NRS-8-24-48 managed Switch
CLI User Manual

CHAPTER 1. INTRODUCTION 6
1.1 Console Port Connection 6
1.2 RJ-45pin Assignment 6
1.3 CONSOLE 6
CHAPTER 2. INTRODUCTION TO CLI 6
2.1 General Introduction 6
2.2 CONSOLE Operation 6
2.3 CLI Modes 7
2.4 Quick Keys 7
2.5 Command Syntax 7
2.6 Basic Configurations 8
2.6.1 Configuring IPv4 Address 8
2.6.2 Enter Config InterfaceMode 8
2.6.3 Save Configurations 9
2.6.4 Restart the Device 9
2.6.5 Load Factory Defaults 9
2.6.6 Show System and Software Information 9
2.6.7 Show Running Configurations 11
2.6.8 Show History Commands 11
2.6.9 Help 12
2.6.10 Logout 12
2.7 Commands in User Mode 12

2.7.1> clear iparp 12
2.7.2> clear lldp statistics 12
2.7.3> clear statistics 13

2.7.4> enable 13
2.7.5> exit 13
2.7.6> help 13
2.7.7> logout 13
2.7.8> ping ip 13
2.7.9> ping ipv6 13
2.7.10 show commands 14
2.8 Commands in EXEC Mode 14
2.8.1 # clear access management statistics 14
2.8.2 # clear access-list ace statistics 14
2.8.3 # clear dot1xstatistics 14
2.8.4 # clear erps 14
2.8.5 # clear iparp 14
2.8.6 # clear ip dhcp detailed statistics 15
2.8.7 # clear ip dhcp relay statistics 15
2.8.8 # clear ip dhcp snooping statistics 15
2.8.9 # clear ip igmp snooping 15
2.8.10 # clear ip statistics 15
2.8.11 # clear ipv6 mld snooping 15
2.8.12 # clear ipv6neighbors 15
2.8.13 # clear ipv6 statistics 15
2.8.14 # clear lacp statistics 16
2.8.15 # clear lldp statistics 16
2.8.16 # clear logging 16
2.8.17 # clear macaddress-table 16
2.8.18 # clear mep 16
2.8.19 # clear spanning-tree 16
2.8.20 # clear statistics 16
2.8.21 # config terminal 16
2.8.22 # copy 17

2.8.23 # delete 17
2.8.24 # dir 18
2.8.26 # dot1x 18
2.8.27 # erps 18
2.8.25 # disable & # enable 18
2.8.28 # firmware swap 19
2.8.29 # firmware upgrade 19
2.8.30 # ip dhcp retry interface vlan 19
2.8.31 # more 19
2.8.32 # ping ip 19
2.8.33 # ping ipv6 19
2.8.34 # reload cold 20
2.8.35 # reload defaults 20
2.8.36 # send 20
2.8.37 # terminal editing 21
2.8.38 # terminal exec-timeout 21
2.8.39 # terminal history size 21
2.8.40 # terminal length 21
2.8.41 # terminal width 22
2.8.42 # no port-security shutdown 22
2.8.43 show commands 22
2.9 Commands in Config Mode 22
2.9.1 (config)# aaa authenticationlogin 22
2.9.2 (config)# access management 23
2.9.3 (config)# access-list 23
2.9.4 (config)# aggregation 27
2.9.5 (config)# banner 28
2.9.6 (config)# clock 28
2.9.7 (config)# default access-list rate-limiter 30
2.9.8 (config)# dot1x 30

