

Format

```
ptp <0-3> sync-rx-to <1-255>
```

Mode

```
Port Configuration Mode
```

■ no ptp sync-rx-to

This command is used to restore the sync-rx-to parameter of a gPTP instance to its default value.

Format

```
no ptp <0-3> sync-rx-to
```

Mode

```
Port Configuration Mode
```

53.1.39. ptp allow-lost-resp

This command is used to configure the maximum number of times a peer_delay_req request message can be sent in gPTP (Generalized Precision Time Protocol) without receiving a response. If the number of unanswered peer_delay_req request messages exceeds the set value, the Pdelay response timeout counter will start, triggering the relevant handling process.

Default

3

Format

ptp *<0-3>* allow-lost-resp *<0-10>*

Mode

Port Configuration Mode

■ no ptp allow-lost-resp

This command is used to restore the allow-lost-resp parameter of a gPTP instance to its default value.

Format

no ptp *<0-3>* allow-lost-resp

Mode

Port Configuration Mode

53.1.40. ptp aed-port-role

This command is used in Port Configuration Mode and allows a port within the same PTP instance to be configured for its role under the AED (Alternate End-to-End Delay) timing mechanism. It can switch between the master port and the slave port roles.

Default

none

Format

ptp *<0-3>* aed-port-role { master | slave }

Mode

Port Configuration Mode

■ no ptp aed-port-role

This command is used to restore the port's role to its default value in port configuration mode.

Format

no ptp *<v_0_to_3>* aed-port-role { master | slave }

Mode

Port Configuration Mode

53.1.41. ptp delay-req

This command is used in Port Configuration Mode to configure the transmission frequency of delay messages in a PTP instance.

Default

0, indicates that one message is sent per second.

Format

ptp *<0-3>* delay-req interval { *<-7-5>* | stop | default }

Mode

Port Configuration Mode

■ no ptp delay-req

This command is used in Port Configuration Mode to restore the transmission frequency of delay messages in a PTP instance to the default setting.

Format

```
no ptp <0-3> delay-req interval
```

Mode

```
Port Configuration Mode
```

53.1.42. ptp gptp-to

This command is used to set the timeout value for Signal messages in gPTP on a port. The value represents the number of intervals for the Signal message timeout. This value multiplied by the message transmission frequency equals the message timeout value.

Default

```
0, indicates that one message is sent per second.
```

Format

```
ptp <0-3> gptp-to <1-255>
```

Mode

```
Port Configuration Mode
```

■ no ptp gptp-to

This command is used in Port Configuration Mode to restore the timeout interval for signal messages in a PTP instance to the default value.

Format

```
no ptp <0-3> gptp-to
```

Mode

```
Port Configuration Mode
```

53.1.43. ptp gptp-interval

This command is used in Port Configuration Mode to configure the transmission frequency of signal messages in a PTP instance.

Default

```
0, indicates that one message is sent per second.
```

Format

```
ptp <0-3> gptp-interval { <int> | stop | default }
```

Mode

```
Port Configuration Mode
```

■ no ptp gptp-interval

This command is used in Port Configuration Mode to restore the transmission frequency of signal messages in a PTP instance to the default setting.

Format

```
no ptp <0-3> gptp-interval
```

Mode

```
Port Configuration Mode
```

53.1.44. ptp statistics

This command is used in Port Mode to query or clear the PTP message statistics for a specific PTP instance.

Default

none

Format

ptp <*0-3*> statistics [clear]

Mode

Port Configuration Mode

53.1.45. ptp system-time

This command is used to manage synchronization operations between the system time and the hardware clock in the PTP protocol. The specific meanings are as follows:
get <*0-3*>: This operation is only applicable to instances where the clock type is "Masteronly." Using this operation, the system time of the device can be periodically synchronized to the hardware clock domain of the specified PTP instance (<*0-3*>).
set: This operation periodically synchronizes the time in hardware clock domain 0 to the system time of the device, ensuring that the system time remains consistent with the PTP hardware clock.

Default

none

Format

ptp system-time { get <*0-3*> | set }

Mode

Global Configuration Mode

no ptp system-time

This command is used to stop the synchronization operations between the system time and the hardware clock in the PTP protocol.

Format

no ptp system-time

Mode

Global Configuration Mode

53.1.46. ptp local-clock

This command is used to manage the local hardware clock of a specified PTP clock instance (<*0-3*>). The specific meanings are as follows:
update: Synchronizes the system time of the device to the hardware clock domain of the specified PTP clock instance, ensuring that the hardware clock is consistent with the system time.
ratio <*-10000000-10000000*>: Adjusts the hardware clock frequency of the specified PTP clock instance. The ratio parameter ranges from -10000000 to 10000000 and is used to fine-tune the hardware clock rate to accurately synchronize time.
With the above commands, you can effectively manage and synchronize the system time with the hardware clock domain of the specified PTP clock instance, while also providing the necessary frequency adjustment capability to maintain the accuracy of time synchronization.

Default

none

Format

ptp <*0-3*> local-clock { update | ratio <*-10000000-10000000*> }

Mode

User EXEC Mode

53.1.47. ptp whitelist

This command is used to enable the PTP whitelist switch. When enabled, devices in the whitelist can synchronize the clock with this device; otherwise, clock synchronization is not allowed.

Default

```
disable
```

Format

```
ptp whitelist { enable | disable }
```

Mode

```
Global Configuration Mode
```

53.1.48. ptp whitelist <0-9>

This command is used to configure the PTP whitelist information. The list becomes effective when the PTP whitelist switch is enabled.

Default

```
none
```

Format

```
ptp whitelist <0-9> clock-identity <word23>
```

Mode

```
Global Configuration Mode
```

53.2. show

53.2.1. show ptp ext

This command is used to show the 1PPS and External clock output configuration and vcxo frequency rate adjustment option.

Format

```
show ptp ext
```

Mode

```
User EXEC Mode
```

53.2.2. show ptp

This command is used to query the static or dynamic service data of a PTP instance. The main parameters are as follows:
default: This command is used to display the default configuration data of the specified PTP instance.
current: This command is used to display the status information of the specified PTP instance.
parent: This command is used to display the status information of the Grandmaster Clock of the specified PTP instance.
time-property: This command is used to display the time-property configuration data of the specified PTP instance.
servo: This command is used to display the convergence algorithm parameters of the specified PTP instance.
port-ds: This command is used to display the PTP configuration data (Port Dataset) for the port configuration of the specified PTP instance. The Port Dataset contains port configuration information and attributes related to the PTP protocol.
port-state: This command is used to display the port status data of the specified PTP instance.
port-statistics: This command is used to display the port statistics data of the specified PTP instance.
vlan-override: This command is used to query whether the PTP function that ignores VLAN tags is currently enabled.

Format

```
show ptp <0-3> { default | current | parent | time-property | filter | servo | clk | ho | uni | master-table-unicast | slave [ details ] | { { port-state | port-statistics | port-ds | wireless | foreign-master-record } [ interface <port_type_list> ] } | log-mode | vlan-override }
```

Mode

```
User EXEC Mode
```

53.2.3. show ptp local-clock

This command is used to display the local clock time information of the specified clock instance.

Format

```
show ptp <0-3> local-clock
```

Mode

```
User EXEC Mode
```

53.2.4. show ptp whitelist

This command is used to display the PTP whitelist configuration information.

Format

```
show ptp whitelist { <0-9> | all }
```

Mode

```
User EXEC Mode
```

54. QoS

QoS functionality is used to ensure that network traffic is effectively managed, with data of differing priorities receiving appropriate handling, particularly in times of network congestion. The key features include traffic classification, traffic marking, queue management, scheduling policies, among others.

54.1. qos

54.1.1. qos cos

This command is used to configure the class of service of QoS port. <*0-7*> represents specific class of service.

Default

```
0
```

Format

```
qos cos <0-7>
```

Mode

```
Port Configuration Mode
```

■ no qos cos

This command is used to configure the class of service of QoS port to the default value.

Format

```
no qos cos
```

Mode

```
Port Configuration Mode
```

54.1.2. qos dpl

This command is used to configure the drop precedence level of QoS port. <*0-3*> represents specific drop precedence level.

Default

```
0
```

Format

```
qos dpl <0-3>
```

Mode

```
Port Configuration Mode
```

■ no qos dpl

This command is used to configure the drop precedence level of QoS port to the default value.

Format

```
no qos dpl
```

Mode

```
Port Configuration Mode
```

54.1.3. qos pcp

This command is used to configure the priority code point of QoS port. *<0-7>* represents specific Priority Code Point.

Default

0

Format

qos pcp *<0-7>*

Mode

Port Configuration Mode

no qos pcp

This command is used to configure the priority code point of QoS port to the default value.

Format

no qos pcp

Mode

Port Configuration Mode

54.1.4. qos dei

This command is used to configure the drop eligible indicator of QoS port. *<0-1>* represents specific Drop Eligible Indicator.

Default

0

Format

qos dei *<0-1>*

Mode

Port Configuration Mode

no qos dei

This command is used to configure the drop eligible indicator of QoS port to the default value.

Format

no qos dei

Mode

Port Configuration Mode

54.1.5. qos class

This command is used to configure the class of service ID of QoS port. *<0-7>* represents specific class of service ID.

Default

0

Format

qos class *<0-7>*

Mode

Port Configuration Mode

no qos class

This command is used to configure the class of service ID of QoS port to the default value.

Format

```
no qos class
```

Mode

```
Port Configuration Mode
```

54.1.6. qos trust tag

This command is used to trust the QoS port with tagged traffic.

Default

```
disabled
```

Format

```
qos trust tag
```

Mode

```
Port Configuration Mode
```

no qos trust tag

This command is used to discard the QoS port with tagged traffic.

Format

```
no qos trust tag
```

Mode

```
Port Configuration Mode
```

54.1.7. qos trust dscp

This command is used to enable the DSCP Based of QoS port.

Default

```
disabled
```

Format

```
qos trust dscp
```

Mode

```
Port Configuration Mode
```

no qos trust dscp

This command is used to disable the DSCP Based of QoS port.

Format

```
no qos trust dscp
```

Mode

```
Port Configuration Mode
```

54.1.8. qos wred-group

This command is used to configure the WRED group of QoS port. *<1-3>* represents specific WRED group.

Default

```
1
```

Format

```
qos wred-group <1-3>
```

Mode

```
Port Configuration Mode
```

■ no qos wred-group

This command is used to configure the WRED group of QoS port to the default value.

Format

```
no qos wred-group
```

Mode

```
Port Configuration Mode
```

54.1.9. qos ingress-map

This command is used to configure the ingress map association of QoS port. *<0-255>* represents map ID.

Default

```
none
```

Format

```
qos ingress-map <0-255>
```

Mode

```
Port Configuration Mode
```

■ no qos ingress-map

This command is used to configure the ingress map association of QoS port to the default value.

Format

```
no qos ingress-map
```

Mode

```
Port Configuration Mode
```

54.1.10. qos egress-map

This command is used to configure the egress map association of QoS port. *<0-511>* represents map ID.

Default

```
none
```

Format

```
qos egress-map <0-511>
```

Mode

```
Port Configuration Mode
```

no qos egress-map

This command is used to configure the egress map association of QoS port to the default value.

Format

```
no qos egress-map
```

Mode

```
Port Configuration Mode
```

54.1.11. qos policer

This command is used to configure the policing of QoS port, including enabling policies, setting rates and units, and controlling flow rates.

Default

```
disable
```

Format

```
qos policer <uint> [ kbps | mbps | fps | kfps ] [ flowcontrol ]
```

Mode

```
Port Configuration Mode
```

no qos policer

This command is used to configure the policing of QoS port to the default value.

Format

```
no qos policer
```

Mode

```
Port Configuration Mode
```

54.1.12. qos queue-policer

This command is used to configure the queue policing of QoS port including enabling queue policies, setting rates and units.

Default

```
disable
```

Format

```
qos queue-policer queue <0-7> <uint> [ kbps | mbps ]
```

Mode

```
Port Configuration Mode
```

no qos queue-policer queue

This command is used to configure the queue policing of QoS port to the default value.

Format

```
no qos queue-policer queue <0-7>
```

Mode

```
Port Configuration Mode
```

54.1.13. qos wrr

This command is used to configure the scheduler of QoS port. Eight set of <*1-100*> respectively represent weight for queue 0-7.

Default

none

Format

qos wrr <*1-100*> <*1-100*> [<*1-100*> [<*1-100*> [<*1-100*> [<*1-100*> [<*1-100*> [<*1-100*>]]]]]]

Mode

Port Configuration Mode

no qos wrr

This command is used to configure the scheduler of QoS port to the default value.

Format

no qos wrr

Mode

Port Configuration Mode

54.1.14. qos shaper

This command is used to configure the shaper of QoS port. <*uint*> represents shaper rate (default kbps). Internally rounded up to the nearest value supported by the port shaper. "kbps" represents unit is kilobits per second (default). "mbps" represents unit is megabits per second. "rate-type" represents setup shaping rate type, include line rate shaping and data rate shaping.

Default

none

Format

qos shaper <*uint*> [kbps | mbps] [rate-type { line | data }]

Mode

Port Configuration Mode

no qos shaper

This command is used to configure the shaper of QoS port to the default value.

Format

no qos shaper

Mode

Port Configuration Mode

54.1.15. qos queue-shaper queue

This command is used to configure the queue shaper of QoS port. <*0-7*> represents specific queue or range, <*uint*> represents Shaper rate (default kbps). Internally rounded up to the nearest value supported by the queue shaper. "kbps" represents unit is kilobits per second (default). "mbps" represents unit is megabits per second. excess represents allow use of excess bandwidth. "credit" represents allow use of credit based shaper. "rate-type" represents setup shaping rate type, include line rate shaping and data rate shaping.

Default

```
none
```

Format

```
qos queue-shaper queue <0-7> <uint> [ kbps | mbps ] [ excess | credit ] [ rate-type { line | data } ]
```

Mode

```
Port Configuration Mode
```

no qos queue-shaper queue

This command is used to configure the queue shaper of QoS port to the default value.

Format

```
no qos queue-shaper queue <0-7>
```

Mode

```
Port Configuration Mode
```

54.1.16. qos tag-remark

This command is used to configure the tag remarking of QoS port. "pcp <*0-7*>" represents specify PCP. "dei <*0-1*>" represents specific DEI. "mapped" represents use mapped values (COS, DPL -> PCP, DEI).

Default

```
none
```

Format

```
qos tag-remark { pcp <0-7> dei <0-1> | mapped }
```

Mode

```
Port Configuration Mode
```

no qos tag-remark

This command is used to configure the tag remarking of QoS port to the default value.

Format

```
no qos tag-remark
```

Mode

```
Port Configuration Mode
```

54.1.17. qos dscp-translate

This command is used to configure uplink port mapping for port DSCP.

Default

```
disable
```

Format

```
qos dscp-translate
```

Mode

```
Port Configuration Mode
```

no qos dscp-translate

This command is used to configure the DSCP translate of QoS port to the default value.

Format

```
no qos dscp-translate
```

Mode

```
Port Configuration Mode
```

54.1.18. qos dscp-classify

This command is used to configure the DSCP classifies of QoS port. "zero" represents classify to new DSCP if DSCP is 0. "selected" represents Classify to new DSCP if classify is enabled for specific DSCP value in global DSCP classify map. "any" represents classify to new DSCP always.

Default

```
disable
```

Format

```
qos dscp-classify { zero | selected | any }
```

Mode

```
Port Configuration Mode
```

no qos dscp-classify

This command is used to configure the DSCP classifies of QoS port to the default value.

Format

```
no qos dscp-classify
```

Mode

```
Port Configuration Mode
```

54.1.19. qos dscp-remark

This command is used to configure the DSCP remark of QoS port. "rewrite" represents rewrite DSCP field with classified DSCP value (no translation). "remap" represents rewrite DSCP field using classified DSCP and DPL=0 remapped through global dscp-egress-translation map. "remap-dp" represents rewrite DSCP field using classified DSCP and DPL remapped through global DSCP egress translation map.

Default

```
disable
```

Format

```
qos dscp-remark { rewrite | remap | remap-dp }
```

Mode

```
Port Configuration Mode
```

no qos dscp-remark

This command is used to configure the DSCP remark of QoS port to the default value.

Format

```
no qos dscp-remark
```

Mode

```
Port Configuration Mode
```

54.1.20. qos map dscp-cos

This command is used to configure the basic QoS inbound classification settings based on QoS DSCP. *<0-63>* represents specific DSCP or range. "cos *<0-7>*" represents specific class of service. "dpl *<dpl>*" represents specific drop precedence level.

Default

```
disable
```

Format

```
qos map dscp-cos { <0-63> | <dscp> } cos <0-7> dpl <dpl>
```

Mode

```
Global Configuration Mode
```

no qos map dscp-cos

This command is used to configure the basic QoS inbound classification settings based on QoS DSCP to the default value.

Format

```
no qos map dscp-cos { <0-63> | <dscp> }
```

Mode

```
Global Configuration Mode
```

54.1.21. qos map dscp-ingress-translation

This command is used to configure the Map for DSCP ingress translation. *<0-63>* represents specific DSCP or range. *<0-63>* represents translated DSCP value.

Default

```
0
```

Format

```
qos map dscp-ingress-translation { <0-63> | <dscp> } to { <0-63> | <dscp> }
```

Mode

```
Global Configuration Mode
```

no qos map dscp-ingress-translation

This command is used to configure the Map for DSCP ingress translation to the default.

Format

```
no qos map dscp-ingress-translation { <0-63> | <dscp> }
```

Mode

```
Global Configuration Mode
```

54.1.22. qos map dscp-egress-translation

This command is used to configure DSCP downlink mapping. *<0-63>* represents specific DSCP or range. *<0-1>* represents specific drop precedence level or range. *<0-63>* represents translated DSCP value.

Default

```
0
```

Format

```
qos map dscp-egress-translation { <0-63> | <dscp> } <0-1> to { <0-63> | <dscp> }
```

Mode

```
Global Configuration Mode
```

no qos map dscp-egress-translation

This command is used to set the DSCP downlink mapping to the default value. *<0-63>* represents specific DSCP or range.

Format

```
no qos map dscp-egress-translation { <0-63> | <dscp> }
```

Mode

```
Global Configuration Mode
```

54.1.23. qos map dscp-classify

This command is used to configure the Map for DSCP classifies enable. *<0-63>* represents specific DSCP or range.

Default

```
0
```

Format

```
qos map dscp-classify { <0-63> | <dscp> }
```

Mode

```
Global Configuration Mode
```

no qos map dscp-egress-translation

This command is used to configure the Map for DSCP classifies disable.

Format

```
no qos map dscp-classify { <0-63> | <dscp> }
```

Mode

```
Global Configuration Mode
```

54.1.24. qos map cos-dscp

This command is used to configure the Map for COS to DSCP. *<0~7>* represents specific class of service or range. *<0~3>* represents specific drop precedence level or range. *<0~63>* represents specific DSCP.

Default

```
0
```

Format

```
qos map cos-dscp <0~7> dpl <0~3> dscp { <0~63> | <dscp> }
```

Mode

```
Global Configuration Mode
```

no qos map cos-dscp

This command is used to configure the Map for COS to DSCP to default.

Format

```
no qos map cos-dscp <0~7> dpl <0~3>
```

Mode

```
Global Configuration Mode
```

54.1.25. qos map cos-tag

This command is used to configure the Map for COS to TAG. *<0~7>* represents specific class of service or range. *<0~1>* represents specific drop precedence level or range. *<0-7>* represents specific PCP. *<0-1>* represents Specific DEI.

Default

0

Format

qos map cos-tag cos *<0~7>* dpl *<0~1>* pcp *<0-7>* dei *<0-1>*

Mode

Port Configuration Mode

■ no qos map cos-tag

This command is used to configure the Map for COS to TAG to default.

Format

no qos map cos-tag cos *<0~7>* dpl *<0~1>*

Mode

Port Configuration Mode

54.1.26. qos map tag-cos

This command is used to configure the Map for COS to DSCP. *<0~7>* represents specific PCP or range. *<0~1>* represents specific DEI or range. *<0-7>* represents specific class of service. *<dpl>* represents specific drop precedence level.

Default

0

Format

qos map tag-cos pcp *<0~7>* dei *<0~1>* cos *<0-7>* dpl *<dpl>*

Mode

Port Configuration Mode

■ no qos map tag-cos

This command is used to configure the Map for TAG to COS to default.

Format

no qos map tag-cos pcp *<0~7>* dei *<0~1>*

Mode

Port Configuration Mode

54.1.27. qos map ingress

This command is used to enter the QoS Ingress Map view. *<0-255>* represents map ID.

Default

none

Format

qos map ingress *<0-255>*

Mode

Global Configuration Mode

no qos map ingress

This command is used to delete the created QoS Ingress Map view.

Format

```
no qos map ingress <0-255>
```

Mode

```
Global Configuration Mode
```

54.1.28. qos map egress

This command is used to enter the downlink mapping view of Qos. *<0-511>* represents map ID.

Default

```
none
```

Format

```
qos map egress <0-511>
```

Mode

```
Global Configuration Mode
```

no qos map egress

This command is used to delete the created QoS Egress Map view.

Format

```
no qos map egress <0-511>
```

Mode

```
Global Configuration Mode
```

54.1.29. qos qce (global)

This command is used to configure the QoS Control List. Update represents update an existing QCE. *<uint>* represents QCE ID. "next" represents place QCE before the next QCE ID, *<uint>* represents the next QCE ID. Last represents place QCE at the end. "interface *<port_type_list>*" represents interfaces and port list. "smac" represents setup matched SMAC, *<mac_addr>* represents matched SMAC (XX-XX-XX-XX-XX-XX). *<oui>* represents matched SMAC OUI (XX-XX-XX). "any" represents match any SMAC. "dmac" represents setup matched DMAC, *<mac_addr>* represents matched DMAC (XX-XX-XX-XX-XX-XX). Unicast represents match unicast DMAC, "multicast" represents match multicast DMAC. "broadcast" represents match broadcast DMAC. "any" represents match any DMAC. "tag" represents setup matched tag type, include untagged frames, tagged frames, c-tagged frames, s-tagged frames, or match tagged and untagged frames. Vid represents setup matched VLAN ID, include match VLAN ID value, range, or any VLAN ID. "pcp" represents setup matched PCP, include match PCP value, range, or any PCP. "dei" represents setup matched DEI, include match DEI, any DEI. Inner-tag represents setup inner tag options, include match untagged frames, match tagged frames, c-tagged represents match C-tagged frames, s-tagged represents match S-tagged frames. "any" represents match tagged and untagged frames. "frame-type" represents setup matched frame type, include match any frame type, match EtherType frames, matched EtherType. "llc" represents match LLC frames, include matched LLC DSAP, match any LLC DSAP, matched LLC SSAP, match any LLC SSAP, matched LLC Control byte, match any LLC Control byte. snap represents match SNAP frames, include setup matched SNAP EtherType, match any SNAP EtherType. "ipv4" represents match IPv4 frames, include matched IP protocol, match TCP frames, match UDP frames, match any IP protocol. "sip" represents setup matched source IP address, include matched source IP address/mask, include match any source IP address. "dip" represents setup matched destination IP address, include matched destination IP address/mask, match any destination IP address. "dscp" represents setup matched DSCP, include matched DSCP value/range, match any DSCP, Fragment represents setup matched IPv4 fragments, include match IPv4 fragments, match IPv4 non-fragments, match any IPv4 fragments. "sport" represents setup matched UDP/TCP source port, include match UDP/TCP source port value/range, match any UDP/TCP source port. "dport" represents setup matched UDP/TCP destination port, include match UDP/TCP destination port value/range, match any UDP/TCP destination port. Ipv6 represents match IPv6 frames, include matched IP protocol, match TCP frames, match UDP frames, match any IP protocol. "action" represents setup action, include assign class of service, keep existing class of service. "dpl" represents setup drop precedence level action, include assign drop precedence level, keep existing drop precedence level. "pcp-dei" represents setup PCP and DEI action, include assign PCP, assign DEI, keep existing PCP and DEI, "dscp" represents setup DSCP action, include assign DSCP, keep existing DSCP. "policy" represents setup ACL policy action, include assign ACL policy, keep existing ACL policy. "ingress-map" represents setup ingress map action, include assign ingress map id, keep existing ingress map.
Note: It is not recommended to configure the protocol value for IPv4 or IPv6 as 0 in QCE.

Default

none

Format

qos qce { [update] } *<uint>* [{ next *<uint>* } | last] [interface *<port_type_list>*] [smac { *<mac_addr>* | *<oui>* | any }] [dmac { *<mac_addr>* | unicast | multicast | broadcast | any }] [tag { [type { untagged | tagged | c-tagged | s-tagged | any }] [vid { *<vcap_vr>* | any }] [pcp { *<pcp>* | any }] [dei { *<0-1>* | any }] }*1] [inner-tag { [type { untagged | tagged | c-tagged | s-tagged | any }] [vid { *<vcap_vr>* | any }] [pcp { *<pcp>* | any }] [dei { *<0-1>* | any }] }*1] [frame-type { any | { etype [{ *<0x600-0x7ff,0x801-0x86dc,0x86de-0xffff>* | any }] } | { llc [dsap { *<0-0xff>* | any }] [ssap { *<0-0xff>* | any }] [control { *<0-0xff>* | any }] } | { snap [{ *<0-0xffff>* | any }] } | { ipv4 [proto { *<0-5,7-16,18-255>* | tcp [sport { *<vcap_vr>* | any }] [dport { *<vcap_vr>* | any }] | udp [sport { *<vcap_vr>* | any }] [dport { *<vcap_vr>* | any }] | any }] [sip { *<ipv4_subnet>* | any }] [dip { *<ipv4_subnet>* | any }] [dscp { *<vcap_vr>* | *<dscp>* | any }] [fragment { yes | no | any }] } | { ipv6 [proto { *<0-5,7-16,18-255>* | tcp [sport { *<vcap_vr>* | any }] [dport { *<vcap_vr>* | any }] | udp [sport { *<vcap_vr>* | any }] [dport { *<vcap_vr>* | any }] | any }] [sip { *<ipv4_subnet>* | any }] [dip { *<ipv4_subnet>* | any }] [dscp { *<vcap_vr>* | *<dscp>* | any }] } }] [action { [cos { *<0-7>* | default }] [dpl { *<dpl>* | default }] [pcp-dei { *<0-7>* *<0-1>* | default }] [dscp { *<0-63>* | *<dscp>* | default }] [policy { *<uint>* | default }] [ingress-map { *<uint>* | default }] }*1]

Mode

Global Configuration Mode

54.1.30. qos qce refresh

This command is used to refresh QCE tables in hardware.

Default

```
none
```

Format

```
qos qce refresh
```

Mode

```
Global Configuration Mode
```

54.1.31. qos qce (port)

This command is used to configure QoS control entry. "addr" represents setup address match mode. "source" represents match SMAC and SIP (default). "destination" represents match DMAC and DIP, setup ingress lookup key type, match outer tag, inner tag, IP protocol, DSCP and DPORT and so on. "key" represents setup ingress lookup key type. "double-tag" represents match outer tag, inner tag, IP protocol, DSCP and DPORT. "normal" represents match outer tag, SMAC/DMAC, IP protocol, DSCP, SIP/DIP, SPORT and DPORT (default). "ip-addr" represents match outer tag, SMAC/DMAC, IP protocol, DSCP, SIP and DIP. "mac-ip-addr" represents match outer tag, inner tag, SMAC, DMAC, IP protocol, DSCP, SIP, DIP, SPORT and DPORT.

Default

```
none
```

Format

```
qos qce { [ addr { source | destination } ] [ key { double-tag | normal | ip-addr
| mac-ip-addr } ] }
```

Mode

```
Port Configuration Mode
```

no qos qce

This command is used to reset address match mode to SMAC and SIP, or reset ingress lookup key type to normal.

Format

```
no qos qce { [ addr ] [ key ] }
```

Mode

```
Port Configuration Mode
```

54.1.32. qos storm (global)

This command is used to enable global unicast, multicast, broadcast, and configure rate. "unicast" represents police unicast frames. "broadcast" represents police broadcast frames. "multicast" represents police multicast frames. <*uint*> represents policer rate (default kbps), internally rounded up to the nearest value supported by the storm policer. "fps" represents unit is frames per second. "kfps" represents unit is kiloframes per second. "kbps" represents unit is kilobits per second (default). "mbps" represents unit is Megabits per second.The multicast rate limiting differs among different product models. Some models limit traffic where the 40th bit of the MAC address is 1, while other models exclude IPv4 multicast traffic with MAC addresses starting with 0x01005E and IPv6 multicast traffic with MAC addresses starting with 0x3333.

Default

```
disable
```

Format

```
qos storm { unicast | broadcast | multicast } <uint> [ fps | kfps | kbps | mbps ]
```

Mode

```
Global Configuration Mode
```

no qos storm (global)

This command is used to disable global unicast, multicast, broadcast.

Format

```
no qos storm { unicast | broadcast | multicast }
```

Mode

```
Global Configuration Mode
```

54.1.33. qos storm (port)

This command is used to enable unicast, unknown, broadcast, unknown-unicast, unknown-multicast and configure rate under the interface. "unicast" represents police unicast frames. "broadcast" represents police broadcast frames. "unknown" represents police unknown (flooded) frames. "unknown-unicast" represents police unknown unicast (flooded) frames. "unknown-multicast" represents police unknown multicast (flooded) frames. <*uint*> represents policer rate (default kbps), internally rounded up to the nearest value supported by the storm policer. "fps" represents unit is frames per second. "kfps" represents unit is kiloframes per second. "kbps" represents unit is kilobits per second (default). "mbps" represents unit is Megabits per second.

Default

```
disable
```

Format

```
qos storm { unicast | broadcast | unknown | unknown-unicast | unknown-multicast }
<uint> [ fps | kfps | kbps | mbps ]
```

Mode

```
Port Configuration Mode
```

no qos storm (port)

This command is used to disable unicast, unknown, broadcast, unknown-unicast, unknown-multicast under the interface.

Format

```
no qos storm { unicast | broadcast | unknown | unknown-unicast | unknown-multicast }
```

Mode

```
Port Configuration Mode
```

54.1.34. qos wred group

This command is used to configure the dpl, minimum fill level, maximum drop probability or fill level, or fill level of wred.

Default

```
disable
```

Format

```
qos wred group <1-3> queue <0-7> dpl <0-3> min-fl <0-100> max <1-100> [ fill-level ]
```

Mode

```
Global Configuration Mode
```

no qos wred group

This command is used to configure the dpl, minimum fill level, maximum drop probability or fill level, or fill level of wred to default.

Format

```
no qos wred group <1-3> queue <0-7> dpl <1-3>
```

Mode

```
Global Configuration Mode
```

54.2. key

54.2.1. key (ingress)

This command is used to configure classified PCP value as key, or configure classified PCP and DEI values as key, or configure the frame's DSCP value as key. For non-IP frames, no mapping is done, or configure the frame's DSCP value as key. For non-IP frames, use classified PCP and DEI values as key.

Default

```
pcp
```

Format

```
key { pcp | pcp-dei | dscp | dscp-pcp-dei }
```

Mode

```
QoS Ingress Map Mode
```

54.2.2. key (egress)

This command is used to configure classified COSID value as key, or configure classified COSID and DPL value as key, or configure classified DSCP value as key, or configure classified DSCP and DPL values as key.

Default

```
pcp
```

Format

```
key { class | class-dpl | dscp | dscp-dpl }
```

Mode

```
QoS Egress Map Mode
```

54.3. action

54.3.1. action (ingress)

This command is used to enable classification actions, enable classification of COSID, enable classification of COS, enable classification of DPL, enable classification of PCP, enable classification of DEI, enable classification of DSCP.

Default

```
disable
```

Format

```
action { [ class ] [ cos ] [ dpl ] [ pcp ] [ dei ] [ dscp ] }
```

Mode

```
QoS Ingress Map Mode
```

no active

This command is used to disable all actions.

Format

```
no active
```

Mode

```
QoS Ingress Map Mode
```

54.3.2. action (egress)

This command is used to enable rewriting of PCP, enable rewriting of DEI, enable rewriting of DSCP.

Default

```
disable
```

Format

```
action { [ pcp ] [ dei ] [ dscp ] }
```

Mode

```
QoS Egress Map Mode
```

no active

This command is used to disable all actions.

Format

```
no active
```

Mode

```
QoS Egress Map Mode
```

54.4. map

54.4.1. map (ingress)

This command is used to configure the mapping between keys and values. "dscp *<0-63>*" represents configure DSCP mapping, and specific DSCP or range. Pcp *<0-7>* represents configure PCP mapping, and specific PCP or range. "dei *<0-1>*" represents configure DEI mapping. If left out, only mapping for DEI 0 is configured, and Specific DEI or range. "to" represents specify the values that will be written to the frame when the key is matched and the action is enabled. "class *<0-7>*" represents configure COSID mapping, and specific COSID or range. cos *<0-7>* represents setup COS value. "dpl *<0-3>*" represents configure DPL mapping. If left out, only mapping for DPL 0 is configured, and specific DPL or range. "pcp *<0-7>*" represents Setup PCP value. "dei *<0-1>*" represents setup DEI value. "dscp *<0-63>*" represents setup DSCP value.

Default

```
0
```

Format

```
map { { dscp { <0-63> | <dscp> } } | { pcp <0-7> [ dei <0-1> ] } } to { [ class <0-7> ]
[ cos <0-7> ] [ dpl <0-3> ] [ pcp <0-7> ] [ dei <0-1> ] [ dscp <0-63> ] }
```

Mode

```
QoS Ingress Map Mode
```

54.4.2. map (egress)

This command is used to configure the mapping between keys and values. "dscp *<0-63>*" represents configure DSCP mapping, and specific DSCP or range. "class *<0-7>*" represents configure COSID mapping, and specific COSID or range. "dpl *<0-3>*" represents configure DPL mapping. If left out, only mapping for DPL 0 is configured, and specific DPL or range. "to" represents specify the values that will be written to the frame when the key is matched and the action is enabled. "pcp *<0-7>*" represents Setup PCP value. "dei *<0-1>*" represents setup DEI value. "dscp *<0-63>*" represents setup DSCP value.

Default

```
0
```

Format

```
map { { { dscp { <0-63> | <dscp> } } | { class <0-7> } } [ dpl <0-3> ] } to { [ pcp
<0-7> ] [ dei <0-1> ] [ dscp <0-63> ] }
```

Mode

```
QoS Egress Map Mode
```

54.5. show

54.5.1. show qos

This command is used to display qos-related information under a specified interface or all interfaces. By using different keywords to display different information, it can display wred, maps with *dscp-cos* to display Map for DSCP to COS, or with *dscp-ingress-translation* to display Map for DSCP ingress translation, or with *dscp-classify* to display Map for DSCP classify enable, or with *cos-dscp* to display Map for COS to DSCP, or with *dscp-egress-translation* to display Map for DSCP egress translation, and other combinations.

Default

```
oui
```

Format

```
show qos [ { interface [ <port_type_list> ] } | wred | { maps [ dscp-cos ]
[ dscp-ingress-translation ] [ dscp-classify ] [ cos-dscp ] [ dscp-egress-translation ]
[ { ingress [ <0-255> ] } ] [ { egress [ <0-511> ] } ] } | storm | { qce [ <1-256> ] } ]
```

Mode

```
User EXEC Mode
```

55. RedBox

The Redbox protocol is used in Time-Sensitive Networking (TSN) for the Redundancy Box (Redbox) protocol. It utilizes redundant network connections to ensure that data network connectivity and stability are maintained even if a single network link or device fails.

55.1. Mode

55.1.1. mode

This command is used to set the mode of this RedBox.

Default

```
prp-san
```

Format

```
mode { prp-san | hsr-san | hsr-prp | hsr-hsr }
```

Mode

```
RedBox Mode
```

no mode

This command is used to set the mode of this RedBox to its default mode.

Format

```
no mode
```

Mode

```
RedBox Mode
```

55.2. port

55.2.1. port-a interface

This command is used to Assign an interface to port A.

Default

```
none
```

Format

```
port-a interface [ <port_type_id> | neighbor ]
```

Mode

```
RedBox Mode
```

no port-a interface

This command is used to Unassign port A's interface. This cannot be done on an enabled instance.

Format

```
no port-a interface
```

Mode

```
RedBox Mode
```

55.2.2. port-b interface

This command is used to Assign an interface to port B.

Default

```
none
```

Format

```
port-b interface [ <port_type_id> | neighbor ]
```

Mode

```
RedBox Mode
```

no port-a interface

This command is used to Unassign port B's interface.

Format

```
no port-b interface
```

Mode

```
RedBox Mode
```

55.3. net

55.3.1. net-id

This command is used to set net id. The mode needs to be configured as either hsr-prp or hsr-hsr.If a frame arriving on an LRE port has a NetId identical to this one, it gets filtered and not forwarded to the interlink port, but may get forwarded to the other LRE port.

Default

```
1
```

Format

```
net-id <1-7>
```

Mode

```
RedBox Mode
```

no net-id

This command is used to set the NetId to its default.

Format

```
no net-id
```

Mode

```
RedBox Mode
```

55.3.2. lan-id

This command is used to set LanId. Need to configure the mode to hsr-prp.The LanId is used to filter frames from a HSR ring towards the PRP network. It must be 'A' for the RedBox connecting to LAN A and 'B' for the RedBox connecting to LAN B.

Default

```
a
```

Format

```
lan-id { a | b }
```

Mode

```
RedBox Mode
```

no lan-id

This command is used to set the LanId to its default.

Format

```
no lan-id
```

Mode

```
RedBox Mode
```

55.4. nodes table

55.4.1. nodes-table-age-time

This command is used to set the number of seconds without activity before a remote node is removed from the NodesTable (default is 60 seconds).

Default

```
60s
```

Format

```
nodes-table-age-time <1-65>
```

Mode

```
RedBox Mode
```

no nodes-table-age-time

This command is used to set the node table age time to its default.

Format

```
no nodes-table-age-time
```

Mode

```
RedBox Mode
```

55.5. proxy node table

55.5.1. proxy-node-table-age-time

This command is used to set the number of seconds without activity before a proxy node is removed from the ProxyNodeTable (default is 60 seconds).

Default

```
60s
```

Format

```
proxy-nodes-table-age-time <1-65>
```

Mode

```
RedBox Mode
```

no proxy-nodes-table-age-time

This command is used to set the proxy node table age time to its default.

Format

```
no poxy-nodes-table-age-time
```

Mode

```
RedBox Mode
```

55.6. duplicate discard

55.6.1. duplicate-discard-age-time

This command is used to set the number of milliseconds before an entry in the duplicate-discard table times out (default is 40 milliseconds).

Default

```
40ms
```

Format

```
duplicate-discard-age-time <10-10000>
```

Mode

```
RedBox Mode
```

no duplicate-discard-age-time

This command is used to set the duplicate-discard age time to its default.

Format

```
no duplicate-discard-age-time
```

Mode

```
RedBox Mode
```

55.7. supervision

55.7.1. supervision-vlan

This command is used to set the VLAN ID and PCP value of a possible VLAN tag used in supervision frames. If the resulting VLAN is configured as tagged on the interlink port, the supervision frame will be transmitted tagged.

Default

```
native
pcp: 7
```

Format

```
supervision-vlan { native | <vlan_id> } [ pcp <0-7> ]
```

Mode

```
RedBox Mode
```

no supervision-vlan

This command is used to set the VLAN ID and PCP value used in possible VLAN tags in supervision frames to their defaults (native and 7).

Format

```
no supervision-vlan
```

Mode

```
RedBox Mode
```

55.7.2. supervision-dmac-lsb

This command is used to set the least significant byte used in the destination MAC address (01-15-4e-00-01-xx) of generated PRP/HSR supervision frames.

Default

```
0x00
```

Format

```
supervision-dmac-lsb <uint8>
```

Mode

```
RedBox Mode
```

■ no supervision-dmac-lsb

This command is used to set the least significant byte of the destination MAC address used in generated PRP/HSR supervision frames to its default (0x00).

Format

```
no supervision-dmac-lsb
```

Mode

```
RedBox Mode
```

55.7.3. supervision-frame-interval

This command is used to set the number of seconds between transmission of supervision frames (default is 2 seconds).

Default

```
2s
```

Format

```
supervision-frame-interval <1-60>
```

Mode

```
RedBox Mode
```

■ no supervision-frame-interval

This command is used to set the interval between supervision frame transmissions to its default (2 seconds).

Format

```
no supervision-frame-interval
```

Mode

```
RedBox Mode
```

55.7.4. supervision-translate-prp-to-hsr

This command is used to if enabled, the RedBox will software-translate supervision frames received on the PRP network to HSR supervision frames and transmit on the HSR ring, otherwise supervision frames will be hardware-forwarded.

Default

```
enable
```

Format

```
supervision-translate-prp-to-hsr
```

Mode

```
RedBox Mode
```

no supervision-translate-prp-to-hsr

This command is used to set the interval between supervision frame transmissions to its default (2 seconds).

Format

```
no supervision-translate-prp-to-hsr
```

Mode

```
RedBox Mode
```

55.7.5. supervision-translate-hsr-to-prp

If enabled, the RedBox will software-translate supervision frames received on the HSR ring to PRP supervision frames and transmit on the PRP network, otherwise supervision frames will be hardware-forwarded.

Default

```
enable
```

Format

```
supervision-translate-hsr-to-prp
```

Mode

```
RedBox Mode
```

no supervision-translate-hsr-to-prp

This command is used to set the interval between supervision frame transmissions to its default (2 seconds).

Format

```
no supervision-translate-hsr-to-prp
```

Mode

```
RedBox Mode
```

55.8. admin-state

55.8.1. admin-state

This command is used to enable or disable this RedBox instance.

Default

```
disable
```

Format

```
admin-state { enable | disable }
```

Mode

```
RedBox Mode
```

55.9. no

55.9.1. no redbox

This command is used to delete a particular or all RedBox instances.

Format

```
no redbox { <uint> | all }
```

Mode

```
Global Configuration Mode
```

55.10. show

55.10.1. show redbox interfaces

This command is used to show which port interfaces can be selected as Port A and Port B for a given RedBox instance.

Format

```
show redbox interfaces [ sort-by-interface ]
```

Mode

```
User EXEC Mode
```

55.10.2. show redbox

This command is used to show the state or counters of one or more RedBox instances.

Format

```
show redbox [ <range_list> ] { status [ details ] | statistics [ details ] | nodes-table
[ details [ filter ] | supervision [ filter ] ] | proxy-node-table [ details [ filter ] ] }
```

Mode

```
User EXEC Mode
```

55.11. clear

55.11.1. clear redbox

This command is used to clear statistics or table contents of one or more RedBox instances.

Format

```
clear redbox [ <range_llist> ] { proxy-node-table | nodes-table | statistics }
```

Mode

```
User EXEC Mode
```

56. RIP

RIP (Routing Information Protocol) is a distance-vector routing protocol used to exchange routing information in local area networks or wide area networks.

56.1. router

56.1.1. router rip

This command is used to enable RIP router mode. And enter RIP router configuration view.

Default

```
disable
```

Format

```
router rip
```

Mode

```
Global Configuration Mode
```

no router rip

This command is used to disable RIP router mode.

Format

```
no router rip
```

Mode

```
Global Configuration Mode
```

56.2. version

56.2.1. version

This command is used to set routing protocol version.

Default

```
none
```

Format

```
version { 1 | 2 }
```

Mode

```
RIP Router Mode
```

no version

This command is used to restore routing protocol version to default.

Format

```
no version
```

Mode

```
RIP Router Mode
```

56.3. timers

56.3.1. timers basic

This command is used to configure the basic routing protocol timers. First <*5-2147483*> represents the value of update timer in seconds. Second <*5-2147483*> represents the value of invalid timer in seconds. Third <*5-2147483*> represents the value of garbage-collection timer in seconds.

Default

```
30 180 120
```

Format

```
timers basic <5-2147483> <5-2147483> <5-2147483>
```

Mode

```
RIP Router Mode
```

no timers basic

This command is used to restore the basic routing protocol timers to default.