2.9.9 (config-if)# duplex 35
2.9.10 (config)# enable 36
2.9.11 (config)# erps 37
2.9.12 (config-if)# excessive-restart 40
2.9.13 (config-if)# flowcontrol { on | off } 40
2.9.14 (config)# green-ethernet 41
2.9.15 (config)# gvrp 43
2.9.16 (config)# hostname 44
2.9.17 (config)# interface 44
2.9.18 (config)# ip 45
2.9.19 (config)# ipmc 60
2.9.20 (config)# ipv6 mldhost-proxy 62
2.9.21(config)# lacp 66
2.9.22 (config)# line 68
2.9.23 (config)# lldp 73
2.9.24 (config)# logging 80
2.9.25 (config)# loop-protect 81
2.9.26 (config)# mac 83
2.9.27 (config-if)# media-type 84
2.9.28 (config-if)# mtu 85
2.9.29 (config)# mep 85
2.9.30 (config)# monitor 93
2.9.31 (config)# ntp 94
2.9.32 (config)#poe(ForPoEModelsOnly) 95
2.9.33 (config)# port-security 96
2.9.34 (config)# privilege 98
2.9.35 (config)# qos 99
2.9.36 (config)# radius-server 110
2.9.37 (config)# rmon 113
2.9.38 (config)# spanning-tree 115

2.9.39 (config-if)# speed 124
2.9.40 (config)# switchport 125
2.9.41 (config)# tacacs-server 131
2.9.42 (config)# upnp 132
2.9.43 (config)# username 133
2.9.44 (config)# vlan 135
2.9.45 (config)# web privilegegroup 136

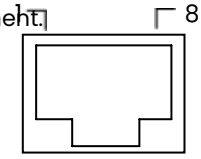
CHAPTER 1. INTRODUCTION

1.1 Console Port Connection

Managed Gigabit Ethernet Switch Series have an asynchronous terminal console port for local management via a serial terminal. The terminal provides management via a CLI (Command Line Interface) which will be familiar to many networking engineers. For most users, the CLI can be used to initially configure TCP/IP access so that further configuration can be completed via the GUI (Graphical User Interface) and any web browser.

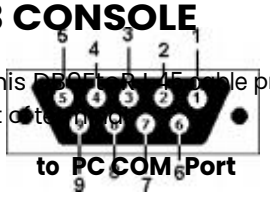
1.2 RJ-45pin Assignment

This RJ-45 connectorprovidesan RS-232DCE(datacommunicationequipment)asynchronousserialconnection for local management.



Pin	Ref.	Definition	Direction
3	RxD	Receive Data	Out towards DTE
6	TxD	Transmit Data	In from DTE
5	SG	Signal Ground	na

1.3 CONSOLE



This DB9F to RJ-45 cable provides a connection forthe RS-232. This cable is used between this device and the serial port of the PC.

Pins		Ref.	Definition	Direction
DB9	RJ-45			
2	3	RxD	Receive Data	Out thedevicetowards DTE
3	6	TxD	Transmit Data	In the device from DTE
5	5	SG	Signal Ground	na

CHAPTER 2. INTRODUCTION TO CLI

2.1 General Introduction

This device provides a number of configuration/management methods. The first and very basic is serial console access. This method is also called out-of-band management and is only available when a terminal or administrator PC can be physically connected to the local switch at the CONSOLE port using RJ45 to RS-232 console cable. Accessing the switch via CONSOLE port allows the user to use Command Line Interface (CLI) to manage and configure the device. The out-of-band management is relatively useful when you lose the network connection to the device.

The out-of-band management via console access, using a command line (CLI), is familiar to most network engineers. For engineers that are not comfortable using CLI, this device can also be managed using any standard Web Browser in a more user friendly 'point-and-click' method. Therefore, in most configuration scenarios, the console will only be used to initially configure the IP address, so that the device may be accessed via the other methods which require working TCP/IP.

After the device has been properly configured for the application and placed into service, a third method of configuration/management can be employed using Simple Network Management Protocol (SNMP). The operator will use SNMP management software to manage and monitor the switches on a network. This requires some configuration of the device to allow SNMP management. In addition, the network management platform will need to import and compile the proprietary MIB (management information base) file so that the manager knows "how" to manage the devices.