Format

```
no timers basic
```

Mode

```
RIP Router Mode
```

56.4. redistribute

56.4.1. redistribute

This command is used to enable the RIP redistributed protocol type for the static routes, connected interfaces or OSPF routes. Use keywords metric to configure the specified metric for route redistribution, default is auto. <*0-16*> represents user specified metric value.

Default

```
disable
```

Format

```
redistribute { static | connected | ospf } [ metric <0-16> ]
```

Mode

```
RIP Router Mode
```

no redistribute

This command is used to disable the RIP redistributed protocol type for the static routes, connected interfaces or OSPF routes.

Format

```
no redistribute { static | connected | ospf }
```

Mode

```
RIP Router Mode
```

56.5. default-metric

56.5.1. default-metric

This command is used to configure the default metric for the redistributed routes. *<1-16>* represents user specified default metric value.

Default

1

Format

default-metric *<1-16>*

Mode

RIP Router Mode

no default-metric

This command is used to restore the default metric for the redistributed routes to default.

Format

no default-metric

Mode

RIP Router Mode

56.6. default-information

56.6.1. default-information originate

This command is used to enable the RIP default route redistribution.

Default

disable

Format

default-information originate

Mode

RIP Router Mode

no default-information originate

This command is used to disable the RIP default route redistribution.

Format

no default-information originate

Mode

RIP Router Mode

56.7. passive-interface

56.7.1. passive-interface default

This command is used to enable all interfaces as passive-interface by default.

Default

```
disable
```

Format

```
passive-interface default
```

Mode

```
RIP Router Mode
```

■ no passive-interface default

This command is used to disable all interfaces as passive-interface by default.

Format

```
no passive-interface default
```

Mode

```
RIP Router Mode
```

56.8. distance

56.8.1. distance

This command is used to configure the RIP administrative distance. *<1-255>* represents administrative distance value.

Default

```
120
```

Format

```
distance <1-255>
```

Mode

```
RIP Router Mode
```

■ no distance

This command is used to restore the RIP administrative distance to default.

Format

```
no distance
```

Mode

```
RIP Router Mode
```

56.9. network

56.9.1. network

This command is used to configure routing on an IPv4 network. *<ipv4_addr>* represents IPv4 address. *<ipv4_mask>* represents the wildcard-mask of the IPv4 address, where 0 is a match, and 1 is a 'do not care' bit.

Default

none

Format

network *<ipv4_addr>* [*<ipv4_mask>*]

Mode

RIP Router Mode

no network

This command is used to delete routing on an IPv4 network.

Format

no network *<ipv4_addr>* [*<ipv4_mask>*]

Mode

RIP Router Mode

56.10. neighbor

56.10.1. neighbor

This command is used to configure a RIP neighbor router. *<ipv4_addr>* represents neighbor address.

Default

none

Format

neighbor *<ipv4_addr>*

Mode

RIP Router Mode

no neighbor

This command is used to delete a RIP neighbor router.

Format

no neighbor *<ipv4_addr>*

Mode

RIP Router Mode

56.11. passive-interface

56.11.1. passive-interface vlan

This command is used to enable routing updates on an interface. <*vlan_list*> represents list of VLAN ID, e.g. 1,3-5,7.

Default

```
disable
```

Format

```
passive-interface vlan <vlan_list>
```

Mode

```
RIP Router Mode
```

no passive-interface vlan

This command is used to disable routing updates on an interface.

Format

```
no passive-interface vlan <vlan_list>
```

Mode

```
RIP Router Mode
```

56.12. offset-list

56.12.1. offset-list

This command is used to configure the offset-list for RIP metric modification. <*word1-31*> represents the name of access-list. <*0-16*> represents user specified metric value. <*vlan_id*> represents VLAN identifier (VID).

Default

```
none
```

Format

```
offset-list <word1-31> { in | out } <0-16> [ vlan <vlan_id> ]
```

Mode

```
RIP Router Mode
```

no offset-list

This command is used to delete the offset-list for RIP metric modification.

Format

```
no offset-list <word1-31> { in | out } <0-16> [ vlan <vlan_id> ]
```

Mode

```
RIP Router Mode
```

56.13. ip rip

56.13.1. ip rip send version

This command is used to configure the RIP version for the advertisement transmission on the interface.

Default

```
none
```

Format

```
ip rip send version { 1 [ 2 ] | 2 [ 1 ] }
```

Mode

```
VLAN Interface Mode
```

no ip rip send version

This command is used to restore the RIP version for the advertisement transmission on the interface to default.

Format

```
no ip rip send version
```

Mode

```
VLAN Interface Mode
```

56.13.2. ip rip receive version

This command is used to configure the RIP version for the advertisement reception on the interface.

Default

```
none
```

Format

```
ip rip receive version { none | 1 [ 2 ] |2 [ 1 ] }
```

Mode

```
VLAN Interface Mode
```

no ip rip receive version

This command is used to restore the RIP version for the advertisement reception on the interface to default.

Format

```
no ip rip receive version
```

Mode

```
VLAN Interface Mode
```

56.13.3. ip rip split-horizon

This command is used to enable split horizon mode to be split horizon or poisoned reverse.

Default

```
splitHorizon
```

Format

```
ip rip split-horizon [ poisoned-reverse ]
```

Mode

```
VLAN Interface Mode
```

no ip rip split-horizon

This command is used to disable split horizon mode to be split horizon or poisoned reverse.

Format

```
no ip rip split-horizon [ poisoned-reverse ]
```

Mode

```
VLAN Interface Mode
```

56.13.4. ip rip authentication mode

This command is used to configure authentication type.

Default

```
none
```

Format

```
ip rip authentication mode { text | md5 }
```

Mode

```
VLAN Interface Mode
```

no ip rip authentication mode

This command is used to restore authentication type to default.

Format

```
no ip rip authentication mode
```

Mode

```
VLAN Interface Mode
```

56.13.5. ip rip authentication string

This command is used to configure simple password authentication. <*word1-15*> represents the unencrypted (Plain Text) user password. Any printable characters including space is accepted. Notice that you have no chance to get the Plain Text password after this command. The system will always display the encrypted password. <*word1-15*> represents the encrypted (hidden) user password. Notice the encrypt password will be decoded by system internally. You cannot directly use it as same as the Plain Text and it is not human-readable text normally.

Default

```
none
```

Format

```
ip rip authentication string { unencrypted <word1-15> | encrypted <word128> }
```

Mode

```
VLAN Interface Mode
```

no ip rip authentication string

This command is used to restore simple password authentication to default.

Format

```
no ip rip authentication string
```

Mode

```
VLAN Interface Mode
```

56.13.6. ip rip authentication key-chain

This command is used to configure key chain used by MD5 authentication. <*word1-31*> represents the key-chain name.

Default

none

Format

ip rip authentication key-chain <*word1-31*>

Mode

VLAN Interface Mode

■ no ip rip authentication key-chain

This command is used to restore key chain used by MD5 authentication to default.

Format

no ip rip authentication key-chain

Mode

VLAN Interface Mode

56.14. show

56.14.1. show ip rip

This command is used to display RIP configuration. Use database keywords to display RIP database information.

Format

show ip rip [database]

Mode

User EXEC Mode

56.15. clear

56.15.1. clear ip rip process

This command is used to reset the current RIP process.

Format

clear ip rip process

Mode

User EXEC Mode

57. RMON

RMON (Remote Network Monitoring) enables remote monitoring and management of network switches and the network traffic flowing through them.

57.1. rmon

57.1.1. rmon collection stats

This command is used to configure the RMON statistics entry. *<1-65535>* represents statistics entry ID.

Default

```
none
```

Format

```
rmon collection stats <1-65535>
```

Mode

```
Port Configuration Mode
```

■ no rmon collection stats

This command is used to delete the specific RMON statistics entry. *<1-65535>* represents statistics entry ID.

Format

```
no rmon collection stats <1-65535>
```

Mode

```
Port Configuration Mode
```

57.1.2. rmon collection history

This command is used to configure the RMON history entry. *<1-65535>* represents history entry ID. *<buckets>* represents requested buckets of intervals. *<1-3600>* represents interval in seconds to sample data for each bucket.

Default

```
none
```

Format

```
rmon collection history <1-65535> [ buckets <buckets> ] [ interval <1-3600> ]
```

Mode

```
Port Configuration Mode
```

■ no rmon collection history

This command is used to delete the specific RMON history entry. *<1-65535>* represents history entry ID.

Format

```
no rmon collection history <1-65535>
```

Mode

```
Port Configuration Mode
```

57.1.3. rmon alarm

This command is used to configure the RMON alarm entry. *<1-65535>* represents alarm entry ID. *<uint>* represents interface index. *<1-2147483647>* represents sample interval. *<rising-threshold>* represents rising threshold value (-2147483648-2147483647). *<rising-index>* represents rising event index (0-65535), if this value is zero, no associated event will be generated, as zero is not a valid event index. *<falling-threshold>* represents falling threshold value (-2147483648-2147483647). *<falling-index>* represents falling event index (0-65535), if this value is zero, no associated event will be generated, as zero is not a valid event index.

Default

```
none
```

Format

```
rmon alarm <1-65535> { ifInOctets | ifInUcastPkts | ifInNUcastPkts | ifInDiscards
| ifInErrors | ifInUnknownProtos | ifOutOctets | ifOutUcastPkts | ifOutNUcastPkts |
ifOutDiscards | ifOutErrors | ifOutQLen } <uint> <1-2147483647> { absolute | delta}
rising-threshold <rising-threshold> <rising-index> falling-threshold
<falling-threshold> <falling-index> { [ rising | falling | both ] }
```

Mode

```
Global Configuration Mode
```

no rmon alarm

This command is used to delete the specific RMON alarm entry. *<1-65535>* represents alarm entry ID.

Format

```
no rmon alarm <1-65535>
```

Mode

```
Global Configuration Mode
```

57.1.4. rmon event

This command is used to configure the RMON event entry. *<1-65535>* represents event entry ID. *<word127>* represents requested SNMP community string. *<line127>* represents event description.

Default

```
none
```

Format

```
rmon event <1-65535> [ log ] [ trap [ <word127> ] ] { [ description <line127> ] }
```

Mode

```
Global Configuration Mode
```

no rmon event

This command is used to delete the specific RMON event entry. *<1-65535>* represents event entry ID.

Format

```
no rmon event <1-65535>
```

Mode

```
Global Configuration Mode
```

57.2. show

57.2.1. show rmon statistics

This command is used to display the RMON statistics table. *<1-65535>* represents statistics entry ID.

Format

```
show rmon statistics [ <1~65535> ]
```

Mode

```
User EXEC Mode
```

57.2.2. show rmon history

This command is used to display the RMON history table. *<1-65535>* represents history entry ID.

Format

```
show rmon history [ <1-65535> ]
```

Mode

```
User EXEC Mode
```

57.2.3. show rmon alarm

This command is used to display the RMON alarm table. *<1-65535>* represents alarm entry ID.

Format

```
show rmon alarm [ <1-65535> ]
```

Mode

```
User EXEC Mode
```

57.2.4. show rmon event

This command is used to display the RMON event table. *<1-65535>* represents event entry ID.

Format

```
show rmon event [ <1-65535> ]
```

Mode

```
User EXEC Mode
```

58. Router

Switches are typically data link layer devices, mainly used for the exchange and forwarding of data packets within local area networks. Therefore, switches usually do not have routing capabilities. However, in some cases, advanced switches like layer 3 switches may have certain routing capabilities, allowing them to forward data packets between different subnets.

58.1. Key-Chain

58.1.1. key chain

This command is used to configure router Key-Chain. And enter router Keychain view. <*word31*> and <*word1-31*> represents Key-Chain name.

Default

```
none
```

Format

```
key chain <word31>
```

Mode

```
Global Configuration Mode
```

■ no key chain

This command is used to delete router Key-Chain.

Format

```
no key chain <word1-31>
```

Mode

```
Global Configuration Mode
```

58.1.2. key key-string

This command is used to configure router Key-Chain Key IDs. <*1-255*> represents Key-Chain Key ID. <*word1-63*> represents the unencrypted (Plain Text) user password. <*word128-224*> represents the encrypted (hidden) user password.

Default

```
none
```

Format

```
key <1-255> key-string { unencrypted <word1-63> | encrypted <word128-224> }
```

Mode

```
Keychain Mode
```

■ no key key-string

This command is used to delete router Key-Chain Key IDs.

Format

```
no key <1-255> key-string
```

Mode

```
Keychain Mode
```

58.1.3. router access-list

This command is used to configure router access list. <*word1-31*> represents the name of the access list. <*ipv4_addr*> represents the IPv4 address for the access list entry. <*ipv4_netmask*> represents the IPv4 network mask for the access list entry.

Default

none

Format

router access-list <*word1-31*> { permit | deny } { any | <*ipv4_addr*> <*ipv4_netmask*> }

Mode

Global Configuration Mode

no router access-list

This command is used to delete router access list.

Format

no router access-list <*word1-31*>

Mode

Global Configuration Mode

58.1.4. router prefix-list

This command is used to configure router prefix list. <*word1-31*> represents the name of the prefix list. <*ipv4_addr*> represents the IPv4 address for the prefix list entry. <*ipv4_netmask*> represents the IPv4 network mask for the prefix list entry.

Default

none

Format

router prefix-list <*word1-31*> { permit | deny } { any | <*ipv4_addr*> <*ipv4_netmask*> }

Mode

Global Configuration Mode

no router prefix-list

This command is used to delete router prefix list.

Format

no router prefix-list <*word1-31*>

Mode

Global Configuration Mode

58.2. Nat

58.2.1. nat static outbound

This command configures static NAT mappings to establish fixed one-to-one bindings between Private IP addresses and Public IP addresses.

Default

none

Format

nat static outbound *<ipv4_addr> <ipv4_addr>*

Mode

Global Configuration Mode

no nat static outbound

This command removes static NAT mapping entries. Use <ipv4_addr> to delete a single specified entry, or all to delete all current entries.

Format

no nat static outbound { *<ipv4_addr>* | all }

Mode

Global Configuration Mode

58.3. show

58.3.1. Show nat

This command displays static NAT entries (all entries or entries mapped to specific private IPs).

Format

show nat { static-table | *<ipv4_addr>* }

Mode

User EXEC Mode

59. Selftest

The Selftest feature is used to conduct self-checks to ensure the normal operation of the device. This includes hardware self-test (Checking if the hardware components of the switch, including interfaces, ports, power supply, and fans, are functioning properly. It also involves monitoring temperature and voltage levels to ensure they are within the normal range), memory self-test (Verifying the storage and access of memory in the switch and detecting any memory faults), hardware diagnostics (Identifying hardware faults through self-tests to facilitate quick troubleshooting and issue resolution).

59.1. selftest

59.1.1. selftest action

This command is used to configure the action that a selftest component should take. "ramtest" represents configure the action for ramtest errors. "cpu" represents configure the action for CPU errors. "memory " represents configure the action for memory errors. "flash" represents configure the action for flash errors. "log-only" represents write a message to the logging file. "send-trap" represents send a trap to the management station.

Default

```
log-only
```

Format

```
selftest action { ramtest } { log-only | send-trap }
```

Mode

```
Global Configuration Mode
```

59.1.2. selftest ramtest enable

This command is used to enable the RAM selftest on cold start of the device. When disabled the device booting time is reduced.

Default

```
disable
```

Format

```
selftest ramtest enable
```

Mode

```
Global Configuration Mode
```

59.1.3. selftest ramtest disable

This command is used to disable the RAM selftest on cold start of the device. When disabled the device booting time is reduced.

Format

```
selftest ramtest disable
```

Mode

```
Global Configuration Mode
```

59.1.4. selftest cpu

This command is used to configure the CPU self-test feature of the device. The optional parameters respectively represent disable the CPU self-test feature of the device. Enable the CPU self-test feature of the device. Configure the CPU self-test interval, the unit is in seconds. Configure the rising threshold for the CPU self-test, the unit is in percentage.

Default

```
disable
```

Format

```
selftest cpu { { disable | enable } | { [ interval <1-60> ] [ threshold <1-100> ] } }
```

Mode

```
Global Configuration Mode
```

no selftest cpu

This command is used to configure the CPU self-test feature to default settings.

Format

```
no selftest cpu { [ interval ] [ threshold ] }
```

Mode

```
Global Configuration Mode
```

59.1.5. selftest memory

This command is used to configure the memory self-test feature of the device.

Default

```
disable
```

Format

```
selftest memory { { disable | enable } | { [ interval <1-60> ] [ threshold <1-100> ] }
```

Mode

```
Global Configuration Mode
```

no selftest memory

This command is used to configure the memory self-test feature to default settings.

Format

```
no selftest memory { [ interval ] [ threshold ] }
```

Mode

```
Global Configuration Mode
```

59.1.6. selftest flash

This command is used to configure the flash self-test feature of the device.

Default

```
disable
```

Format

```
selftest flash { { disable | enable } | { [ interval <1-60> ] [ threshold <1-4096> ] } }
```

Mode

```
Global Configuration Mode
```

no selftest flash

This command is used to configure the flash self-test feature to default settings.

Format

```
no selftest flash { [ interval ] [ threshold ] }
```

Mode

```
Global Configuration Mode
```

59.2. show

59.2.1. show selftest action

This command is used to display the actions the device takes if an error occurs.

Format

```
show selftest action
```

Mode

```
User EXEC Mode
```

59.2.2. show selftest settings

This command is used to display the selftest settings.

Format

```
show selftest settings
```

Mode

```
User EXEC Mode
```

60. sFlow

sFlow (Sampled Flow) is a network traffic monitoring technique based on packets sampling, and it's mainly used for statistical analysis of network traffic.

There are two sampling mechanisms for sFlow:

1) Packets-based Sampling: Obtain relevant information of data stream via packets sampling of the device port.

2) Time-based Port Statistics Sampling: Periodically query the enabled sFlow property port, and obtain statistics information of each port.

sFlow system contains a sFlow Agent embedded in the device and a remote sFlow Collector. The sFlow Agent is used for obtaining port statistics information and port data stream information. It will assemble these information groups into sFlow packets. And send them to sFlow Collector to analyze sFlow packets and display the analyzing results.

As a network traffic monitoring technology, sFlow has the following advantages:

1) Support accurate network traffic monitoring on Gigabit or higher speed network.

2) It has good scalability. And a sFlow Collector can monitor multiple sFlow Agent.

3) Realize sFlow Agent at a very low cost.

60.1. sflow

60.1.1. sflow

This command is used to enable flow sampler in port configuration mode.

Default

```
disable
```

Format

```
sflow
```

Mode

```
Port Configuration Mode
```

no sflow

This command is used to disable flow sampler in port configuration mode.

Format

```
no sflow
```

Mode

```
Port Configuration Mode
```

60.1.2. sflow agent-ip

This command is used to configure the agent IP address used as agent-address in UDP datagrams. <*ipv4_addr*> represents IPv4 address. <*ipv6_addr*> represents IPv6 address.

Default

```
127.0.0.1
```

Format

```
sflow agent-ip { ipv4 <ipv4_addr> | ipv6 <ipv6_addr> }
```

Mode

```
Global Configuration Mode
```

no sflow agent-ip

This command is used to set the agent IP address used as agent-address in UDP datagrams to 127.0.0.1.

Format

```
no sflow agent-ip
```

Mode

```
Global Configuration Mode
```

60.1.3. sflow collector-address

This command is used to configure the receiver address in the configuration mode. <*ipv4_addr*> represents IPv4 address identifying the collector receiver. <*ipv6_ucast*> represents IPv6 address identifying the collector receiver. <*domain_name*> represents domain name identifying the collector receiver.

Default

```
0.0.0.0
```

Format

```
sflow collector-address { <ipv4_addr> | <ipv6_ucast> | <domain_name> }
```

Mode

```
Global Configuration Mode
```

no sflow collector-address

This command is used to set the receiver address in the configuration mode to 0.0.0.0.

Format

```
no sflow collector-address
```

Mode

```
Global Configuration Mode
```

60.1.4. sflow collector-port

This command is used to configure the receiver UDP port in the configuration mode. <*1-65535*> represents the UDP port number.

Default

```
6343
```

Format

```
sflow collector-port <1-65535>
```

Mode

```
Global Configuration Mode
```

no sflow collector-port

This command is used to restore the receiver UDP port in the configuration mode to default.

Format

```
no sflow collector-port
```

Mode

```
Global Configuration Mode
```

60.1.5. sflow timeout

This command is used to configure the timeout in the configuration mode. *<0-2147483647>* represents number of seconds.

Default

```
0
```

Format

```
sflow timeout <0-2147483647>
```

Mode

```
Global Configuration Mode
```

■ no sflow timeout

This command is used to restore the timeout in the configuration mode to default.

Format

```
no sflow timeout
```

Mode

```
Global Configuration Mode
```

60.1.6. sflow max-datagram-size

This command is used to configure the maximum packet size in the configuration mode. *<200-1468>* represents bytes.

Default

```
1400
```

Format

```
sflow max-datagram-size <200-1468>
```

Mode

```
Global Configuration Mode
```

■ no sflow max-datagram-size

This command is used to restore the maximum packet size in the configuration mode to default.

Format

```
no sflow max-datagram-size
```

Mode

```
Global Configuration Mode
```

60.1.7. sflow sampling-rate

This command is used to configure the traffic sampling rate in port configuration mode, valid range depends on the chip capability. *<1-16777215>* represents sampling rate.

Default

```
0
```

Format

```
sflow sampling-rate <1-16777215>
```

Mode

```
Port Configuration Mode
```

no sflow sampling-rate

This command is used to restore the traffic sampling rate in port configuration mode to default.

Format

```
no sflow sampling-rate
```

Mode

```
Port Configuration Mode
```

60.1.8. sflow max-sampling-size

This command is used to configure the maximum flow sampling size in port configuration mode. *<14-200>* represents bytes.

Default

```
128
```

Format

```
sflow max-sampling-size <14-200>
```

Mode

```
Port Configuration Mode
```

no sflow max-sampling-size

This command is used to restore the maximum flow sampling size in port configuration mode to default.

Format

```
no sflow max-sampling-size
```

Mode

```
Port Configuration Mode
```

60.1.9. sflow counter-poll-interval

This command is used to enable counter poll in port configuration mode and set the interval. *<1-3600>* represents seconds.