2.2 CONSOLE Operation

Using the provided accessory cable, connect the "CONSOLE" port (RJ-45) to the PC terminal communications port (DB9). Run any terminal emulation program (Hyper Terminal, PuTTY, TeraTerm Pro, etc.) and configure the

communication parameters as follows:

Speed: 115,200

Data: 8 bits Parity:

none Stop bits: 1

Flow Control: None

From a cold start, the following screen will be displayed. At the "Username" prompt, **enter 'admin' and the password 'admin'**.

```
+Luton10 board detected (8539 Rev. D).
--Welcome to use our system
--Software version V2.00
== Executing boot scipt in 1.000 seconds - enter ^C to abort
RedBoot> fis load -d managed
Image loaded from 0x80040000-0x81016178
RedBoot> go
Press ENTER to get started
Username: admin
Password:
```

2.3 CLI Modes

The Command Line Interface (CLI) is mainly divided into four basic modes; these are User mode, EXEC mode, Config mode and Config Interface mode. After entering the username and password, you start from the Exec mode (prompted with "#"). The commands available in User mode and EXEC mode are limited. For more advanced configurations, you must enter Config mode or Config Interface mode. In each mode, a question mark (?) at the system prompt can be issued to obtain a list of commands available for each command mode. The following table provides a brief overview of modes available in this device.

Mode	Prompt	Enter Method	Exit Method
User mode	>	enable	disable
EXEC mode	#	Enter authorized username and password	Exit, logout
Global Config Mode	(config)#	Enter "configure terminal" after "#"	End, exit, do logout
Config Interface Mode	(config-if)#	Specify interface, interface type and number after (config)#	End, exit, do logout

2.4 Quick Keys

There are several useful quick keys you can use when editing command lines.

Keyboard	Action
?	Issue "?" to get a list of commands available in the current mode.
Up arrow key	To view the previous entered commands.
Down arrow key	To view the previous entered commands.
Tab key	To complete an unfinished command.

2.5 Command Syntax

Commands introduced in this user manual are written using the coherent symbols and easy-to-understand syntax and style. Although users can issue Help command to complete a desired command in CLI, it is useful to understand frequently-used symbols and syntax conventions. The following table lists the syntax conventions used in this user manual together with an example.

2.5.1 Example: (config-if-vlan)# ip address { { <address> <netmask> } |{ dhcp [fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]] } }

Symbol	Function	Example	Explanation
< > (Angle bracket)	Enter a value, alphanumeric strings or keywords.	<address> <netmask>	Enter IPaddress and subnet mask.
[ ] (Square bracket)	This is an optional parameter.	[fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]]	Fallback parameterisan optional item .
{ } (Curly bracket)	A curly bracket has the following two functions: 1. If there are more than two options available,a curly bracket can be used to separate them. 2. The uter curly bracket means that this is a must parameter.At leasetone valueshould bespecified.	{ { <address> <netmask> } | { dhcp [fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]] } }	At leastspecifyone option to complete thecommand.
| (Vertical bar)	Use avertical bar to separate options.	{ { <address> <netmask> } | { dhcp [fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]] } }	Enter IPaddress or use DHCP to assign IP address automatically.

2.6 Basic Configurations

This section introduces users how to change the default IP address to the desired one and save the current running configurations to startup configurations. For detailed introductions to commands, please see section 3.7, 3.8, 3.9.

2.6.1 Configuring IPv4 Address

IP address: 192.0.3.254

Subnet mask: 255.255.255.0

Enter Port 3 ' s Config Interface mode.

```
# config terminal
(config)# interface GigabitEthernet 1/3
(config-if)#
```

Note: 1/3 means Ethernet Interface 1, Port 3.

```
# config terminal
(config)# interface vlan 1
(config-if-vlan)# ip address 192.0.3.254 255.255.255.0
(config-if-vlan)# exit
(config)# exit
# show ip interface brief
Vlan Address Method Status
1 192.0.3.254/24 Manual DOWN
```

2.6.2 Enter Config InterfaceMode

```
# config terminal
(config)# interface GigabitEthernet 1/1-3
(config-if)#
```

Note: 1/1-3 means Ethernet Interface 1, Port 1 to Port 3.

```
Enter Port 1~3 & Port 5's Config Interface mode.
# config terminal
(config)# interface GigabitEthernet 1/1-3,5
(config-if)#
```

Note: 1/1-3,5 means Ethernet Interface 1, Port 1 to Port 3 and Port 5.

2.6.3 Save Configurations

```
Building configuration...
% Saving 1520 bytes to flash:startup-config
#
```

2.6.4 Restart the Device

```
# reload cold
% Cold reload in progress, please standby.
#
 +Luton10 board detected (8539 Rev. D).
--Welcome to use our system
--Software version V2.00
== Executing boot script in 1.000 seconds - enter ^C to abort
RedBoot> fis load -d managed
Image loaded from 0x80040000-0x810156c8
RedBoot> go
Press ENTER to get started
```

2.6.5 Load Factory Defaults

Load factory default settings

```
# reload defaults
% Reloading defaults. Please standby.
```

Load factory defaults but keep IP settings

```
# reload defaults keep-ip

% Reloading defaults, attempting to keep IP address. Please standby.
```

2.6.6 Show System and Software Information

```
# show version
MEMORY          : Total=87066 KBytes, Free=73379 KBytes, Max=73286 KBytes
FLASH           : 0x40000000-0x40ffffff, 256 x 0x10000 blocks
MAC Address     : 00-02-c1-93-9a-35
Previous Restart : Cold
System Contact  :
System Name     :
System Location :
System Time     : 06-06-2019T02:04:31-10:00
System Uptime   : 00:03:33
Active Image
Image           : ce_switch_caracal1_l10_ref.dat (primary)
Version         : CEServicesCEServices---V1.00
Date            : 09-2019
Alternate Image
Image           : ce_switch_caracal1_l10_ref.dat (backup)
Version         : CEServicesCEServices---V1.00
Date            : 09-2019
----------
Bootloader
Image           : RedBoot (bootloader)
Version         : version 1_20-Vitesse
Date            : 12:02:42, Aug 19 2019
```

2.6.7 Show Running Configurations

```
# show running-config
Building configuration...
username admin privilege 15 password encrypted YWRtaW4=
!
vlan 1
!
!
!
!
clock timezone sz1111 -10
spanning-tree mst name 02-00-c1-93-4a-01 revision 0
poe management mode allocation-reserved-power
voice vlan oui 00-01-E3 description Siemens AG phones
voice vlan oui 00-03-6B description Cisco phones
voice vlan oui 00-0F-E2 description H3C phones
voice vlan oui 00-60-B9 description Philips and NEC AG phones
voice vlan oui 00-D0-1E description Pingtel phones
voice vlan oui 00-E0-75 description Polycom phones
voice vlan oui 00-E0-BB description 3Com phones
!
interface GigabitEthernet 1/1
 poe mode plus
 poe power limit 90.0
 poe delay limit 1.3
!
interface GigabitEthernet 1/2
 poe mode plus
 poe power limit 90.0
 poe delay limit 1.2
!
interface GigabitEthernet 1/3
 poe mode plus
 poe power limit 50.0
 poe delay limit 1.1
!
```

2.6.8 Show History Commands

```
# show history
 config t
 exit
 config t
 ip arp ex
 exit
```

```
> show history
 config t
 interface GigabitEthernet 1/3
 exit
 interface GigabitEthernet1/1-5
 exit
 interface GigabitEthernet 1/1-3,5,7
 flowcontrol on
 exit
 showinterface*status
 disable
 show clock detail
 show dot1x
 show history
```

2.6.9 Help

Help command can be issued in User, Exec, and Global Config mode to get a hint message describing how to use "show" command to get help from CLI.

```
# help

    Help may be requested at any point in a command by entering a question mark '?'. If nothing
    matches, the help list will be empty and you must backup until entering a '?' shows the available
    options.

Two styles of help are provided:

    Full help is available when you are ready to enter a command argument (e.g. 'show ?')
    and describes each possible argument.Partial help is provided when an abbreviated
    argument is entered and you want to know what arguments match the input (e.g. 'show pr?'.)
```

2.6.10 Logout

To close an active terminal session, issue the "logout" command in User or EXEC mode.

```
(config)# exit

# logout

Press ENTER to get started
```

```
# disable

> logout

Press ENTER to get started
```

2.7 Commands in User Mode

When you successfully login in Command Line Interface, you are in Exec Mode (prompted with "#"). To enter User mode, issue "disable" command after # prompt. Then you will be directed to User mode with ">" prompt.

```
Username: admin

Password:admin

#

# disable

>
```

In User mode, only limited commands are available. These commands are used for clearing statistics, entering Exec mode and pinging the specified destination. To configure a function, you should enter Config mode or Config Interface mode.