Default

```
disable
```

Format

```
sflow counter-poll-interval <1-3600>
```

Mode

```
Port Configuration Mode
```

no sflow counter-poll-interval

This command is used to disable counter poll in port configuration mode.

Format

```
no sflow counter-poll-interval
```

Mode

```
Port Configuration Mode
```

60.1.10. sflow export-rate-limit

This command is used to configure sflow sampling packet rate to control-plane.

Default

300

Format

sflow export-rate-limit *<100-1500>*

Mode

Global Configuration Mode

60.2. show

60.2.1. show sflow

This command is used to display the current sFlow configuration.

Format

show sflow

Mode

User EXEC Mode

60.2.2. show sflow statistics

This command is used to show sflow statistics for either receiver or sample interface. <*port_type_list*> represents port interfaces.

Format

show sflow statistics { receiver | samplers [interface *<port_type_list>*] }

Mode

User EXEC Mode

60.3. clear

60.3.1. clear sflow statistics

This command is used to clear statistics for receiver or specific interfaces. <*port_type_list*> represents port interfaces.

Format

clear sflow statistics { receiver | samplers [interface *<port_type_list>*] }

Mode

User EXEC Mode

61. SNMP

SNMP (Simple Network Management Protocol) is an application layer protocol that is designed for the management and monitoring of network devices such as switches, routers, firewalls, etc. SNMP enables administrators to remotely collect and configure information on network devices, thereby allowing for more effective management of network performance, the discovery and resolution of problems, as well as planning for network growth.

61.1. snmp-server

61.1.1. snmp-server contact

This command is used to specify the system contact string.

Default

```
none
```

Format

```
snmp-server contact <line255>
```

Mode

```
Global Configuration Mode
```

■ no snmp-server contact

This command is used to unspecify the system contact string.

Format

```
no snmp-server contact
```

Mode

```
Global Configuration Mode
```

61.1.2. snmp-server location

This command is used to specify the system location string.

Default

```
none
```

Format

```
snmp-server location <line255>
```

Mode

```
Global Configuration Mode
```

■ no snmp-server location

This command is used to unspecify the system location string.

Format

```
no snmp-server location
```

Mode

```
Global Configuration Mode
```

61.1.3. snmp-server

This command is used to enable SNMP server.The command can enable SNMP server on SNMPv1, SNMPv2c, or SNMPv3.

Default

none

Format

snmp-server

Mode

Global Configuration Mode

no snmp-server

This command is used to disable SNMP server.The command can disable SNMP server on SNMPv1, SNMPv2c, or SNMPv3.

Format

no snmp-server

Mode

Global Configuration Mode

61.1.4. snmp-server engine-id local

This command is used to specify SNMP server's engine ID.

Default

none

Format

snmp-server engine-id local *<word10-64>*

Mode

Global Configuration Mode

no snmp-server engine-id local

This command is used to set SNMP server's engine ID to default value.

Format

no snmp-server engine-id local

Mode

Global Configuration Mode

61.1.5. snmp-server host

This command is used to set server's name of the host configurations.

Default

none

Format

snmp-server host *<word32>*

Mode

Global Configuration Mode

■ no snmp-server host

This command is used to unset server's name of the host configurations.

Format

```
no snmp-server host
```

Mode

```
Global Configuration Mode
```

61.1.6. snmp-server trap

This command is used to set the trap source configuration. <*cword*> represents trap source table/event name. "id <*0-127*>" use specific filter ID. <*word255*> represents OID to use as index filter. Include represents Include filter type. Exclude represents Exclude filter type.

Default

```
none
```

Format

```
snmp-server trap <cword> [ id <0-127> ] [ <word255> { include | exclude } ]
```

Mode

```
Global Configuration Mode
```

■ no snmp-server trap

This command is used to unset the trap source configuration.

Format

```
no snmp-server trap <cword> { [ id <0-127> ] | [ <word255> { include | exclude } ] }
```

Mode

```
Global Configuration Mode
```

61.1.7. snmp-server community

This command is used to set the SNMP community information. <*word32*> represents security name. "ip-range <*ipv4_addr*> <*ipv4_netmask*>" represent range, IPv4 address, and netmask. "ipv6-range <*ipv6_subnet*>" represent use IPv6 range, and IPv6 subnet. <*word32*> represents community secret. "encrypted <*word96-160*>" represent use encrypted community secret.

Default

```
none
```

Format

```
snmp-server community <word32> [ { ip-range <ipv4_addr> <ipv4_netmask> | ipv6-range
<ipv6_subnet> } ] { <word32> | encrypted <word96-160> }
```

Mode

```
Global Configuration Mode
```

■ no snmp-server community

This command is used to unset the SNMP community information.

Format

```
no snmp-server community <word32> [ { ip-range <ipv4_addr> <ipv4_netmask> | ipv6-range
<ipv6_subnet> } ]
```

Mode

```
Global Configuration Mode
```

61.1.8. snmp-server user

This command is used to set the SNMPv3 user's configurations. <*word32*> represents username. "engine-id <*word10-64*>" represents engine ID octet string. "md5 <*word8-32*>" represents MD5 unencrypted password. "encrypted <*word16-64*>" represents MD5 encrypted password. "sha <*word8-40*>" represents SHA unencrypted password. "encrypted <*word16-80*>" represents specifies an encrypted password will follow. "priv" represents set privacy, include DES and AES protocol. <*word8-32*> represents privacy unencrypted password. "encrypted <*word16-64*>" represents specifies an encrypted password will follow.

Default

```
none
```

Format

```
snmp-server user <word32> engine-id <word10-64> [ { md5 { <word8-32> | { encrypted <word16-64> } } | sha { <word8-40> | { encrypted <word16-80> } } } [ priv { des | aes } { <word8-32> | { encrypted <word16-64> } } ] ]
```

Mode

```
Global Configuration Mode
```

no snmp-server user

This command is used to unset the SNMPv3 user's configurations.

Format

```
no snmp-server user <word32> engine-id <word10-64>
```

Mode

```
Global Configuration Mode
```

61.1.9. snmp-server security-to-group model

This command is used to configure the model, security user, and group name of the snmp-server.

Default

```
none
```

Format

```
snmp-server security-to-group model { v1 | v2c | v3 } name <word32> group <word32>
```

Mode

```
Global Configuration Mode
```

no snmp-server security-to-group model

This command is used to unset security user of the snmp-server.

Format

```
no snmp-server security-to-group model { v1 | v2c | v3 } name <word32>
```

Mode

```
Global Configuration Mode
```

61.1.10. snmp-server view

This command is used to configure the view of the snmp-server.

Default

```
none
```

Format

```
snmp-server view <word32> <word255> { include | exclude }
```

Mode

```
Global Configuration Mode
```

■ no snmp-server view

This command is used to unset the view of the snmp-server.

Format

```
no snmp-server view <word32> <word255>
```

Mode

```
Global Configuration Mode
```

61.1.11. snmp-server access

This command is used to configure the access rights of the SNMP server (group name), mode (v1, v2c, v3, any), security level ((NOAuth, NoPriv), (Auth, NoPriv), (Auth, Priv)), read (view name), and write (view name).

Default

```
none
```

Format

```
snmp-server access <word32> model { v1 | v2c | v3 | any } level { auth | noauth | priv } [ read <word32> ] [ write <word32> ]
```

Mode

```
Global Configuration Mode
```

■ no snmp-server access

This command is used to unconfigure the access permissions and other settings of the snmp-server.

Format

```
no snmp-server access <word32> model { v1 | v2c | v3 | any } level { auth | noauth | priv }
```

Mode

```
Global Configuration Mode
```

61.2. shutdown

61.2.1. shutdown

This command is used to disable the trap configuration.

Default

```
none
```

Format

```
shutdown
```

Mode

```
SNMP Server Host Mode
```

■ no shutdown

This command is used to enable the trap configuration.

Format

```
no shutdown
```

Mode

```
SNMP Server Host Mode
```

61.3. host

61.3.1. host

This command is used to configure the IP addresses for interfaces, including the loopback interface.

Default

none

Format

host { *<ipv4_ucast>* | *<domain_name>* } [*<1-65535>*] [traps | informs]

Mode

SNMP Server Host Mode

■ no host

This command removes the IP address configuration from an interface, including the loopback interface.

Format

no host

Mode

SNMP Server Host Mode

61.4. version

61.4.1. version

This command is used to configure the SNMP trap version.

Default

none

Format

version { v1 [{ *<word63>* | encrypted *<word96-224>* }] | v2 [{ *<word63>* | encrypted *<word96-224>* }] | v3 engineID *<word10-64>* [*<word32>*] }

Mode

SNMP Server Host Mode

Example

```
Switch(config)# snmp-server host ff
Switch(config-snmps-host)# version v3 engineID 800087bf033029be550513 ddd
```

■ no version

This command is used to negate the SNMP trap version.

Format

no version

Mode

SNMP Server Host Mode

61.5. informs

61.5.1. informs retries

This command is used to set retires inform messages and timeout period. *<0-255>* indicates the retry count, and *<0-2147>* indicates the timeout period.

Default

none

Format

informs retries *<0-255>* timeout *<0-2147>*

Mode

SNMP Server Host Mode

no informs

This command is used to cancel inform messages to this host.

Format

no informs

Mode

SNMP Server Host Mode

61.6. show

61.6.1. show snmp

This command is used to display SNMP configurations.

Format

show snmp

Mode

User EXEC Mode

61.6.2. show snmp view

This command is used to show the view of the snmp-server information.

Format

show snmp view [*<word32>* [*<word255>*]]

Mode

User EXEC Mode

62. Software

This module primarily facilitates the reboot of the switch device and manages the configuration files as well as other files.

62.1. reload

1.1.4.reload cold

This command is used to reload cold.

Format

```
reload cold
```

Mode

```
User EXEC Mode
```

62.1.1. reload defaults

This command is used to reload defaults without rebooting.

Format

```
reload defaults
```

Mode

```
User EXEC Mode
```

62.2. configuration

62.2.1. copy running-config startup-config

This command is used to copy running-config to startup-config, thereby ensuring that the currently active configuration will be used at the next reboot.

Format

```
copy running-config startup-config
```

Mode

```
User EXEC Mode
```

62.2.2. copy (download)

This command is used to download startup-config, running-config or default-config on the switch to the remote. <*url_file*> represents download file URL to remote directory.

Format

```
copy { startup-config | running-config | default-config } <url_file>
```

Mode

```
User EXEC Mode
```

62.2.3. copy (upload)

This command is used to upload a file from the remote to all the files on the switch, except default-config which is read-only. *<url_file>* represents download file URL to remote directory. *<file>* represents the file on the switch, starting with *flash* .

Format

```
copy <url_file> { startup-config | running-config | <file> }
```

Mode

```
User EXEC Mode
```

62.2.4. copy running-config

This command is used to activate any of the configuration files present on the switch, except for running-config which represents the currently active configuration.

Format

```
copy { startup-config | default-config } running-config
```

Mode

```
User EXEC Mode
```

62.3. file

62.3.1. copy (download)

This command is used to download any of the files on the switch to the remote. *<file>* represents the file on the switch, starting with *flash:* . *<url_file>* represents download file URL to remote directory.

Format

```
copy <file> <url_file>
```

Mode

```
User EXEC Mode
```

62.3.2. copy (upload)

This command is used to upload a file from the remote to any of the files on the switch. *<url_file>* represents upload file URL from remote directory. *<file>* represents the file on the switch, starting with *flash:* .

Format

```
copy <url_file> <file>
```

Mode

```
User EXEC Mode
```

62.4. delete

62.4.1. delete

This command is used to delete any of the writable files stored in flash on the switch. *<file>* represents the file on the switch, starting with *flash:* .

Format

```
delete <file>
```

Mode

```
User EXEC Mode
```

62.4.2. delete startup-config

This command is used to delete any of the writable files stored in flash, including startup-config. If this is done and the switch is rebooted without a prior Save operation, this effectively resets the switch to default configuration.

Format

```
delete startup-config
```

Mode

```
User EXEC Mode
```

63. SSH

SSH (Secure Shell) is primarily used to provide a secure method for network administrative access. It allows network administrators to configure and manage switches through encrypted remote sessions. Compared to the earlier protocol Telnet, SSH offers enhanced security as it prevents the transmission of passwords and other sensitive information in plain text across the network.

63.1. ip

63.1.1. ip ssh

This command is used to enable the SSH mode.

Default

```
disable
```

Format

```
ip ssh
```

Mode

```
Global Configuration Mode
```

■ no ip ssh

This command is used to disable the SSH mode.

Format

```
no ip ssh
```

Mode

```
Global Configuration Mode
```

63.1.2. ip telnet

This command is used to enable the telnet mode.

Default

```
enable
```

Format

```
ip telnet
```

Mode

```
Global Configuration Mode
```

■ no ip telnet

This command is used to disable the telnet mode.

Format

```
no ip telnet
```

Mode

```
Global Configuration Mode
```

63.1.3. ssh user (ipv4)

This command is used to initiate an SSH session to a specified IPv4 address or domain name with a specified username. A non-default TCP port can also be specified.

Default

```
TCP port: 22
```

Format

```
ssh { <ipv4_addr> | <domain_name> } user <word64> [ port { <1025-65535> | 22 } ]
```

Mode

```
User EXEC Mode
```

63.1.4. ssh user (ipv6)

This command is used to initiate an SSH session to a specified IPv6 address with a specified username. A non-default TCP port can also be specified.

Default

```
TCP port: 22
```

Format

```
ssh <ipv6_addr> user <word64> [ port { <1025-65535> | 22 } ]
```

Mode

```
User EXEC Mode
```

63.2. show

63.2.1. show ip ssh

This command is used to display SSH status.

Format

```
show ip ssh
```

Mode

```
User EXEC Mode
```

64. Statusmanager

Status Manager Status configuration management is mainly related to the management of device status and security status. It offers inspection items related to device status, device security, relay, and resources. By detecting these inspection items, we can understand the status of the devices, security, relays, and resources.

64.1. device-status

64.1.1. device-status monitor

This command is used to configure the monitoring of a specific inspection item for device status.

Format

```
device-status monitor { link-failure | ring-redundancy | temperature }
```

Mode

```
Global Configuration Mode
```

■ no device-status monitor

This command is used to cancel device status monitoring.

Format

```
no device-status monitor { link-failure | ring-redundancy | temperature }
```

Mode

```
Global Configuration Mode
```

64.1.2. device-status link-alarm

This command is used to configure the monitoring of the link status of a port. You need to enter a specific port.

Format

```
device-status link-alarm
```

Mode

```
Port Configuration Mode
```

■ no device-status monitor

This command is used to cancel device monitoring.

Format

```
no device-status link-alarm
```

Mode

```
Port Configuration Mode
```

64.2. security-status

64.2.1. security-status monitor

This command is used to configure the monitoring status of a specific item for device security. Use the "no" command to disable monitoring of a specific item for device security.

Format

```
security-status monitor { https-certificate | pwd-change | pwd-min-length |
pwd-policy-config | snmp-unsecure }
```

Mode

```
Global Configuration Mode
```

■ no device-status monitor

This command is used to cancel device monitoring.

Format

```
no security-status monitor { https-certificate | pwd-change | pwd-min-length |
pwd-policy-config | snmp-unsecure }
```

Mode

```
Global Configuration Mode
```

64.3. relay-status

64.3.1. relay-status monitor power-supply

This command is used to configure the monitoring of the power supply status of the device.

Format

```
relay-status monitor power-supply <1-2>
```

Mode

```
Global Configuration Mode
```

■ no relay-status monitor power-supply

This command configures the system to not monitor device power status.

Format

```
no relay-status monitor power-supply <1-2>
```

Mode

```
Global Configuration Mode
```

64.3.2. relay-status monitor relay

This command is used to configure the monitoring of the relay status of the device.

Format

```
relay-status monitor relay
```

Mode

```
Global Configuration Mode
```

■ no relay-status monitor relay

This command is used to set the relay to unmonitored status.

Format

```
no relay-status monitor relay
```

Mode

```
Global Configuration Mode
```

64.4. resource-status

64.4.1. resource-status monitor

This command is used to configure the monitoring of a specific inspection item for device resource status.

Format

```
resource-status monitor { CPU | Memory | Flash }
```

Mode

```
Global Configuration Mode
```

■ no relay-status monitor relay

This command is used to cancel resource monitoring.

Format

```
no resource-status monitor { CPU | Memory | Flash }
```

Mode

```
Global Configuration Mode
```

64.5. show

64.5.1. show device-status monitor

This command is used to show Device Status Monitor Check the monitoring status of each device status inspection item.

Format

```
show device-status monitor
```

Mode

```
User Mode
```

64.5.2. show device-status events

This command is used to show Device Status Events Check the reported device status alarm information on the current device.

Format

```
show device-status events
```

Mode

```
User Mode
```

64.5.3. show device-status link-alarm

This command is used to show Device Status Link-Alarm Check the monitoring status of the link status of all ports.

Format

```
show device-status events
```

Mode

```
User Mode
```

64.5.4. show security-status events

This command is used to show Security Status Events Check the reported device security status alarm information on the current device.

Format

```
show device-status events
```

Mode

```
User Mode
```

64.5.5. show relay-status monitor

This command is used to show Relay Status Monitor Check the monitoring status of each device relay status inspection item (whether it is being monitored).

Format

```
show relay-status monitor
```

Mode

```
User Mode
```

64.5.6. show relay-status events

This command is used to show Relay Status Events Check the reported relay status alarm information on the current device.

Format

```
show relay-status  events
```

Mode

```
User Mode
```

64.5.7. show resource-status monitor

This command is used to show Resource Status Monitor Check the monitoring status of each device resource status inspection item (whether it is being monitored).

Format

```
show resource-status monitor
```

Mode

```
User Mode
```

64.5.8. show resource-status events

This command is used to show Resource Status Events Check the reported resource status alarm information on the current device.

Format

```
show resource-status events
```

Mode

```
User Mode
```

65. Syslog

This module is primarily used for setting up system logging-related functions, including enabling logging, configuring the log host address, log message severity level, SNMP trap settings, and more.

65.1. logging

65.1.1. logging on

This command is used to enable the logging server.

Default

none

Format

logging on

Mode

Global Configuration Mode

■ no logging on

This command disables the logging server.

Format

no logging on

Mode

Global Configuration Mode

65.1.2. logging host

This command is used to modify or add log server information for a specified serial number. If the entry does not exist, an IP address or domain name must be configured when adding it.

Default

none

Format

logging host *<1-20>* [addr { *<ipv4_var>* | *<name_var>* }] [level { informational | notice | warning | error }] [mode { enable | disable }]

Mode

Global Configuration Mode

■ no logging host

This command deletes syslog server information by index.

Format

no logging host *<1-20>*

Mode

Global Configuration Mode

65.1.3. logging notification listen

This command is used to enable logging of state changes for specified variable.

Default

none

Format

logging notification listen *<name>* level { informational | notice | warning | error } *<node>*

Mode

Global Configuration Mode

no logging notification listen

This command disables logging of state changes for specified variable.

Format

no logging notification listen [*<kword127>*]

Mode

Global Configuration Mode

65.1.4. logging snmp-request get

This command is used to enable logging snmp-request get. Record the get operations of the mib tool in syslog.

Default

disable

Format

logging snmp-request get

Mode

Global Configuration Mode

no logging snmp-request get

This command is used to disable the logging snmp-request get.

Format

no logging snmp-request get

Mode

Global Configuration Mode

65.1.5. logging snmp-request get severity

This command is used to record the level of logs recorded by mib tool get operations in syslog.

Default

informational

Format

logging snmp-request get severity { informational | notice | warning | error }

Mode

Global Configuration Mode

■ no logging snmp-request severity

This command is used to disable logging snmp-request get severity.

Format

```
no logging snmp-request severity
```

Mode

```
Global Configuration Mode
```

65.1.6. logging snmp-request set

This command is used to enable logging snmp-request set.Record the set operations of the mib tool in syslog.

Default

```
disable
```

Format

```
logging snmp-request set
```

Mode

```
Global Configuration Mode
```

■ no logging snmp-request set

This command is used to disable logging snmp-request set.

Format

```
no logging snmp-request set
```

Mode

```
Global Configuration Mode
```

65.1.7. logging snmp-request set severity

This command is used to record the level of logs recorded by mib tool set operations in syslog.

Default

```
informational
```

Format

```
logging snmp-request set severity { informational | notice | warning | error }
```

Mode

```
Global Configuration Mode
```

■ no logging snmp-request severity set

This command is used to disable logging snmp-request set.

Format

```
no logging snmp-request set
```

Mode

```
Global Configuration Mode
```

65.2. show

65.2.1. show logging

This command use the show logging privileged EXEC command without keywords to display the logging configuration, or particularly the logging message summary for the logging level.

Format

```
show logging [ informational ] [ notice ] [ warning ] [ error ]
```

Mode

```
User EXEC Mode
```

65.2.2. show logging

This command is use the show logging privileged EXEC command with logging ID to display the detail logging message.

Format

```
show logging <1-4294967295>
```

Mode

```
User EXEC Mode
```

65.2.3. show logging history

This command is use to display all command history logging on Flash.

Format

```
show logging history
```

Mode

```
User EXEC Mode
```

65.2.4. show logging host

This command is use to view global logging function status (Enabled/Disabled) and configured server list.

Format

```
show logging host
```

Mode

```
User EXEC Mode
```

65.3. clear

65.3.1. clear logging

This command is use the clear logging privileged EXEC command to clear the logging message.

Format

```
clear logging [ informational ] [ notice ] [ warning ] [ error ]
```

Mode

```
User EXEC Mode
```

66. Sysutil

This module is used to set the system name for devices, display switch version information, LED status information, as well as the system's CPU status, etc.

66.1. hostname

66.1.1. hostname

This command is used to set system's network name.

Default

```
none
```

Format

```
hostname <host_name>
```

Mode

```
Global Configuration Mode
```

Example

```
(config)# hostname my-device
my-device(config)#
```

no hostname

This command is used to delete system's network name.

Format

```
no hostname
```

Mode

```
Global Configuration Mode
```

66.2. show

66.2.1. show version

This command is used to display system hardware and software status.