2.7.1> clear iparp

Syntax: > clear ip arp

Explanation: Clear ARP cache.

2.7.2> clear lldpstatistics

Syntax: > clear lldp statistics

Explanation: Clear LLDP statistics.

2.7.3> clear statistics

Syntax: > clear statistics {[interface] (<port_type> [<v_port_type_list>])}

<port_type>: Specify the interface type.

[<v_port_type_list>: Specify the ports that you want to clear.

Explanation: Clear statistics of the specified interfaces.

Syntax: > enable [<new_priv>]

2.7.4> enable

[<new_priv: 0-15>]: Choose a privilege level.

Explanation: Enter the Exec mode.

2.7.5> exit

Syntax: > exit

Explanation: Return to the previous mode. Issuing this command in User mode will logout the Command Line Interface.

2.7.6> help

Syntax: > help

Explanation: Provide help messages.

2.7.7> logout

Syntax: > logout

Explanation: Logout the Command Line Interface.

2.7.8> ping ip

Syntax: > ping ip <v_ip_addr> [repeat <count>] [size <size>] [interval <seconds>]

<v_ip_addr>: Specify IPv4 address that you want to ping.

[repeat <count>]: The number of packets that are sent to the destination IP or host. [size <size>]: The size of the packet.

[interval <seconds>]: Timeout interval. The ping test is successful only when it receives echo reply from the destination IP or host within the time specified here.

Explanation: To carry out ping tests on the specified destination IPv4 address or host.

2.7.9> ping ipv6

Syntax: > ping ipv6 <v_ipv6_addr> [repeat <count>] [size <size>] [interval <seconds>]

<v_ipv6_addr>: Specify IPv6 address that you want to ping.

[repeat <count>]:The number of packets that are sent to the destination IP or host. [size <size>]: The size of the ping packet.

[interval <seconds>]: Timeout interval. The ping test is successful only when it receives echo reply from the destination IP or host within the time specified here.

Explanation: To carry out ping tests on the specified destination IPv6 address or host.

2.7.10 show commands

In User mode, "show" commands can be issued to display current status or settings of a certain command. They will be introduced in Section 3.9 "Commands in Config Mode".

2.8 Commands in EXEC Mode

2.8.1 # clear access management statistics

Syntax: # clear access management statistics

Explanation: Clear access (HTTaP, HTTPs, SNMP, Telnet, SSH) management statistics.

2.8.2 # clear access-list ace statistics

Syntax: # clear access-list ace statistics

Explanation: Clear access list entry statistics.

2.8.3 # clear dot1xstatistics

Syntax: # clear dot1x statistics [interface (<port_type> [<v_port_type_list>])]

Parameter:

[interface (<port_type> [<v_port_type_list>])]: Specify the interface that you want to clear.

Explanation: Clear (the specified interfaces') dot1x statistics.

2.8.4 # clearerps

Syntax: # clear erps [<groups>] statistics

Parameter:

[<groups>]: Specify the ERPS group that you want to clear.

Explanation: Clear (the specified group ' s) ERPS statistics.

2.8.5 # clear ip arp

Syntax: # clear ip arp

Explanation: Clear ARP cache.

2.8.6 # clear ip dhcp detailed statistics

Syntax: # clear ip dhcp detailed statistics { server | client | snooping | relay | helper | all } [interface (<port_type> [<in_port_list>])]

Explanation: ClearIP DHCP statistics.

Parameter:

{ server | client | snooping | relay | helper | all }: Specify the type of information that you want to clear.
[interface (<port_type> [<in_port_list>])]: Specify the interface type and port number.

2.8.7 # clear ip dhcp relay statistics

Syntax: # clear ip dhcp relay statistics

Explanation: Clear IP DHCP Relay statistics.

2.8.8 # clear ip dhcp snooping statistics

Syntax: # clear ip dhcp snooping statistics [interface (<port_type> [<in_port_list>])]

Explanation: Clear IP DHCP Snooping statistics.