Format

```
show version [ brief ]
```

Mode

```
User EXEC Mode
```

66.2.2. show system led status

This command is used to show led status. <*switch_list*> represents List of switch ID, ex, 1,3-5,6.

Format

```
show system led status [ switch <switch_list> ]
```

Mode

```
User EXEC Mode
```

66.2.3. show system cpu status

This command is used to show system cpu status.

Format

```
show system cpu status
```

Mode

```
User EXEC Mode
```

66.2.4. show memory

This command is used to display memory information.

Format

```
show memory
```

Mode

```
User EXEC Mode
```

66.3. clear

66.3.1. clear system led status

This command is used to clear led status. <*switch_list*> represents List of switch ID, ex, 1,3-5,6. "fatal" represents clear fatal error status of the system LED. "software" represents clear generic software error status of the system LED. "ztp" represents clear ZTP (Zero Touch Provisioning) error status of the system LED. "stack-firmware" represents clear stack firmware version check error status of the system LED. "all" represents clear all error status of the system LED and back to normal indication.

Format

```
clear system led status [ switch <switch_list> ] { fatal | software | ztp |
stack-firmware | all }
```

Mode

```
User EXEC Mode
```

67. SyncE

SyncE (Synchronous Ethernet) is a technology used in Ethernet links and networks for the transmission of synchronization information. SyncE allows the transmission of clock signals through the physical layer, rather than just data packets, thus providing a synchronization source for network devices. This is very important for maintaining communication quality, reducing data packet loss, and minimizing jitter in delay.

67.1. network-clock

67.1.1. network-clock clk-source (nominate)

This command is used to nominate a clock input to become a selectable clock source. *<range_list>* represents clock source number, The range of values is from 1 to 2. "clk-in" represents nominate the station clock input as a source. The PCB104 SyncE module supports 10 MHz station clock input. "ptp *<0-3>*" represents nominate an ethernet interface as a source. "interface *<port_type_id>*" represents interface, and port list.

Default

```
none
```

Format

```
network-clock clk-source <range_list> nominate { clk-in | { ptp <0-3> } | { interface <port_type_id> } }
```

Mode

```
Global Configuration Mode
```

■ no network-clock clk-source

This command is used to delete a clock source.

Format

```
no network-clock clk-source <range_list> nominate
```

Mode

```
Global Configuration Mode
```

67.1.2. network-clock input-source

This command is used to set the station clock input frequency.

Default

```
none
```

Format

```
network-clock input-source { 1544khz | 2048khz | 10mhz }
```

Mode

```
Global Configuration Mode
```

■ no network-clock input-source

This command is used to delete the station clock input frequency.

Format

```
no network-clock input-source
```

Mode

```
Global Configuration Mode
```

67.1.3. network-clock output-source

This command is used to set the station clock output frequency.

Default

none

Format

network-clock output-source { 1544khz | 2048khz | 10mhz }

Mode

Global Configuration Mode

■ no network-clock output-source

This command is used to delete the station clock output frequency.

Format

no network-clock output-source

Mode

Global Configuration Mode

67.1.4. network-clock clk-source (aneg-mode)

This command is used to set the preferred negotiation. Include activate prefer master negotiation, activate prefer slave negotiation, activate forced slave negotiation.

Default

none

Format

network-clock clk-source *<range_list>* aneg-mode { [master | slave | forced] }

Mode

Global Configuration Mode

■ no network-clock clk-source

This command is used to remove the preferred negotiation.

Format

no network-clock clk-source *<range_list>* aneg-mode

Mode

Global Configuration Mode

67.1.5. network-clock clk-source (hold-timeout)

This command is used to set the hold-timeout.

Default

none

Format

network-clock clk-source *<range_list>* hold-timeout *<3-18,100>*

Mode

Global Configuration Mode

no network-clock clk-source

This command is used to delete the hold-timeout.

Format

```
no network-clock clk-source <range_list> hold-timeout
```

Mode

```
Global Configuration Mode
```

67.1.6. network-clock selector

This command is used to set selection mode of nominated clock sources.

Default

```
none
```

Format

```
network-clock selector { [ { manual clk-source <uint> } | selected | nonrevertive
| revertive | holdover | freerun ] }
```

Mode

```
Global Configuration Mode
```

no network-clock selector

This command is used to delete selection mode of nominated clock sources.

Format

```
no network-clock selector
```

Mode

```
Global Configuration Mode
```

67.1.7. network-clock clk-source (priority)

This command is used to set priority of nominated clock sources.

Default

```
none
```

Format

```
network-clock clk-source <range_list> priority <uint>
```

Mode

```
Global Configuration Mode
```

no network-clock clk-source

This command is used to delete priority of nominated clock sources.

Format

```
no network-clock clk-source <range_list> priority
```

Mode

```
Global Configuration Mode
```

67.1.8. network-clock wait-to-restore

This command is used to set WTR time.

Default

none

Format

network-clock wait-to-restore *<0-12>*

Mode

Global Configuration Mode

■ no network-clock wait-to-restore

This command is used to delete WTR time.

Format

no network-clock wait-to-restore

Mode

Global Configuration Mode

67.1.9. network-clock ssm-holdover

This command is used to set Hold Over SSM overwrite. "prc" represents primary reference clock, ssua represents synchronization supply unit A. "ssub" represents synchronization supply unit B, eec2 represents syncE ethernet equipment clock option 1. "eec1" represents syncE ethernet equipment clock option 2. "dnu "represents do not use. "inv" represents receiving invalid SSM (not defined) - NOT possible to set. "prs" represents primary reference source. "stu" represents synchronization traceability unknown. "st2" represents stratum 2. "tnc" represents transit node clock. "st3e" represents stratum 3E. "smc" represents SONET minimum clock. "prov" represents provisionable by network operator, "dus" represents don't use for sync.

Default

none

Format

network-clock ssm-holdover { [prc | ssua | ssub | eec2 | eec1 | dnu | inv | prs | stu | st2 | tnc | st3e | smc | prov | dus] }

Mode

Global Configuration Mode

■ no network-clock ssm-holdover

This command is used to delete Hold Over SSM overwrite.

Format

no network-clock ssm-holdover

Mode

Global Configuration Mode

67.1.10. network-clock ssm-freerun

This command is used to set Free Running SSM overwrite.

Default

none

Format

network-clock ssm-freerun { [prc | ssua | ssub | eec2 | eec1 | dnu | inv | prs | stu | st2 | tnc | st3e | smc | prov | dus] }

Mode

Global Configuration Mode

■ no network-clock ssm-freerun

This command is used to delete Free Running SSM overwrite.

Format

```
no network-clock ssm-freerun
```

Mode

```
Global Configuration Mode
```

67.1.11. network-clock clk-source

This command is used to set Clock source SSM overwrite.

Default

```
none
```

Format

```
network-clock clk-source <range_list> ssm-overwrite { prc | ssua | ssub | eec2 | eec1 | dnu | prs | stu | st2 | tnc | st3e | smc | prov | dus }
```

Mode

```
Global Configuration Mode
```

■ no network-clock clk-source

This command is used to delete Clock source SSM overwrite.

Format

```
no network-clock clk-source <range_list> ssm-overwrite
```

Mode

```
Global Configuration Mode
```

67.1.12. network-clock option

This command is used to set EEC options.

Default

```
none
```

Format

```
network-clock option { eec1 | eec2 }
```

Mode

```
Global Configuration Mode
```

■ no network-clock option

This command is used to delete EEC options.

Format

```
no network-clock option
```

Mode

```
Global Configuration Mode
```

67.1.13. network-clock synchronization ssm

This command is used to enable SSM.

Default

none

Format

network-clock synchronization ssm

Mode

Global Configuration Mode

■ no network-clock synchronization ssm

This command is used to disable SSM.

Format

no network-clock synchronization ssm

Mode

Global Configuration Mode

67.2. show

67.2.1. show network-clock

This command is used to display the clock synce configuration/status. It can show information based on clock type, port configuration, port status, PTP port, source-nomination-config, station-clock-config, and synchronization.

Format

show network-clock { [clock-selection-config | port-config | port-status | ptp-ports | source-nomination-config | station-clock-config | synchronization] }

Mode

User EXEC Mode

68. TCN

TCN (Train Communication Network) is an architectural framework designed to provide standardized communication systems for railway vehicles. Developed to address the growing communication demands of modern trains, TCN establishes an efficient solution for data exchange between various subsystems within the train.

68.1. ttdp

68.1.1. tcn ttdp

This command is used to enable/Disable TTDP Service.

Default

```
disable
```

Format

```
tcn ttdp { enable | disable }
```

Mode

```
Global Configuration Mode
```

68.1.2. tcn ttdp uuid

This command is used to configure the TTDP Formation Identifier. Here is the English translation: *<string36-36>* represents a configuration UUID string with the format: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx. *<word3-20>* represents a configuration string used to generate the UUID, containing 3 to 20 characters in length.

Default

```
none
```

Format

```
tcn ttdp { uuid <string36-36> | cst-str <word3-20> }
```

Mode

```
Global Configuration Mode
```

no tcn ttdp uuid

This command is used to delete the TTDP Formation Identifier.

Default

```
none
```

Format

```
no tcn ttdp uuid
```

Mode

```
Global Configuration Mode
```

68.1.3. tcn ttdp cnset

This command is used to all formation subnet information of ETBN.<*1-32*> represents the formation network set,<*vlan_id*> specifies the VLAN associated with this formation network,<*ipv4_addr*> indicates the host IPv4 address assigned to this formation network.

Default

none

Format

tcn ttdp cnset <*1-32*> [interface vlan <*vlan_id*> host-addr <*ipv4_addr*>]

Mode

Global Configuration Mode

■ no tcn ttdp cnset

This command is used to delete the ETBN formation subnet information. <*1-32*> represents the formation network set.

Default

none

Format

no tcn ttdp cnset <*1-32*>

Mode

Global Configuration Mode

68.1.4. tcn ttdp static-position

This command is used to the static location information of ETBN within the formation subnet. <*1-32*> represents the static location identifier of ETBN.

Default

none

Format

tcn ttdp static-position <*1-32*>

Mode

Global Configuration Mode

■ no tcn ttdp static-position

This command is used to delete the static location information of the ETBN subnet.

Default

none

Format

no tcn ttdp static-position

Mode

Global Configuration Mode

68.1.5. tcn ttdp etbn-num

The number of ETBNs in the formation subnet. *<1-32>* represents the quantity of ETBNs in the formation subnet.

Default

32

Format

tcn ttdp etbn-num *<1-32>*

Mode

Global Configuration Mode

no tcn ttdp etbn-num

This command is used to delete the number of ETBNs in the formation subnet.

Default

none

Format

no tcn ttdp etbn-num

Mode

Global Configuration Mode

68.1.6. tcn ttdp line

This command is used to configure TTDP links and link identifiers. *<1-2>* represents the line number. { A | B | C | D } represents the line identifier.

Default

none

Format

tcn ttdp line *<1-2>* { A | B | C | D }

Mode

Port Configuration Mode

no tcn ttdp line

This command is used to delete TTDP links and link identifiers. *<1-2>* represents the line number.{ A | B | C | D } represents the line identifier.

Default

none

Format

no tcn ttdp line *<1-2>* { A | B | C | D }

Mode

Port Configuration Mode

68.2. trdp

68.2.1. tcn trdp

This command is used to enable/Disable TTDP Service.

Default

```
disable
```

Format

```
tcn trdp { enable | disable }
```

Mode

```
Global Configuration Mode
```

68.2.2. tcn role etbn

This command is used to configure the device with the TCN role as ETBN.

Default

```
none
```

Format

```
tcn role etbn
```

Mode

```
Global Configuration Mode
```

■ no tcn role etbn

This command is used to delete device with the TCN role as ETBN.

Default

```
none
```

Format

```
no tcn role etbn
```

Mode

```
Global Configuration Mode
```

68.2.3. tcn trdp pd subscribe comid mcast-dest

This command is used to configure PD messages for subscription. <*1001-65535*> represents the comid to be configured, <*ipv4_mcast*> specifies the multicast address.

Default

```
none
```

Format

```
tcn trdp pd subscribe comid <1001-65535> mcast-dest <ipv4_mcast>
```

Mode

```
VLAN Configuration Mode
```

68.2.4. tcn trdp pd publish comid mcast-dest interval

This command is used to configure PD messages for publication. *<1001-65535>* represents the comid to be configured. *<ipv4_mcast>* specifies the multicast address. The *<1000-65535>* represents the interval for publishing PD messages, in milliseconds.

Default

none

Format

tcn trdp pd publish comid *<1001-65535>* mcast-dest *<ipv4_mcast>* interval *<1000-65535>*

Mode

VLAN Configuration Mode

no tcn trdp pd comid

The "no" command will no longer publish or subscribe to the PD message. *<1001-65535>* represents the comid to be configured.

Default

none

Format

no tcn trdp pd comid *<1001-65535>*

Mode

VLAN Configuration Mode

68.3. show

68.3.1. show tcn etbn status

This command is used to query the ETBN status information.

Format

show tcn etbn status

Mode

User EXEC Mode

68.3.2. show tcn ttdp status

This command is used to query the TTDP status information.

Format

show tcn ttdp status

Mode

User EXEC Mode

68.3.3. show tcn ttdp statistics

This command is used to query the TTDP statistics information.

Format

show tcn ttdp statistics

Mode

User EXEC Mode

68.4. clear

68.4.1. clear tcn ttdp statistics

This command is used to delete the TTDP statistics information.

Format

```
clear tcn ttdp statistics
```

Mode

```
User EXEC Mode
```

69. Thermal Protection

Thermal protection refers to the internal heat protection mechanism of a switch, which is used to monitor and maintain the temperature of the switch to prevent damage caused by overheating. This feature is crucial for ensuring the long-term stable operation of the switch.

69.1. thermal-protect

69.1.1. thermal-protect grp temperature

This command is used to set the temperature at which to turn ports mapped to corresponding group off. *<0~3>* group number.*<0-255>* Temperature at which to turn ports mapped to the corresponding group off.

Default

```
255
```

Format

```
thermal-protect grp <0~3> temperature <0-255>
```

Mode

```
Global Configuration Mode
```

■ no thermal-protect grp

This command is used to set the temperature at which to turn ports mapped to corresponding group off to default.

Format

```
no thermal-protect grp <0~3>
```

Mode

```
Global Configuration Mode
```

69.1.2. thermal-protect grp

This command is used to set the group for the port (s). *<0~3>* group number.

Default

```
disable
```

Format

```
thermal-protect grp <0~3>
```

Mode

```
Port Configuration Mode
```

■ no thermal-protect grp

This command is used to set the group for the ports to default.

Format

```
no thermal-protect grp
```

Mode

```
Port Configuration Mode
```

69.2. show

69.2.1. show thermal-protect

This command is used to shows thermal protection status (chip temperature and port status).

Format

```
show thermal-protect [ interface <port_type_list> ]
```

Mode

```
User EXEC Mode
```

70. Track

Track is used in network devices to monitor the status of specified objects and perform certain actions based on that status.

70.1. track

70.1.1. track ping

This command is used to set the monitoring parameters for a target, where address <*ipv4_addr*> indicates setting an IPv4 address; interface vlan <*vlan_id*> specifies the source interface number for the ping tracking instance; interval <*500-20000*> sets the value for the ping tracking interval, which must be a multiple of 100; timeout <*100-10000*> sets the timeout duration for ping replies, in milliseconds, and the value must be a multiple of 100; ttl <*1-255*> sets the value for the Time To Live (TTL) for ping request packets, with the range being from 1 to 255; success <*1-10*> sets the number of consecutive successful pings required for the tracked object to be considered reachable (up), with the range being from 1 to 10; lose <*1-10*> sets the number of consecutive failed pings required for the tracked object to be considered unreachable (down), with the range being from 1 to 10.

Default

none

Format

track ping <*1-128*> [address <*ipv4_addr*>] [interface vlan <*vlan_id*>] [interval <*500-20000*>] [timeout <*100-10000*>] [ttl <*1-255*>] [success <*1-10*>] [lose <*1-10*>]

Mode

Global Configuration Mode

no track ping

This command is used to delete track ping.

Format

no track ping <*1-128*>

Mode

Global Configuration Mode

no track ping address

This command is used to delete the address of the router to be monitored.

Format

no track ping <*1-128*> address

Mode

Global Configuration Mode

no track ping interface vlan

This command is used to delete the source interface number of the ping tracking instance.

Format

no track ping <*1-128*> interface vlan

Mode

Global Configuration Mode

no track ping interval

This command is used to delete the number of milliseconds between the pings to the target router address.

Format

```
no track ping <1-128> interval
```

Mode

```
Global Configuration Mode
```

no track ping timeout

This command is used to configure the timeout in milliseconds for a ping reply to default.

Format

```
no track ping <1-128> timeout
```

Mode

```
Global Configuration Mode
```

no track ping ttl

This command is used to configure the time to live for a ping request packet to default.

Format

```
no track ping <1-128> ttl
```

Mode

```
Global Configuration Mode
```

no track ping success

This command is used to delete the consecutive of ping successes.

Format

```
no track ping <1-128> success
```

Mode

```
Global Configuration Mode
```

no track ping lose

This command is used to delete the number of consecutive ping misses.

Format

```
no track ping <1-128> lose
```

Mode

```
Global Configuration Mode
```

70.1.2. track ping (enable)

This command is used to activate or deactivate a tracking instance.

Default

```
disable
```

Format

```
track ping <1-128> { enable | disable }
```

Mode

```
Global Configuration Mode
```

70.1.3. track interface

This command is used to configure interface track instances. <*1-128*> is track id. <*port_type_id*> is port interface. <*0-255*> is value for interface tracking that could be between 0 and 255.

Default

none

Format

track interface <*1-128*> [interface <*port_type_id*>] [linkup-delay <*0-255*>] [linkdown-delay <*0-255*>]

Mode

Global Configuration Mode

■ no track interface

This command is used to delete track interface.

Format

no track interface <*1-128*>

Mode

Global Configuration Mode

■ no track interface interface

This command is used to delete physical interface associated with the track instance.

Format

no track interface <*1-128*> interface

Mode

Global Configuration Mode

■ no track interface linkup-delay

This command is used to restore linkup-delay with the track instance to 0.

Format

no track interface <*1-128*> linkup-delay

Mode

Global Configuration Mode

■ no track interface linkdown-delay

This command is used to restore linkdown-delay with the track instance to 0.

Format

no track interface <*1-128*> linkdown-delay

Mode

Global Configuration Mode

70.1.4. track interface (enable)

This command is used to activate or deactivate a tracking instance.

Default

```
disable
```

Format

```
track interface <1-128> { enable | disable }
```

Mode

```
Global Configuration Mode
```

70.2. show

70.2.1. show track ping

This command is used to show the information for the ping tracking instances.

Format

```
show track ping [ <1-128> ]
```

Mode

```
User EXEC Mode
```

70.2.2. show track interface

This command is used to show the information for the interface tracking instances.

Format

```
show track interface [ <1-128> ]
```

Mode

```
User EXEC Mode
```

70.2.3. show track application

This command is used to show the applications subscribing to track objects.

Format

```
show track application
```

Mode

```
User EXEC Mode
```

71. TSN

TSN (Time-Sensitive Networking) is primarily used for implementing time synchronization, traffic scheduling, low latency, and traffic shaping.

71.1. tsn frame-preemption

71.1.1. tsn frame-preemption

This command is used to frame preemption interface configuration.

Default

```
disable
```

Format

```
tsn frame-preemption
```

Mode

```
Port Configuration Mode
```

■ no tsn frame-preemption

This command is used to disable frame-preemption on interface.

Format

```
no tsn frame-preemption
```

Mode

```
Port Configuration Mode
```

71.1.2. tsn frame-preemption verify-disable

This command is used to enable verify-disable on interface.

Default

```
disable
```

Format

```
tsn frame-preemption verify-disable
```

Mode

```
Port Configuration Mode
```

■ no tsn frame-preemption verify-disable

This command is used to disable verify-disable on interface.

Format

```
no tsn frame-preemption verify-disable
```

Mode

```
Port Configuration Mode
```

71.1.3. tsn frame-preemption queue

This command is used to enable frame-preemption on specific queue(s).*<0-6>* Specific queue or range.

Default

```
disable
```

Format

```
tsn frame-preemption queue <0-6>
```

Mode

```
Port Configuration Mode
```

■ no tsn frame-preemption queue

This command is used to disable frame-preemption on specific queue(s).*<0-6>* Specific queue or range.

Format

```
no tsn frame-preemption queue <0-6>
```

Mode

```
Port Configuration Mode
```

71.1.4. tsn frame-preemption ignore-lldp

This command is used to do not wait to receive lldp message before starting frame-preemption in transmit direction.

Default

```
disable
```

Format

```
tsn frame-preemption ignore-lldp
```

Mode

```
Port Configuration Mode
```

■ no tsn frame-preemption ignore-lldp

This command is used to wait to receive lldp message before starting frame-preemption in transmit direction.

Format

```
no tsn frame-preemption ignore-lldp
```

Mode

```
Port Configuration Mode
```

71.2. tsn tas

71.2.1. tsn tas always-guard-band

This command is used to guard band is implemented for any queue to scheduled queues transition.

Default

```
enable
```

Format

```
tsn tas always-guard-band
```

Mode

```
Global Configuration Mode
```

■ no tsn tas always-guard-band

This command is used to guard band is implemented for any queue to scheduled queues transition to default.

Format

```
no tsn tas always-guard-band
```

Mode

```
Global Configuration Mode
```

71.2.2. tsn tas gate-enabled

This command is used to enable time aware shaper.

Default

```
disable
```

Format

```
tsn tas gate-enabled
```

Mode

```
Port Configuration Mode
```

■ no tsn tas gate-enabled

This command is used to disable time aware shaper.

Format

```
no tsn tas gate-enabled
```

Mode

```
Port Configuration Mode
```

71.2.3. tsn tas gate-states queue

This command is used to configure initial gate states for each queue.<*0-7*> Specific queue or range.

Default

```
open
```

Format

```
tsn tas gate-states queue <0~7> { open | closed }
```

Mode

```
Port Configuration Mode
```

■ no tsn tas gate-states

This command is used to configure initial gate states for each queue to default value.

Format

```
no tsn tas gate-states
```

Mode

```
Port Configuration Mode
```

71.2.4. tsn tas control-list-length

This command is used to configure Control List Length.

Default

0

Format

tsn tas control-list-length *<uint>*

Mode

Port Configuration Mode

■ no tsn tas control-list-length

This command is used to configure control List Length default value.

Format

no tsn tas control-list-length

Mode

Port Configuration Mode

71.2.5. tsn tas control-list index

This command is used to configure admin control list,*<0-255>* Admin Control List index,*<0~7>* Specific queue or range.

Default

none

Format

tsn tas control-lis index *<0-255>* gate-state queue *<0~7>* { open | closed } time-interval *<1-999999999>* [operation { set | set-hold | set-release }]

Mode

Port Configuration Mode

71.2.6. tsn tas cycle-time

This command is used to configure admin cycle time.

Default

100 ms

Format

tsn tas cycle-time *<1-999999999>* { ms | us | ns }

Mode

Port Configuration Mode

■ no tsn tas cycle-time

This command is used to set admin cycle time to default.

Format

no tsn tas cycle-time

Mode

Port Configuration Mode

71.2.7. tsn tas cycle-time-extension

This command is used to configure admin cycle time extenstion.

Default

256

Format

tsn tas cycle-time-extension *<256-999999999>*

Mode

Port Configuration Mode

no tsn tas cycle-time-extension

This command is used to set admin cycle time extenstion to default.

Format

no tsn tas cycle-time-extension

Mode

Port Configuration Mode

71.2.8. tsn tas base-time seconds

This command is used to configure admin base time. "seconds" represents seconds, and "nanoseconds" represents nanoseconds.

Default

256

Format

tsn tas base-time seconds *<0-4294967295>* nanoseconds *<0-999999999>*

Mode

Port Configuration Mode

no tsn tas base-time

This command is used to configure admin base time to default.

Format

no tsn tas base-time

Mode

Port Configuration Mode

71.2.9. tsn tas config-change

This command is used to start a configuration change.

Default

disable

Format

tsn tas config-change

Mode

Port Configuration Mode

71.2.10. tsn tas max-sdu queue

This command is used to configure max-sdu for particular queue or range of queues.

Default

```
disable
```

Format

```
tsn tas max-sdu queue <0-7> <0-10240>
```

Mode

```
Port Configuration Mode
```

■ no tsn tas max-sdu queue

This command is used to configure max-sdu for particular queue or range of queues to default value.

Format

```
no tsn tas max-sdu queue <0-7>
```

Mode

```
Port Configuration Mode
```

71.3. dmac

71.3.1. dmac

This command is used to Specify a destination MAC to match against incoming frames. <*mac_addr*> A destination MAC address to match against incoming frames. "/" Specify a mask. If no mask is specified, all bits of the destination MAC address shall match the incoming frame. <*dmac_mask*> A mask in the form xx:xx:xx:xx:xx:xx, that specifies which bits of the destination MAC address that shall match the incoming frames. Default is to match all 48 bits. "any" Match any destination MAC address. "broadcast" Match the broadcast destination MAC address."multicast" Match any multicast destination MAC address (excluding broadcast)."not-broadcast" Match any MAC address, except the broadcast MAC address."not-unicast" Match any multicast or the broadcast destination MAC address."unicast" Match any unicast MAC address.

Default

```
any
```

Format

```
dmac { <dmac_addr> [ / <dmac_mask> ] | multicast | broadcast | unicast | not-broadcast
| not-unicast | any }
```

Mode

```
STREAM Configuration Mode
```

■ no dmac

This command is used to don't match on incoming destination MAC address.

Format

```
no dmac
```

Mode

```
STREAM Configuration Mode
```

71.4. smac

71.4.1. smac

This command is used to Specify a source MAC mask to match against incoming frames. <*mac_addr*> A source MAC address to match against incoming frames. “/” Specify a mask. If no mask is specified, all bits of the destination MAC address shall match the incoming frame. < *mask_mac_addr* > A mask in the form xx:xx:xx:xx:xx:xx, that specifies which bits of the destination MAC address that shall match the incoming frames. Default is to match all 48 bits.“any” Match any source mac address.

Default

```
disable
```

Format

```
smac { <mac_addr> [ / <mask_mac_addr> ] | any }
```

Mode

```
STREAM Configuration Mode
```

no smac

This command is used to don't match on incoming source MAC address.

Format

```
no smac
```

Mode

```
STREAM Configuration Mode
```

71.5. outer-tag

71.5.1. outer-tag

This command is used to configuration of an outer tag to match against incoming frames. “none” The frame must be untagged.“vid” The frame must be tagged. The next keyword tells whether all VLANs are matched or only a specific with an optional mask. “/” Specify a mask. If no mask is specified, all bits of the VLAN ID shall match the incoming frame. <*0-4095*> VLAN ID to match incoming frames against. “any” Match any incoming VLAN ID.“pcp” Configuration of a PCP value to match against incoming frames. <*0-7*> The PCP value to match the incoming frames against. <*0-7*> A mask that specifies the bits of the PCP value that shall match the incoming frame. “dei” Specify a DEI value to match the incoming frame against. <*0-1*> The DEI value that shall match the incoming frame. “c-tag” If specified, only match C-tagged frames (EtherType = 0x8100). “s-tag” If specified, only match S-tagged frames (EtherType = 0x88a8).

Default

```
disable
```

Format

```
outer-tag { none | vid { { <vid> [ / <0-4095> ] | any } [ pcp <0-7> [ / <0-7> ] ]
[ dei <0-1> ] [ { c-tag | s-tag } ] } }
```

Mode

```
STREAM Configuration Mode
```

no outer-tag

This command is used to don't use outer tag for matching. It may be both tagged and untagged.

Format

```
no outer-tag
```

Mode

```
STREAM Configuration Mode
```

71.6. inner-tag

71.6.1. inner-tag

This command is used to configuration of an inner tag to match against incoming frames. “none” The frame must be untagged.“vid” The frame must be tagged. The next keyword tells whether all VLANs are matched or only a specific with an optional mask. “/” Specify a mask. If no mask is specified, all bits of the VLAN ID shall match the incoming frame. *<0-4095>* VLAN ID to match incoming frames against. “any” Match any incoming VLAN ID.“pcp” Configuration of a PCP value to match against incoming frames. *<0-7>* The PCP value to match the incoming frames against. *<0-7>* A mask that specifies the bits of the PCP value that shall match the incoming frame. “dei” Specify a DEI value to match the incoming frame against. *<0-1>* The DEI value that shall match the incoming frame. “c-tag” If specified, only match C-tagged frames (EtherType = 0x8100). “s-tag” If specified, only match S-tagged frames (EtherType = 0x88a8).

Default

```
disable
```

Format

```
inner-tag { none | vid { { <vid> [ / <0-4095> ] | any } [ pcp <0-7> [ / <0-7> ] ]
[ dei <0-1> ] [ { c-tag | s-tag } ] } }
```

Mode

```
STREAM Configuration Mode
```

no inner-tag

This command is used to don't use inner tag for matching. It may be both tagged and untagged.

Format

```
no inner-tag
```

Mode

```
STREAM Configuration Mode
```

71.7. etype

71.7.1. etype

This command is used to match EtherType frames. *<0x600-0xffff>* Matched EtherType.

Default

```
none
```

Format

```
etype <0x600-0xffff>
```

Mode

```
STREAM Configuration Mode
```

no etype

This command is used to don't match incoming frames EtherType.

Format

```
no etype
```

Mode

```
STREAM Configuration Mode
```

71.8. llc

71.8.1. llc

This command is used to match Logical Link Control (LLC) frames, i.e. frames with EtherType/TypeLength field less than 0x600. *<0x0-0xff>* Matched LLC Destination Service Access Point (DSAP). *<0x0-0xff>* Matched LLC Source Service Access Point (SSAP).

Default

```
none
```

Format

```
llc <0x0-0xff> <0x0-0xff>
```

Mode

```
STREAM Configuration Mode
```

no llc

This command is used to don't match LLC frames.

Format

```
no llc
```

Mode

```
STREAM Configuration Mode
```

71.9. snap

71.9.1. snap

This command is used to match Subnetwork Access Protocol (SNAP) frames, i.e. frames with EtherType/TypeLength field less than 0x600 and DSAP = 0xaa and SSAP = 0xAA and Control field = 0x03. *<0x0-0xffffff>* SNAP OUI (Range 0x000000 - 0XFFFFFF). “rfc-1042” SNAP OUI is speficied in RFC1042, that is, 00:00:00.“snap-8021h” SNAP OUI is specified in 802.1H, that is, 00:00:F8.< *0x0-0xffff* > Protocol ID (Range: 0x0 - 0xFFFF). If OUI is all-zeros (rfc-1042), then this must be a valid EtherType (>= 0x600).

Default

```
none
```

Format

```
snap { <0x0-0xffffff> | rfc-1042 | snap-8021h } <0x0-0xffff>
```

Mode

```
STREAM Configuration Mode
```

no snap

This command is used to don't match SNAP frames.

Format

```
no snap
```

Mode

```
STREAM Configuration Mode
```

71.10. ipv4

71.10.1. ipv4

This command is used to match IPv4 frames. “sip” Match on source IPv4 address. <*sip*> Match on source IPv4 address/mask. “any” Match on any source IPv4 address. “dip” Match on destination IPv4 address. <*dip*> Match on source IPv4 address/mask.“dscp” Match on DSCP. <*dscp_vr*> Matched DSCP value/range. “be” Default PHB (DSCP 0) for best effort traffic. “af #” Assured Forwarding PHB AF “cs #” Class Selector PHB CS1 precedence #. “fragment” Setup matching on IPv4 fragments. “any” Match any values of IPv4 header's MF bit and fragment offset value. “yes” Match IPv4 headers with MF bit set or a fragment offset > 0. “no” Match IPv4 headers with MF bit cleared and fragment offset 0.“proto” Match on IP protocol. <*0-255*> Match a custom IP protocol number. “tcp” Match TCP frames (protocol number 6). “udp” Match UDP frames (protocol number 17). “any” Match any IP protocol. “dport” Setup matching on UDP/TCP destination port. <*dport_vr*> Match UDP/TCP destination port value/range (e.g. 123-345 or 123). “any” Match any UDP/TCP destination port.

Default

```
none
```

Format

```
ipv4 [ sip { <sip> | any } ] [ dip { <dip> | any } ] [ dscp { <dscp_vr> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any } ] [ fragment { yes | no | any } ] [ proto { <0-255> | tcp | udp | any } ] [ dport { <dport_vr> | any } ]
```

Mode

```
STREAM Configuration Mode
```

■ no ipv4

This command is used to don't match IPv4 frames.

Format

```
no ipv4
```

Mode

```
STREAM Configuration Mode
```

71.11. ipv6

71.11.1. ipv6

This command is used to match IPv6 frames. “sip” Match on source IPv4 address. <*sip*> Match on source IPv4 address/mask. “any” Match on any source IPv4 address. “dip” Match on destination IPv4 address. <*dip*> Match on source IPv4 address/mask.“dscp” Match on DSCP. <*dscp_vr*> Matched DSCP value/range. “be” Default PHB (DSCP 0) for best effort traffic. “af#” Assured Forwarding PHB AF “cs#” Class Selector PHB CS1 precedence #.“proto” Match on IP protocol. <*0-255*> Match a custom IP protocol number. “tcp” Match TCP frames (protocol number 6). “udp” Match UDP frames (protocol number 17). “any” Match any IP protocol. “dport” Setup matching on UDP/TCP destination port. <*dport_vr*> Match UDP/TCP destination port value/range (e.g. 123-345 or 123). “any” Match any UDP/TCP destination port.

Default

```
none
```

Format

```
ipv6 [ sip { <sip> | any } ] [ dip { <dip> | any } ] [ dscp { <dscp_vr> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any } ] [ proto { <0-255> | tcp | udp | any } ] [ dport { <dport_vr> | any } ]
```

Mode

```
STREAM Configuration Mode
```

no ipv6

This command is used to don't Match IPv6 frames.

Format

```
no ipv6
```

Mode

```
STREAM Configuration Mode
```

71.12. cir

71.12.1. cir

This command is used to configure flow meter committed information rate in kbps. <*uint*> Committed Information Rate measured in kbps. Gets rounded up to the nearest value supported by the policer and will be reflected in running-config.This rate refers to the payload rate of the data frame.

Default

```
10000
```

Format

```
cir <uint>
```

Mode

```
TSN PSFP Flow Meter Mode
```

no cir

This command is used to configure flow meter committed information rate in kbps to default.

Format

```
no cir <uint>
```

Mode

```
TSN PSFP Flow Meter Mode
```

71.13. cbs

71.13.1. cbs

This command is used to configure flow meter committed burst size in bytes.<*uint*> Committed Burst Size measured in bytes. Gets rounded up to the nearest value supported by the policer and will be reflected in running-config.

Default

```
2048
```

Format

```
cbs <uint>
```

Mode

```
TSN PSFP Flow Meter Mode
```

no cbs

This command is used to configure flow meter committed burst size in bytes to default.

Format

```
no cbs <uint>
```

Mode

```
TSN PSFP Flow Meter Mode
```

71.14. eir

71.14.1. eir

This command is used to configure excess information rate in kbps. <*uint*> Excess Information Rate measured in kbps. Gets rounded up to the nearest value supported by the policer and will be reflected in running-config.This rate refers to the payload rate of the data frame.

Default

```
0
```

Format

```
eir <uint>
```

Mode

```
TSN PSFP Flow Meter Mode
```

no eir

This command is used to configure excess information rate in kbps to default.

Format

```
no eir <uint>
```

Mode

```
TSN PSFP Flow Meter Mode
```

71.15. ebs

71.15.1. ebs

This command is used to configure flow meter excess burst size in bytes.<*uint*> Excess Burst Size measured in bytes. Gets rounded up to the nearest value supported by the policer and will be reflected in running-config.

Default

```
0
```

Format

```
ebs <uint>
```

Mode

```
TSN PSFP Flow Meter Mode
```

no ebs

This command is used to configure flow meter excess burst size in bytes to default.

Format

```
no ebs <uint>
```

Mode

```
TSN PSFP Flow Meter Mode
```

71.16. coupling-flag

71.16.1. coupling-flag

This command is used to configure coupling flag to be enabled.

Default

```
0
```

Format

```
coupling-flag
```

Mode

```
TSN PSFP Flow Meter Mode
```

no coupling-flag

This command is used to configure coupling flag to be disabled.

Format

```
no coupling-flag
```

Mode

```
TSN PSFP Flow Meter Mode
```

71.17. color-mode

71.17.1. color-mode

This command is used to configure color mode enabled.

Default

```
disable
```

Format

```
color-mode
```

Mode

```
TSN PSFP Flow Meter Mode
```

no color-mode

This command is used to configure color mode disabled.

Format

```
no color-mode
```

Mode

```
TSN PSFP Flow Meter Mode
```

71.18. mark-red-enable

71.18.1. mark-red-enable

This command is used to set PSFP flow meter mark all frames red enable.

Default

```
disable
```

Format

```
mark-red-enable
```

Mode

```
TSN PSFP Flow Meter Mode
```

■ no mark-red-enable

This command is used to set PSFP flow meter mark all frames red disabled.

Format

```
no mark-red-enable
```

Mode

```
TSN PSFP Flow Meter Mode
```

71.19. drop-on-yellow

71.19.1. drop-on-yellow

This command is used to set PSFP flow meter Drop on Yellow.

Default

```
disable
```

Format

```
drop-on-yellow
```

Mode

```
TSN PSFP Flow Meter Mode
```

■ no drop-on-yellow

This command is used to clear PSFP Flow Meter Drop on Yellow.

Format

```
no drop-on-yellow
```

Mode

```
TSN PSFP Flow Meter Mode
```

71.20. no tsn

71.20.1. no tsn flow meter

This command is used to delete flow meter.

Format

```
no tsn flow meter <uint>
```

Mode

```
Global Configuration Mode
```

71.20.2. no tsn stream filter

This command is used to delete stream filter.

Format

```
no tsn stream filter <uint>
```

Mode

```
Global Configuration Mode
```

71.20.3. no tsn stream gate

This command is used to delete stream gate.

Format

```
no tsn stream gate <uint>
```

Mode

```
Global Configuration Mode
```

71.21. stream-id

71.21.1. stream-id

This command is used to set filter to point to a stream.

Default

```
0
```

Format

```
stream-id <1-127>
```

Mode

```
TSN PSFP Stream Filter Mode
```

■ no stream-id

This command is used to remove configuration of stream for the filter.

Format

```
no stream-id
```

Mode

```
TSN PSFP Stream Filter Mode
```

71.22. stream-collection-id

71.22.1. stream-collection-id

This command is used to if more than one stream is to be matched in generator mode, use stream collections.
<*1-63*> ID of the stream collection to attach this filter to.

Default

```
disable
```

Format

```
stream-collection-id <1-63>
```

Mode

```
TSN PSFP Stream Filter Mode
```

no stream-collection-id

This command is used to remove configuration of stream collection ID.

Format

```
no stream-collection-id
```

Mode

```
TSN PSFP Stream Filter Mode
```

71.23. priority

71.23.1. priority

This command is used to set PSFP priority to match (0-7).

Default

```
none
```

Format

```
priority { <0-7> | any }
```

Mode

```
TSN PSFP Stream Filter Mode
```

no priority

This command is used to set PSFP priority to default.

Format

```
no priority
```

Mode

```
TSN PSFP Stream Filter Mode
```

71.24. gate id

71.24.1. gate id

This command is used to set PSFP stream gate instance ID.

Default

```
none
```

Format

```
gate id <0-254>
```

Mode

```
TSN PSFP Stream Filter Mode
```

■ no gate

This command is used to set PSFP stream gate instance ID to default.

Format

```
no gate
```

Mode

```
TSN PSFP Stream Filter Mode
```

71.25. max-sdu

71.25.1. max-sdu

This command is used to set PSFP maximum SDU size.<*uint*> Set maximum allowed frame size for the filter. Any frame exceeding this value will be discarded. A value of 0 disables the feature.

Default

```
0
```

Format

```
max-sdu <uint>
```

Mode

```
TSN PSFP Stream Filter Mode
```

■ no max-sdu

This command is used to set PSFP maximum SDU size to default.

Format

```
no max-sdu
```

Mode

```
TSN PSFP Stream Filter Mode
```

71.26. flow-meter

71.26.1. flow-meter id

This command is used to set PSFP flow meter instance ID.*<1-1022>* ID of a flow meter to use with this filter.

Default

```
0
```

Format

```
flow-meter id <1-1022>
```

Mode

```
TSN PSFP Stream Filter Mode
```

■ no flow-meter

This command is used to set PSFP flow meter instance ID to default.

Format

```
no flow-meter
```

Mode

```
TSN PSFP Stream Filter Mode
```

71.27. block-due-to-oversize-enable

71.27.1. block-due-to-oversize-enable

This command is used to set PSFP stream blocked due to oversize frame enable.

Default

```
disable
```

Format

```
block-due-to-oversize-enable
```

Mode

```
TSN PSFP Stream Filter Mode
```

■ no block-due-to-oversize-enable

This command is used to set PSFP stream blocked due to oversize frame disable.

Format

```
no block-due-to-oversize-enable
```

Mode

```
TSN PSFP Stream Filter Mode
```

71.28. enable

71.28.1. enable

This command is used to enable the gate.

Default

```
0
```

Format

```
enable
```

Mode

```
TSN PSFP Stream Gate Mode
```

no enable

This command is used to disable the gate.

Format

```
no enable
```

Mode

```
TSN PSFP Stream Gate Mode
```

71.29. state

71.29.1. state

This command is used to set state when no gate control list is executing. Default state is closed.

Default

```
closed
```

Format

```
state { open | closed }
```

Mode

```
TSN PSFP Stream Gate Mode
```

71.30. config-change

71.30.1. config-change

This command is used to apply current config to hardware. When changing configuration while gate is enabled, config-change needs to be issued before the configuration is applied.

Default

```
none
```

Format

```
config-change
```

Mode

```
TSN PSFP Stream Gate Mode
```

71.31. cycle-time

71.31.1. cycle-time

This command is used to set admin cycle time in units of either milliseconds (ms), microseconds (us) or nano seconds (ns).

Default

```
0 ns
```

Format

```
cycle-time <1-1000000000> { ms | us | ns }
```

Mode

```
TSN PSFP Stream Gate Mode
```

no cycle-time

This command is used to set admin cycle time to 0, ie. disable the gate control list.

Default

```
0
```

Format

```
no cycle-time
```

Mode

```
TSN PSFP Stream Gate Mode
```

71.32. control-list-length

71.32.1. control-list-length

This command is used to set size of gate control list. *<0-4>* Length of gate control list.

Default

```
0
```

Format

```
control-list-length <0-4>
```

Mode

```
TSN PSFP Stream Gate Mode
```

71.33. base-time

71.33.1. base-time seconds

This command is used to set admin base time. *<0-4294967295>* Seconds. “nanoseconds” Specify nanoseconds. *<0-999999999>* Nanoseconds. Default is 0.

Default

```
0
```

Format

```
base-time seconds <0-4294967295> [ nanoseconds <0-999999999> ]
```

Mode

```
TSN PSFP Stream Gate Mode
```

no base-time

This command is used to set admin base time to 0 second.

Format

```
no base-time
```

Mode

```
TSN PSFP Stream Gate Mode
```

71.34. ipv

71.34.1. ipv

This command is used to set admin internal priority value to be used when no gate control list is executing.<*0-7*> Set frame's initial internal priority value (egress queue). May be overridden by a control list entry later.

Default

```
0
```

Format

```
ipv <0-7>
```

Mode

```
TSN PSFP Stream Gate Mode
```

no ipv

This command is used to not set the administrative internal priority value when a gated control list is not executed.

Format

```
no ipv
```

Mode

```
TSN PSFP Stream Gate Mode
```

71.35. close-due-to-invalid-rx-enable

71.35.1. close-due-to-invalid-rx-enable

This command is used to enable the gate closure function when invalid data is received.