2.8.9 # clear ip igmp snooping

Syntax: # clear ip igmp snooping [vlan <v_vlan_list>] statistics

Explanation: Clear IP IGMP Snooping statistics.

2.8.10 # clear ip statistics

Syntax: # clear ip statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]

Explanation: Clear IPv4 statistics for system, interface and ICMP.

2.8.11 # clear ipv6 mld snooping

Syntax: # clear ipv6 mld snooping [vlan <v_vlan_list>] statistics

Explanation: Clear statistics for IPv6 MLD Snooping.

2.8.12 # clear ipv6 neighbors

Syntax: # clear ipv6 neighbors

Explanation: Clear the table for IPv6 neighbors.

2.8.13 # clear ipv6 statistics

Syntax: # clear ipv6 statistics [system] [interface vlan <v_vlan_list>] [icmp] [icmp-msg <type>]

Explanation: Clear IPv6 statistics for system, interface and ICMP.

2.8.14 # clear lacp statistics

Syntax: # clear lacp statistics

Explanation: Clear LACP statistics.

2.8.15 # clear lldp statistics

Syntax: # clear lldp statistics

Explanation: Clear LLDP statistics.

2.8.16 # clearlogging

Syntax: # clear logging [info] [warning] [error] [switch <switch_list>]

Explanation: Clear specific syslog events.

2.8.17 # clear macaddress-table

Syntax: # clear mac address-table

Explanation: Clear MAC address table.

2.8.18 # clearmep

Syntax: # clear mep <inst> { lm | dm | tst }

Explanation: Clear a specific instance MEP information.

2.8.19 # clearspanning-tree

Syntax: #clear spanning-tree{{statistics[interface(<port_type>[<v_port_type_list>])]}|{detected-protocols [interface (<port_type> [<v_port_type_list_1>])] } }

Explanation: Clear specific interfaces' Spanning Tree statistics.

2.8.20 # clear statistics

Syntax: # clear statistics [interface] (<port_type> [<v_port_type_list>])

Explanation: Clear Fast Ethernet and/or Gigabit Ethernet interfaces' statistics.

2.8.21 # config terminal

Syntax: # config terminal

Explanation: Enter the Global Config mode.

```
# config t
(config)#
```

2.8.22 # copy

Syntax: # copy { startup-config | running-config | <source_path> } { startup-config | running-config | <destination_path> } [syntax-check]

{ startup-config |running-config| <source_path>}:Specify the file type that you want to copy from. This can be "startup-config", "running-config" or a specific source file in flash or TFTP server.

{ startup-config |running-config |<destination_path>}: Specify the file type that you want to copy to. This can be "startup-config", "running-config" or a specific destination file in flash or TFTP server.

Explanation: Save running configurations to startup configurations.

runningconfigurations to startupconfiguratio

```
# copy  running-config startup-config
Building configuration...

% Saving 1596  bytes to flash:startup-config
#
```

Explanation: Save startup configurations to running configurations.

runningconfigurations to startupconfigurations

```
# copy  startup-config running-config
Building configuration...

% Saving 1596  bytes to flash:startup-config
#
```

Explanation: Save running configurations to Flash 201

```
# copy running-config Flash:201
Building configuration...

% Saving 1487 bytes to flash:201
# dir

Directory of flash:

    r- 01-01-1970 00:00:00       284
                                      default-config
    rw 01-01-1970 01:56:32      1487
                                      startup-config
    rw 01-01-2015 01:56:49      1487
                                      201
3 files, 3258 bytes total.
```

2.8.23 # delete

Syntax: # delete <path>

Explanation: Delete a file saved in Flash.

Parameters:

```
# dir
Directory of flash:

     r- 01-01-1970 00:00:00       284 default-config
     rw 01-01-1970 01:56:32
     rw 01-01-1970 01:56:49      1487 startup-config
                                 1487 201
3 files, 3258 bytes total.

# delete flash:201
```

<Path : word>: Name of the file in Flash to be deleted.