Default

```
disable
```

Format

```
close-due-to-invalid-rx-enable
```

Mode

```
TSN PSFP Stream Gate Mode
```

no close-due-to-invalid-rx-enable

This command is used to disable the gate closure function when invalid data is received.

Format

```
no close-due-to-invalid-rx-enable
```

Mode

```
TSN PSFP Stream Gate Mode
```

71.36. close-due-to-octets-exceeded-enable

71.36.1. close-due-to-octets-exceeded-enable

This command is used to set gate closed due to octets exceeded Rx enable.

Default

```
disable
```

Format

```
close-due-to-octets-exceeded-enable
```

Mode

```
TSN PSFP Stream Gate Mode
```

■ no close-due-to-octets-exceeded-enable

This command is used to set gate closed due to octets exceeded Rx disable.

Format

```
no close-due-to-octets-exceeded-enable
```

Mode

```
TSN PSFP Stream Gate Mode
```

71.37. control-list

71.37.1. control-list index

This command is used to configures PSFP admin control list. Index *<0-3>* represent specify index. Gate-state represents configure gate state, include open, and closed stream gate. Time-interval *<1-999999999>* represent configure time interval. Ipv *<0-7>* represent configure Internal priority value. Octet-max <uint> represent configure Max number of octets.

Default

```
none
```

Format

```
control-list index <0-3> gate-state { open | closed } time-interval <1-999999999>
{ ms | us | ns } [ ipv <0-7> ] [ octet-max <uint> ]
```

Mode

```
TSN PSFP Stream Gate Mode
```

■ no control-list index

This command is used to remove entry from control list.

Format

```
no control-list index <0-3>
```

Mode

```
TSN PSFP Stream Gate Mode
```

71.38. time-extension

71.38.1. time-extension

This command is used to set the gate's cycle time extension. *<1-1000000000>* Set the gate's cycle time extension. An extension of up to 1 second can be specified. ms Set admin cycle time extension value in units of milliseconds.With this unit, the cycle time extension cannot exceed 1000 ms us Set admin cycle time extension value in units of microseconds.With this unit, the cycle time extension cannot exceed 1,000,000 us ns Set admin cycle time extension value in units of nanoseconds.With this unit, the cycle time extension cannot exceed 1,000,000,000 ns.

Default

```
disable
```

Format

```
time-extension <1-1000000000> { ms | us | ns }
```

Mode

```
TSN PSFP Stream Gate Mode
```

■ no time-extension

This command is used to set the gate's cycle time extension to 0.

Format

```
no time-extension
```

Mode

```
TSN PSFP Stream Gate Mode
```

71.39. stream-id-list

71.39.1. stream-id-list

This command is used to select the ingress streams that should map to this FRER instance. Only one stream ID can be specified in generator mode. *<1-127>* List of stream IDs. This indirectly gives the ingress ports.

Default

```
disable
```

Format

```
stream-id-list <1-127>
```

Mode

```
STREAM-COLLECTION Configuration Mode
```

■ no stream-id-list

This command is used to clear the list of ingress stream IDs.

Format

```
no stream-id-list
```

Mode

```
STREAM-COLLECTION Configuration Mode
```

71.40. show

71.40.1. show tsn current-time

This command is show current TSN time.

Format

```
show tsn current-time
```

Mode

```
User EXEC Mode
```

71.40.2. show tsn tas status

This command is used to display the operational parameters of TAS.

Format

```
show tsn tas status [ interface <port_type_list> ]
```

Mode

```
User EXEC Mode
```

71.40.3. show tsn flow meter

This command is used to show statistics for PSFP filter.

Format

```
show tsn flow meter [ <0~1022> ] status
```

Mode

```
User EXEC Mode
```

71.40.4. show tsn stream gate

This command is used to show status of TSN stream gate.

Format

```
show tsn stream gate [ <0~1022> ] status
```

Mode

```
User EXEC Mode
```

71.40.5. show tsn stream filter

This command is used to show statistics for PSFP filter.

Format

```
show tsn stream filter [ <0~1022> ] { statistics | status }
```

Mode

```
User EXEC Mode
```

71.40.6. show tsn frame-preemption status

This command is used to display the frame-preemption status.

Format

```
show tsn frame-preemption status [ interface <port_type_list> ]
```

Mode

```
User EXEC Mode
```

71.40.7. show stream

This command is used to show status of streams. <*1-127*> ID of stream for which to show status. “details” Show detailed stream status.

Format

```
show stream [ <1-127> ] status [ details ]
```

Mode

```
User EXEC Mode
```

71.40.8. show stream-collection

This command is used to show status of stream collections. <*1-63*> ID of stream collection for which to show status.

Format

```
show stream-collection [ <1-63> ] status [ details ]
```

Mode

```
User EXEC Mode
```

71.41. clear

71.41.1. clear tsn flow meter

This command is used to clear the markAllFramesRed flag.

Format

```
clear tsn flow meter [ <0~1022> ] [ mark-red ]
```

Mode

```
User EXEC Mode
```

71.41.2. clear tsn stream gate

This command is used to clear the stream-closed flags on stream gate.

Format

```
clear tsn stream gate [ <0~1022> ] [ gate-closed-due-to-octets-exceeded |
gate-closed-due-to-invalid-rx ]
```

Mode

```
User EXEC Mode
```

71.41.3. clear tsn stream filter

This command is used to clear the gate-closed-due-to-octets-exceeded flag.

Format

```
clear tsn stream filter [ <0~1022> ] [ statistics |
stream-blocked-due-to-oversize-frame ]
```

Mode

```
User EXEC Mode
```

72. UART2NET

UART2NET is a technology or device that converts UART serial communication into network communication. In the Internet of Things and embedded systems, the UART2NET function is often used to connect local serial devices to remote network servers to achieve remote management and data transmission of devices.

72.1. uart

72.1.1. uart session-mode udp

This command is used to configure the serial port as the udp session mode.

Default

```
startup defaults to no server and no client
```

Format

```
uart session-mode udp port <5000-29997> ip-address <ipv4_addr>
```

Mode

```
Uart Mode
```

72.1.2. uart session-mode tcp-server

This command is used to configure the serial port as the TCP server session mode.

Default

```
startup defaults to no server and no client
```

Format

```
uart session-mode tcp-server port <5000-29997>
```

Mode

```
Uart Mode
```

72.1.3. uart session-mode udp

This command is used to configure the serial port as the udp session mode.

Default

```
startup defaults to no server and no client
```

Format

```
uart session-mode tcp-client port <5000-29997> ip-address <ipv4_addr>
```

Mode

```
Uart Mode
```

72.1.4. uart session-mode none

This command is used to close all sessions of the serial port.

Default

```
none
```

Format

```
uart session-mode none
no uart session-mode
```

Mode

```
Uart Mode
```

72.1.5. mode

This command is used to set the working mode of the serial port.

Default

```
RS232-full
```

Format

```
mode { RS232-full | RS485-half | RS485-full }
```

Mode

```
Uart Mode
```

■ no mode

This command is used to turn off the working mode of the serial port.

Format

```
no mode
```

Mode

```
Uart Mode
```

72.1.6. speed

This command is used to set the baud rate of the serial port.

Default

```
9600
```

Format

```
speed { 9600 | 19200 | 38400 | 57600 | 115200 }
```

Mode

```
Uart Mode
```

■ no speed

This command is used to restore the serial port baud rate to Default.

Format

```
no speed
```

Mode

```
Uart Mode
```

72.1.7. databits

This command is used to set the number of data bits of the serial port.

Default

```
8
```

Format

```
databits <5-8>
```

Mode

```
Uart Mode
```

■ no databits

This command is used to restore the number of serial port data bits to Default.

Format

```
no databits
```

Mode

```
Uart Mode
```

72.1.8. stopbits

This command is used to set the number of stop bits of the serial port.

Default

```
1
```

Format

```
stopbits <1-2>
```

Mode

```
Uart Mode
```

■ no stopbits

This command is used to restore the working mode to the number of stop bits.

Format

```
no stopbits
```

Mode

```
Uart Mode
```

72.1.9. parity

This command is used to set the serial port verification mode.

Default

```
none
```

Format

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

Mode

```
Uart Mode
```

■ no speed

This command is used to turn off the serial port verification mode.

Format

```
no parity
```

Mode

```
Uart Mode
```

72.1.10. flow-control

This command is used to configure uart flow control mode.

Default

```
none
```

Format

```
flow-control { none | software | hardware }
```

Mode

```
Uart Mode
```

■ no flow-control

This command is used to turn off uart flow control mode.

Format

```
no flow-control
```

Mode

```
Uart Mode
```

72.1.11. keep-alive

This command is used to set the serial port to enable the livekeeping mechanism on the TCP server/client.

Default

```
keep-alive
```

Format

```
keep-alive
```

Mode

```
Uart Mode
```

■ no keep-alive

This command is used to turn off the serial port tcp server/client livekeeping mechanism.

Format

```
no keep-alive
```

Mode

```
Uart Mode
```

72.1.12. loop-detect

This command is used to test whether uart is in loopback status.

Default

```
none
```

Format

```
loop-detect
```

Mode

```
Uart Mode
```

72.2. show

72.2.1. show uart

This command is used to display uart configuration information.

Format

```
show uart [ <1-4> ]
```

Mode

```
User EXEC Mode
```

72.3. Clear

72.3.1. clear uart statistics

This command is used to clear and clear uart statistics.

Format

```
clear uart [ <1-4> ] statistics
```

Mode

```
User EXEC Mode
```

73. UDLD

UDLD (Uni Directional Link Detection). UDLD protocol monitors the physical configuration of the links between devices and ports that support UDLD. It detects the existence of unidirectional links. Its functionality is to provide mechanisms useful for detecting one way connections before they create a loop or other protocol malfunction. RFC 5171 specifies a way at data link layer to detect Uni directional link.

73.1. udld

73.1.1. Udld

This command is used to enable UDLD in aggressive or normal mode on all fiber-optic ports.

Default

```
disable
```

Format

```
udld { aggressive | enable }
```

Mode

```
Global Configuration Mode
```

■ no udld

This command is used to disable UDLD in normal mode or disable aggressive mode on all fiber-optic ports.

Format

```
no udld { aggressive | enable }
```

Mode

```
Global Configuration Mode
```

73.1.2. udld message time-interval

This command is used to configure the period of time between UDLD probe messages on all ports that are in the advertisement phase and are determined to be bidirectional. *<7-90>* represents message interval value.

Default

```
7
```

Format

```
udld message time-interval <7-90>
```

Mode

```
Global Configuration Mode
```

73.1.3. udld port

This command is used to enable UDLD in the aggressive mode on an interface.

Default

```
disable
```

Format

```
udld port aggressive
```

Mode

```
Port Configuration Mode
```

no udld port

This command is used to disable UDLD in the aggressive mode on an interface.

Format

```
no udld port
```

Mode

```
Port Configuration Mode
```

73.1.4. udld port message

This command is used to configure the period of time between UDLD probe messages on a port that are in the advertisement phase and are determined to be bidirectional. <*7-90*> represents message interval value.

Default

```
7
```

Format

```
udld port message time-interval <7-90>
```

Mode

```
Port Configuration Mode
```

73.2. show

73.2.1. show udld

This command is used to display the UDLD status of the ports. <*port_type_list*> represents UDLD port.

Format

```
show udld [ interface <port_type_list> ]
```

Mode

```
User EXEC Mode
```

74. UPnP

UPnP (Universal Plug and Play) is used to automatically discover devices on the network so that devices can maintain a continuous and uninterrupted connection and communication.

74.1. upnp

74.1.1. upnp

This command is used to enable UPnP.

Default

```
disable
```

Format

```
upnp
```

Mode

```
Global Configuration Mode
```

■ no upnp

This command is used to disable UPnP.

Format

```
no upnp
```

Mode

```
Global Configuration Mode
```

74.1.2. upnp advertising-duration

This command is used to set advertising duration specified in seconds.

Default

```
100s
```

Format

```
upnp advertising-duration <100-86400>
```

Mode

```
Global Configuration Mode
```

■ no upnp advertising-duration

This command is used to set advertising duration to default value.

Format

```
no upnp advertising-duration
```

Mode

```
Global Configuration Mode
```

74.1.3. upnp ip-addressing-mode

This command is used to set IP addressing mode to dynamic or static.

Default

```
dynamic
```

Format

```
upnp ip-addressing-mode { dynamic | static }
```

Mode

```
Global Configuration Mode
```

■ no upnp ip-addressing-mode

This command is used to set IP addressing mode to default.

Format

```
no upnp ip-addressing-mode
```

Mode

```
Global Configuration Mode
```

74.1.4. upnp static interface vlan

This command is used to configure the VLAN interface ID during static addressing.

Default

```
1
```

Format

```
upnp static interface vlan <vlan_id>
```

Mode

```
Global Configuration Mode
```

■ no upnp static interface vlan

This command is used to configure the VLAN interface ID to default.

Format

```
no upnp static interface vlan
```

Mode

```
Global Configuration Mode
```

74.2. show

74.2.1. show upnp

This command is used to display UPnP configuration.

Format

```
show upnp
```

Mode

```
User EXEC Mode
```

75. Users

This module is primarily used to set up user accounts, levels, passwords, and password policy configurations, etc.

75.1. username

User management includes user name and privilege level configuration.

75.1.1. username privilege password none

This command configures user account, level and password. <*word31*> represents an account string with a length of no more than 31 characters. <*0-15*> represents an account level within the range of 0-15.<*line31*> represents a plaintext password with a length of no more than 31 characters.

Default

`none`

Format

`username <word31> privilege <0-15> password { unencrypted <line31> | none }`

Mode

`Global Configuration Mode`

no username

This command deletes the user account.

Format

`no username <word31>`

Mode

`Global Configuration Mode`

75.2. passwords

75.2.1. passwords min-length

This command configures the minimum character length in the switch user's password policy. <*1-31*> means the minimum length of the password setting is 1-31.

Default

`6`

Format

`passwords min-length <1-31>`

Mode

`Global Configuration Mode`

75.2.2. passwords min-lowercase-chars

This command configures the minimum number of lowercase letters to be included in the switch user's password policy. *<0-7>* means that the minimum number of lowercase letters in the password setting is 0-7.

Default

1

Format

passwords min-lowercase-chars *<0-7>*

Mode

Global Configuration Mode

75.2.3. passwords min-numeric-chars

This command configures the minimum number of digits to be included in the switch user's password policy. *<0-7>* means that the minimum number of digits in the password is 0-7.

Default

1

Format

passwords min-numeric-chars *<0-7>*

Mode

Global Configuration Mode

75.2.4. passwords min-special-chars

This command configures the minimum number of special characters included in the password policy of the switch user. *<0-7>* means that the minimum number of special characters in the password is 0-7.

Default

1

Format

passwords min-special-chars *<0-7>*

Mode

Global Configuration Mode

75.2.5. passwords min-uppercase-chars

This command configures the minimum number of uppercase letters to be included in the switch user's password policy. *<0-7>* means that the minimum number of uppercase letters in the password is 0-7.

Default

1

Format

passwords min-uppercase-chars *<0-7>*

Mode

Global Configuration Mode

75.2.6. passwords max-login-attempts

This command limits the number of attempts that each user can make to log in within a certain time. Whenever a user attempts to log in and fails, a log in failure will be recorded. If the number of consecutive failed login attempts within a specified time reaches the configured maximum number of login attempts, the user will be blocked from logging in. *<0-5>* means that the maximum limit for the number of failed logins within a specified time is 0-5.

Default

```
5
```

Format

```
passwords max-login-attempts <0-5>
```

Mode

```
Global Configuration Mode
```

75.2.7. passwords login-attempt-period

This command is used to limit the number of login attempts for the same IP address or username within a specified time period. If the number of consecutive failed login attempts reaches the configured maximum limit, the IP address or username will be automatically blocked, and the lockout duration will be set. *<0-60>* indicates that the lockout duration for the same IP address or username after a failed login is between 0 and 60 minutes.

Default

```
5
```

Format

```
passwords login-attempt-period <0-60>
```

Mode

```
Global Configuration Mode
```

75.3. users unlock

75.3.1. users unlock username

This command is used to unlock a user after exceeding the maximum number of login attempts. It can be used with administrator privileges to unlock a locked user.

Format

```
users unlock username <word31>
```

Mode

```
Global Configuration Mode
```

75.3.2. users unlock ip

This command is used to unlock a user after exceeding the maximum number of login attempts. It can be used with administrator privileges to unlock a locked user.

Format

```
users unlock ip { <ipv4_addr> | <ipv6_addr> }
```

Mode

```
Global Configuration Mode
```

75.4. show

75.4.1. show passwords

This command is used to view the configured password policy and print all the configuration parameters of the set password policy.

Format

```
show passwords
```

Mode

```
User EXEC Mode
```

76. VCL

VLAN Control List (VCL) is used for access control of VLAN members on a switch. Through VCL, administrators can allocate and manage access permissions to different VLANs, enabling control and restriction of communication between VLAN members. This feature allows administrators to define access policies, such as permitting or denying communication between specific VLAN members, applying access rules, and limiting data traffic, to enhance network security and management. VCL helps administrators implement fine-grained access control at the switch level to meet network security and business requirements.

76.1. switchport

76.1.1. switchport vlan mac

This command is used to add MAC-based VLAN configuration.

Default

```
none
```

Format

```
switchport vlan mac <mac_addr> vlan <vlan_id>
```

Mode

```
Port Configuration Mode
```

■ no switchport vlan mac

This command is used to remove MAC-based VLAN configuration.

Format

```
no switchport vlan mac <mac_addr> vlan <vlan_id>
```

Mode

```
Port Configuration Mode
```

76.1.2. switchport vlan protocol group

This command is used to set group name vlan mapping table.

Default

```
none
```

Format

```
switchport vlan protocol group <group_name> vlan <vlan_id>
```

Mode

```
Port Configuration Mode
```

■ no switchport vlan protocol group

This command is used to remove group name vlan mapping table.

Format

```
no switchport vlan protocol group <group_name> vlan <vlan_id>
```

Mode

```
Port Configuration Mode
```

76.1.3. switchport vlan ip-subnet

This command is used to set IP Subnet-based VLAN configuration.

Default

none

Format

switchport vlan ip-subnet [id *<1-128>*] *<ipv4_subnet>* vlan *<vid>*

Mode

Port Configuration Mode

■ no vlan ip-subnet

This command is used to remove IP Subnet-based VLAN configuration.

Format

no switchport vlan ip-subnet *<ipv4_subnet>*

Mode

Port Configuration Mode

76.1.4. switchport vlan mac enable

This command is used to enable MAC-based VLAN configuration.

Default

disable

Format

switchport vlan mac enable

Mode

Port Configuration Mode

■ no switchport vlan mac enable

This command is used to disable MAC-based VLAN configuration.

Format

no switchport vlan mac enable

Mode

Port Configuration Mode

76.1.5. switchport vlan ip-subnet enable

This command is used to enable IP Subnet-based VLAN configuration.

Default

disable

Format

switchport vlan ip-subnet enable

Mode

Port Configuration Mode

■ no switchport vlan ip-subnet enable

This command is used to disable IP Subnet-based VLAN configuration.

Format

```
no switchport vlan ip-subnet enable
```

Mode

```
Port Configuration Mode
```

76.1.6. switchport vlan protocol enable

This command is used to enable Protocol-based VLAN configuration.

Default

```
disable
```

Format

```
switchport vlan protocol enable
```

Mode

```
Port Configuration Mode
```

■ no switchport vlan protocol enable

This command is used to disable Protocol-based VLAN configuration.

Format

```
no switchport vlan protocol enable
```

Mode

```
Port Configuration Mode
```

76.2. vlan

76.2.1. vlan mac

This command is used to set MAC-based VLAN configuration.

Default

```
none
```

Format

```
vlan mac <mac_addr> vlan <vlan_id>
```

Mode

```
Global Configuration Mode
```

■ no vlan mac

This command is used to remove MAC-based VLAN configuration.

Format

```
no vlan mac <mac_addr> vlan <vlan_id>
```

Mode

```
Global Configuration Mode
```

76.2.2. vlan protocol

This command is used to set protocol group mapping table.

Default

none

Format

vlan protocol [Frame Type] <*value*> group <*group_name*>

Mode

Global Configuration Mode

■ no vlan protocol

This command is used to remove protocol group mapping table.

Format

no vlan protocol [Frame Type] <*value*> group <*group_name*>

Mode

Global Configuration Mode

76.2.3. vlan protocol group

This command is used to set group name vlan mapping table.

Default

none

Format

vlan protocol group <*group_name*> vlan <*vlan_id*>

Mode

Global Configuration Mode

■ no vlan protocol group

This command is used to remove group name vlan mapping table.

Format

no vlan protocol group <*group_name*> vlan <*vlan_id*>

Mode

Global Configuration Mode

76.2.4. vlan ip-subnet

This command is used to set IP Subnet-based VLAN configuration.

Default

none

Format

vlan ip-subnet <*ipv4_subnet*> vlan <*vid*>

Mode

Global Configuration Mode

no vlan ip-subnet

This command is used to remove IP Subnet-based VLAN configuration.

Format

```
no vlan ip-subnet <ipv4_subnet>
```

Mode

```
Global Configuration Mode
```

77. VLAN

VLAN (Virtual Local Area Network) is used to divide a network into multiple logically independent virtual LANs, providing better network management and security. VLAN allows different users or devices to be grouped into separate virtual networks, even if they are connected to the same physical switch, achieving logical isolation. This helps to reduce broadcast storms, enhance network security, and simplify network management and configuration.

77.1. flooding

77.1.1. flooding

This command is used to enable VLAN flooding.

Default

```
enable
```

Format

```
flooding
```

Mode

```
VLAN Configuration Mode
```

■ no flooding

This command is used to disable VLAN flooding.

Format

```
no flooding
```

Mode

```
VLAN Configuration Mode
```

77.2. switchport

77.2.1. switchport

This command is used to set port vlan. "access" represents configure a port to a VLAN, "hybrid native" represents configure a port VLAN ID for a hybrid port, "trunk native" represents configure a port VLAN ID for a trunk port.

Default

```
1
```

Format

```
switchport { access | hybrid native | trunk native } vlan <vlan_id>
```

Mode

```
Port Configuration Mode
```

■ no switchport

This command is used to delete port vlan.

Format

```
no switchport { access | hybrid native | trunk native } vlan
```

Mode

```
Port Configuration Mode
```

77.2.2. switchport mode

This command is used to set port mode. "access" represents set mode to ACCESS unconditionally, "hybrid" represents set mode to HYBRID unconditionally, "trunk " represents set mode to TRUNK unconditionally.

Default

```
access
```

Format

```
switchport mode { access | hybrid | trunk }
```

Mode

```
Port Configuration Mode
```

■ no switchport mode

This command is used to delete port mode.

Format

```
no switchport mode
```

Mode

```
Port Configuration Mode
```

77.2.3. switchport hybrid port-type

This command is used to set port type. "unaware" represents port in not aware of VLAN tags, "c-port" represents customer port, "s-port" represents provider port, "s-custom-port" represents custom provider port.

Default

```
c-port
```

Format

```
switchport hybrid port-type { unaware | c-port | s-port | s-custom-port }
```

Mode

```
Port Configuration Mode
```

■ no switchport hybrid port-type

This command is used to delete port type.

Format

```
no switchport hybrid port-type
```

Mode

```
Port Configuration Mode
```

77.2.4. switchport hybrid ingress-filtering

This command is used to set ingress filtering.

Default

```
disable
```

Format

```
switchport hybrid ingress-filtering
```

Mode

```
Port Configuration Mode
```

no switchport hybrid ingress-filtering

This command is used to disable ingress filtering.

Format

```
no switchport hybrid ingress-filtering
```

Mode

```
Port Configuration Mode
```

77.2.5. switchport hybrid acceptable-frame-type

This command is used to set hybrid ports allow for changing the type of frames that are accepted on ingress. "all" represents allow all frames, "tagged" represents allow only tagged frames, "untagged" represents allow only untagged frames.

Default

```
all
```

Format

```
switchport hybrid acceptable-frame-type { all | tagged | untagged }
```

Mode

```
Port Configuration Mode
```

no switchport hybrid acceptable-frame-type

This command is used to delete hybrid ports allow for changing the type of frames that are accepted on ingress.

Format

```
no switchport hybrid acceptable-frame-type
```

Mode

```
Port Configuration Mode
```

77.2.6. switchport hybrid egress-tag

This command is used to set ports in hybrid mode may control the tagging of frames on egress. "none" represents no egress tagging, "all" represents tag all frames, "except-native" represents tag all frames except frames classified to native VLAN of the hybrid port.

Default

```
all except-native
```

Format

```
switchport hybrid egress-tag { none | all [ except-native ] }
```

Mode

```
Port Configuration Mode
```

no switchport hybrid egress-tag

This command is used to set ports in hybrid mode delete the tagging of frames on egress.

Format

```
no switchport hybrid egress-tag
```

Mode

```
Port Configuration Mode
```

77.2.7. switchport allowed vlan

This command is used to set ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members. "all" represents all VLANs, "none " represents no VLANs, "add" represents add VLANs to the current list, "remove" represents remove VLANs from the current list, "except" represents all VLANs except the following.

Default

```
allowed vlan 1-4095
```

Format

```
switchport { trunk | hybrid } allowed vlan { all | none | [ add | remove | except ] <vlan_list> }
```

Mode

```
Port Configuration Mode
```

no switchport

This command is used to delete ports in Trunk and Hybrid mode delete which VLANs they are allowed to become members.

Format

```
no switchport { trunk | hybrid } allowed vlan
```

Mode

```
Port Configuration Mode
```

77.2.8. switchport forbidden vlan

This command is used to set a port to never be a member of one or more VLANs. "add" represents add to existing list, "remove" represents remove from existing list.

Default

```
none
```

Format

```
switchport forbidden vlan { add | remove }
```

Mode

```
Port Configuration Mode
```

no switchport forbidden vlan

This command is used to delete a port may be configured to never be a member of one or more VLANs.

Format

```
no switchport forbidden vlan
```

Mode

```
Port Configuration Mode
```

77.2.9. switchport trunk vlan tag native

This command is used to enable tag native VLAN.

Default

```
disable
```

Format

```
switchport trunk vlan tag native
```

Mode

```
Port Configuration Mode
```

no switchport trunk vlan tag native

This command is used to disable tag native VLAN.

Format

```
no switchport trunk vlan tag native
```

Mode

```
Port Configuration Mode
```

77.3. name

77.3.1. name

This command is used to set vlan name.

Default

```
VLAN <four-digit number>
Examples: VLAN0002, VLAN0010
```

Format

```
name <vword32>
```

Mode

```
VLAN Configuration Mode
```

no name

This command is used to delete vlan name.

Format

```
no name
```

Mode

```
VLAN Configuration Mode
```

77.4. vlan

77.4.1. vlan

This command is used to add vlan.

Default

```
vlan 1
```

Format

```
vlan <vlan_list>
```

Mode

```
Global Configuration Mode
```

no vlan

This command is used to delete vlan.

Format

```
no vlan <vlan_list>
```

Mode

```
Global Configuration Mode
```

77.4.2. vlan ethertype s-custom-port

This command is used to set ethertype for custom s-ports. *<0x8100,0x88a8,0x9100,0x9200>* represents EtherType.

Default

```
0x88a8
```

Format

```
vlan ethertype s-custom-port <0x8100,0x88a8,0x9100,0x9200>
```

Mode

```
Global Configuration Mode
```

no vlan ethertype s-custom-port

This command is used to delete ethertype for custom s-ports.

Format

```
no vlan ethertype s-custom-port
```

Mode

```
Global Configuration Mode
```

77.5. svl

77.5.1. svl fid

This command is used to set shared VLAN learning.

Default

```
none
```

Format

```
svl fid <1-4095> vlan <vlan_list>
```

Mode

```
Global Configuration Mode
```

no svl fid

This command is used to remove shared VLAN learning.

Format

```
no svl fid <1-4095>
```

Mode

```
Global Configuration Mode
```

77.6. show

77.6.1. show svl

This command is used to show svl configuration/status. "fid" represents a given FID, *<range_list>* represents list of FIDs to show.

Format

```
show svl { [ fid [ <range_list> ] ] | [ vlan [ <vlan_list> ] ] }
```

Mode

```
User EXEC Mode
```

77.6.2. show vlan

This command is used to show vlan status. "all" represents all VLANs (if left out only access VLANs are shown), "name <*vword32*>" represents VLAN status by VLAN name, "brief" represents VLAN summary information, "ip-subnet [<*ipv4_subnet*>] " represents VCL IP subnet entries, "mac [address <*mac_ucast*>] " represents a specific MAC entry, "protocol" represents protocol-based VLAN status, "eth2" represents ethernet protocol based VLAN status, "<*0x600-0xffff*>, arp, ip, ipx and at" represent ether type, "snap" represents SNAP-based VLAN status, "<*0x0-0xffffff*>, rfc-1042, snap-8021h" represent SNAP OUI, <*0x0-0xffff*> represents PID, "llc" represents LLC-based VLAN status, "<*0x0-0xff*>" represents DSAP and SSAP.

Format

```
show vlan [ all | id <vlan_list> | name <vword32> | brief | ip-subnet [ <ipv4_subnet> ] | mac [ address <mac_ucast> ] | protocol [ eth2 { <0x600-0xffff> | arp | ip | ipx | at } ] [ snap { <0x0-0xffffff> | rfc-1042 | snap-8021h } <0x0-0xffff> ] [ llc <0x0-0xff> <0x0-0xff> ] ]
```

Mode

```
User EXEC Mode
```

77.6.3. show vlan status

This command is used to show vlan status. "admin" represents the VLANs configured by administrator, "all" represents VLANs configured VLANs for all VLAN users, "combined" represents the combined set of configured VLANs, "conflicts" represents VLAN configurations that have conflicts, "erps" represents the VLANs configured by ERPS, "gvrp" represents the VLANs configured by GVRP, "mrp" represents the VLANs configured by MRP, "mstp" represents the VLANs configured by MSTP, "mvr" represents the VLANs configured by MVR, "nas" represents the VLANs configured by NAS, "rmirror" represents the VLANs configured by Remote mirroring, "vcl" represents the VLANs configured by VCL, "voice-vlan" represents the VLANs configured by Voice VLAN.

Format

```
show vlan status [ interface <port_type_list> ] [ admin | all | combined | conflicts | erps | gvrp | mrp | mstp | mvr | nas | rmirror | vcl | voice-vlan ]
```

Mode

```
User EXEC Mode
```

78. VLAN Translation

VLAN Translation allows network administrators to exchange and convert data between different VLANs. By using VLAN Translation, administrators can transfer data between different VLANs, thus achieving more flexible and efficient network management. This functionality is typically used for integrating or reorganizing network structures, as well as simplifying network configuration. VLAN Translation can help administrators address challenges related to network expansion, integration, and management, thereby enhancing the flexibility and manageability of the network.

78.1. switchport

78.1.1. switchport vlan mapping (port)

This command is used to set port to group configuration.

Default

```
none
```

Format

```
switchport vlan mapping <gid>
```

Mode

```
Port Configuration Mode
```

■ no switchport vlan mapping

This command is used to delete port to group configuration.

Format

```
no switchport vlan mapping
```

Mode

```
Port Configuration Mode
```

78.1.2. switchport vlan mapping (global)

This command is used to set VLAN translation mapping.

Default

```
none
```

Format

```
switchport vlan mapping <gid>
```

Mode

```
Global Configuration Mode
```

■ no switchport vlan mapping

This command is used to delete VLAN translation mapping.

Format

```
no switchport vlan mapping <gid>
```

Mode

```
Global Configuration Mode
```

79. Voice VLAN

Voice VLAN is a VLAN divided for user's voice data stream. By creating Voice VLAN and add the port connecting the voice device to Voice VLAN, it can be centralized to transmit voice data in Voice VLAN. It can provide targeted QoS configuration for voice stream. In this case, it will improve voice traffic transmission priority and ensure voice quality.

79.1. voice vlan

79.1.1. voice vlan

This command is used to globally enable voice vlan.

Default

```
disable
```

Format

```
voice vlan
```

Mode

```
Global Configuration Mode
```

■ no voice vlan

This command is used to globally disable voice vlan.

Format

```
no voice vlan
```

Mode

```
Global Configuration Mode
```

79.1.2. voice vlan vid

This command is used to configure the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. <*vlan_id*> represents VLAN ID, 1-4095.

Default

```
1000
```

Format

```
voice vlan vid <vlan_id>
```

Mode

```
Global Configuration Mode
```

■ no voice vlan vid

This command is used to restore the default Voice VLAN ID.

Format

```
no voice vlan vid
```

Mode

```
Global Configuration Mode
```

79.1.3. voice vlan aging-time

This command is used to configure the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval. <*10-10000000*> represents aging time.

Default

```
86400
```

Format

```
voice vlan aging-time <10-10000000>
```

Mode

```
Global Configuration Mode
```

■ no voice vlan aging-time

This command is used to restore the default voice vlan aging-time.

Format

```
no voice vlan aging-time
```

Mode

```
Global Configuration Mode
```

79.1.4. voice vlan class

This command is used to configure the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class. <*0-7*> represents traffic class value.

Default

```
7
```

Format

```
voice vlan class <0-7>
```

Mode

```
Global Configuration Mode
```

■ no voice vlan class

This command is used to restore the default Voice VLAN traffic class.

Format

```
no voice vlan class
```

Mode

```
Global Configuration Mode
```

79.1.5. voice vlan oui

This command is used to configure the oui entry for voice vlan. <*oui*> represents a telephony OUI address is a globally unique identifier assigned to a vendor by IEEE, it must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit). <*line32*> represents the description of OUI address, normally, it describes which vendor telephony device it belongs to, the allowed string length is 0 to 32.

Default

```
none
```

Format

```
voice vlan oui <oui> [ description <line32> ]
```

Mode

```
Global Configuration Mode
```

no voice vlan oui

This command is used to delete the oui entry. <*oui*> represents a telephony OUI address is a globally unique identifier assigned to a vendor by IEEE.

Format

```
no voice vlan oui <oui>
```

Mode

```
Global Configuration Mode
```

79.2. switchport voice vlan

79.2.1. switchport voice vlan mode

This command is used to configure Voice VLAN port mode. "auto" is enable auto detect mode, it detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically. "force" is force join to Voice VLAN. "disable" is disjoin from Voice VLAN.

Default

```
disable
```

Format

```
switchport voice vlan mode { auto | force | disable }
```

Mode

```
Port Configuration Mode
```

no switchport voice vlan mode

This command is used to restore the default Voice VLAN port mode.

Format

```
no switchport voice vlan mode
```

Mode

```
Port Configuration Mode
```

79.2.2. switchport voice vlan security

This command is used to enable the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds.

Default

```
disable
```

Format

```
switchport voice vlan security
```

Mode

```
Port Configuration Mode
```

no switchport voice vlan security

This command is used to disable the Voice VLAN port security mode.

Format

```
no switchport voice vlan security
```

Mode

```
Port Configuration Mode
```

79.2.3. switchport voice vlan discovery-protocol

This command is used to configure the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "lldp" or "both". Changing the discovery protocol to "oui" or "lldp" will restart auto detect process. "oui" is detect telephony device by OUI address. "lldp" is detect telephony device by LLDP. "both" is both OUI and LLDP.

Default

```
oui
```

Format

```
switchport voice vlan discovery-protocol { oui | lldp | both }
```

Mode

```
Port Configuration Mode
```

no switchport voice vlan discovery-protocol

This command is used to restore the default Voice VLAN port discovery protocol.

Format

```
no switchport voice vlan discovery-protocol
```

Mode

```
Port Configuration Mode
```

79.3. show

79.3.1. show voice vlan interface

This command is used to display voice VLAN configuration without keywords. Use interface keyword to display particularly switchport configuration for the interface. *<port_type_list>* represents ports.

Format

```
show voice vlan [ interface <port_type_list> ]
```

Mode

```
User EXEC Mode
```

79.3.2. show voice vlan oui

This command is used to display voice VLAN configuration without any keywords. Use oui keyword to display oui configuration. *<oui>* represents oui value.

Format

```
show voice vlan [ oui [ <oui> ] ]
```

Mode

```
User EXEC Mode
```

80. VRRP

This chapter provides a detailed explanation of the Virtual Router Redundancy Protocol (VRRP) commands. The commands are divided by functionality into the following different groups:

- Show commands are used to display switch settings, statistics and other information.
- Configuration Commands are used to configure features and options of the switch. Each configuration command can be viewed in the show running-config or the show vrrp command.

80.1. vrrp

80.1.1. vrrp associate

This command is used to configure the virtual IP address for VRRP. <*vrid*> is the virtual routing switch ID, ranging from 1 to 255. The virtual IP address must be on the same network segment as the port IP address, otherwise the virtual routing switch will not function. When the virtual IP address is the same as the port IP address, the system will automatically raise the routing switch priority to 255. The virtual routing switch can be configured with one virtual IP address.

Default

```
none
```

Format

```
vrrp <vrid> associate <virtual-address>
```

Mode

```
VLAN Interface Mode
```

no vrrp

Associate is an optional keyword. The no vrrp <*vrid*> command is used to delete VRRP groups, while the no vrrp <*vrid*> associate command is used to delete the virtual IP address of VRRP. <*vrid*> is the virtual routing switch ID, ranging from 1 to 255.

Format

```
no vrrp <vrid> [ associate ]
```

Mode

```
VLAN Interface Mode
```

80.1.2. vrrp description

This command configures the description information for VRRP, the range of <*vrid*> is 1 to 255, and <*WORD*> is the description string, Spaces are illegal characters and cannot exceed 64 characters in length.

Default

```
none
```

Format

```
vrrp <vrid> description <WORD>
```

Mode

```
VLAN Interface Mode
```

no vrrp description

This command restores the default description information, which is blank. The range of <*vrid*> is 1 to 255.

Format

```
no vrrp <vrid> description
```

Mode

```
VLAN Interface Mode
```

80.1.3. vrrp preempt

This command configures the priority preemption mode of VRRP. The range of <*vrid*> is 1 to 255.

Default

```
enable
```

Format

```
vrrp <vrid> preempt
```

Mode

```
VLAN Interface Mode
```

no vrrp preempt

This command turns off the priority preemption mode of VRRP. The range of <*vrid*> is 1 to 255.

Format

```
no vrrp <vrid> preempt
```

Mode

```
VLAN Interface Mode
```

80.1.4. vrrp preempt delay

This command configures the priority of VRRP preemption delay time. The range of <*vrid*> is 1 to 255, The range of <*second*> is 0-255.

Default

```
0
```

Format

```
vrrp <vrid> preempt delay <second>
```

Mode

```
VLAN Interface Mode
```

no vrrp preempt delay

This command restores the priority preemption delay time of VRRP to the default value of 0. The range of <*vrid*> is 1 to 255.

Format

```
no vrrp <vrid> preempt delay
```

Mode

```
VLAN Interface Mode
```

80.1.5. vrrp priority

This command sets the priority value for the virtual router configured on a specified interface. The priority of the interface is a priority integer from 1 to 254 and defaults to 100. The parameter <*vrid*> is the virtual router ID which has an integer value ranging from 1 to 255. When interface IP is the same as the virtual IP, priority takes precedence to 255, indicating the IP address owner. This value can be configured, but the configured value does not work.
The priority of a virtual router cannot be set to a value lower than the sum of the decrement values of all tracking entries for that virtual router.

Default

```
100
```

Format

```
vrrp <vrid> priority <value>
```

Mode

```
VLAN Interface Mode
```

no vrrp priority

This command sets the default priority value for the virtual router configured on a specified interface.

Format

```
no vrrp <vrid> priority
```

Mode

```
VLAN Interface Mode
```

80.1.6. vrrp timers

This command is used to configure the advertise clock of the VRRP <*second*> is the Advertise clock value, which is measured in seconds and has a value range of 1 to 255. The clock value determines the shortest time for the virtual routing switch to recover from the failure. When the master routing switch goes down, the backup routing switch will recover within 3 * advertise + skew_delta The advertise clock interval after which the switch will transition to the master route. The advertised time interval is too long, which is obviously not conducive to fault recovery. It is recommended to use the default value.

Default

```
1
```

Format

```
vrrp <vrid> timers advertise <second>
```

Mode

```
VLAN Interface Mode
```

no vrrp timers

This command restores the Advertise clock value to the default value of 1 second.

Format

```
no vrrp <vrid> timers advertise
```

Mode

```
VLAN Interface Mode
```

80.1.7. vrrp authentication

This command configures the port VRRP to use the simple-text authentication method, with a value range of 1 to 255 for <*vrid*> and an 8-character authentication string for <*WORD*>. A data message received by a VRRP group is considered valid only if it matches the configured authentication string. When configuring, it is important to note that if different authentication strings appear within a group, it will result in multiple masters coexisting. This function is only available for IPv4 VRRP groups.

Default

```
none
```

Format

```
vrrp <vrid> authentication <WORD>
```

Mode

```
VLAN Interface Mode
```

no vrrp authentication

This command restores the authentication string to its default value, which is empty and does not require authentication.

Format

```
no vrrp <vrid> authentication
```

Mode

```
VLAN Interface Mode
```

80.1.8. vrrp enable

This command is used to enable/disable the VRRP instance.

Default

```
enable
```

Format

```
vrrp <vrid> { enable | disable }
```

Mode

```
VLAN Interface Mode
```

80.1.9. vrrp ping enable

This command is used to enable/disable the ping to virtual IP address of the VRRP group.

Default

```
enable
```

Format

```
vrrp <vrid> ping { enable | disable }
```

Mode

```
VLAN Interface Mode
```

80.1.10. vrrp track

This command is used to configure a virtual router as a monitored object. Configure the object to be monitored and priority penalty value using the "track" command. The value range of <*vrid*> is from 1 to 255, the parameter <*cword*> is the track instances name, and <value> is the priority penalty value, which ranges from 1 to 254. The configured penalty value must not be greater than the priority of the current VRRP group.

Default

none

Format

vrrp <*vrid*> track <*cword*> decrement <*value*>

Mode

VLAN Interface Mode

no vrrp track

This command is used to cancel the monitoring function.

Format

no vrrp <*vrid*> track <*cword*>

Mode

VLAN Interface Mode

80.2. show

80.2.1. show vrrp

This command displays the information of the VRRP routing group, including brief and detailed information.

80.2.2. show vrrp brief

This command displays brief information on the VRRP group, where the interface <*intf-id*> is an optional parameter. When present, the command displays a specific physical interface's brief information, while not present, it displays brief information for all configured interfaces.

Format

show vrrp [interface <*intf-id*>] brief

Mode

User EXEC Mode

80.2.3. show vrrp detail

This command displays the detailed information of VRRP. The interface <*intf-id*> and *vrid* are optional parameters. When both parameters are present, the detailed information of a specific physical port and group is displayed. When only the interface <*intf-id*> parameter is present, the detailed information of a specific physical port is displayed. When neither of the two parameters is present, the detailed information of all configured physical ports and groups is displayed. Where *vrid* ranges from 1 to 255.

Format

show vrrp [interface <*intf-id*> [*vrid*]] detail

Mode

User EXEC Mode

80.2.4. show vrrp statistics

This command can view the statistical information of the VRRP group configured for a specific physical port on the switch. The parameter <*intf-id*> is the specific physical port, and the parameter <*vrid*> is the switch ID, with a value range of 1 to 255.

Format

```
show vrrp interface <intf-id> <vrid> statistics
```

Mode

```
User EXEC Mode
```

80.3. clear

80.3.1. clear vrrp statistics

This command clears the statistical information for the VRRP group configured on a physical port on the switch to null. The parameter <*intf-id*> is the specific physical port, and the parameter <*vrid*> is the switch ID, with a value range of 1 to 255.

Format

```
clear vrrp interface vlan <intf-id> <vrid> statistics
```

Mode

```
User EXEC Mode
```

A Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

B Technical Support

Technical Questions

For technical questions, please contact any dealer in your area or our company directly.
You will find the addresses of our partners on the Internet.
A list of local telephone numbers and email addresses for technical support directly from the company is available on the Internet.
This site also includes a free of charge knowledge base and a software download section.

Technical Documents

The current manuals and operating instructions for the company's products are available on the Internet.