Example: Delete a file named 201 in Flash.

```
# dir
Directory of flash:
    r-  01-01-1970 00:00:00       284 default-config
    rw  01-01-1970 01:56:32      1487 startup-config
2 files, 1771 bytes total.
```

2.8.24 # dir

Explanation: Display files in flash.

Example:

```
# dir
Directory of flash:
                                     default-config
    r-  01-01-1970 00:00:00       284
                                     startup-config
    rw  06-06-1970 01:56:32      1487

2 files, 3258 bytes total.
```

2.8.26 # dot1x

Syntax: # dot1x initialize [interface (<port_type> [<plist>])

[interface (<port_type> [<plist>])]: Specify the type of interface that you intend to use. "*" means all interfaces.

<plist>: Specify the ports that apply to this command.

Explanation: To initialize dot1x function in an interface immediately.

2.8.27 # erps

Syntax: # erps <group> command {clear | force | manual} {port0 | port1}

Explanation: Configure ERPS instance.

Parameters:

<group: 1-64>: Specify a group number between 1~64.

{clear | force | manual}: Specify an action.

{port0 | port1}: Specify port0 (east) or port1 (west) that applies to this command.

2.8.25 # disable & # enable

Explanation: Return to user mode or enter exec mode.

```
# disable
>
>
> enable
#
#
# enable 0
>
```

2.8.28 # firmware swap

Syntax: # firmware swap

Explanation: Use the other standby firmware image file uploaded to flash.

2.8.29 # firmware upgrade

Syntax: # firmware upgrade <TFTPServer_path_file : word>

<TFTPServer_path_file : word>: Specify the TFTP server IP address and firmware filename.

Explanation: Upgrade the firmware image.

2.8.30 # ip dhcp retry interface vlan

Syntax: # ip dhcp retry interface vlan <vlan_id>

<vlan_id>: Specify the valid VLAN ID for DHCP query.

Explanation: Restart the DHCP query process.

2.8.31 # more

Syntax: # more <path>

<path>: Specify the filename.

Explanation: Display file in Flash or in TFTP server.

2.8.32 # ping ip

Syntax: # ping ip <v_ip_addr> [repeat <count>] [size <size>] [interval <seconds>]

Explanation: Ping the specified IP.

Parameters:

<addr>: Specify the IPv4 address or IPv6 address for ping test.

2.8.33 # ping ipv6

Syntax: #ping ipv6 <v_ipv6_addr> [repeat <count>] [size <size>] [interval <seconds>] [interface vlan <v_vlan_id>]

< v_ipv6_addr >: Specify the IPv4 address or IPv6 address for ping test.

Explanation: Ping the specified IPv6 address.

Parameters:

[repeat <count>]: The number of echo packets will be sent.

[size <size>]: The size or length of echo packets.

[interval <seconds>]: The time interval between each ping

request. [interface vlan <v_vlan_id>]: Specify the VLAN ID.

2.8.34 # reload cold

Syntax: # reload cold

Explanation: Perform a cold reload on the system.

2.8.35 # reload defaults

Syntax: # reload defaults [keep-ip]

Explanation: Restore the device to factory default settings.

Parameters:

[keep-ip]: Keep VLAN 1 IP setting.

2.8.36 # send

Syntax: # send { * | <session_list> | console 0 | vty <vty_list> } <message>

Explanation: Send messages to other tty lines.

Parameters:

{ * | <session_list> | console 0 | vty <vty_list> }: Choose one of the options.

* : Specify "*" to denote all tty users.

<session_list>:Specify a session number between 0 and 16.

console 0: This means primary terminal line.

<vty_list>: Send a message to a virtual terminal.

<message>: Enter a message in 128 characters that you want to send.

2.8.37 # terminal editing

Syntax: # terminal editing

Explanation: Enable command line editing.

Show: >showterminal

show terminal

Negation: # no terminal editing

2.8.38 # terminal exec-timeout

Syntax: # terminal exec-timeout <0- 1440> [<0-3600>]

Parameters:

<0- 1440>:Specify the timeout value in minutes.

[<0-3600>]: Specify the timeout value in seconds.

Explanation: Set up terminal timeout value.

Show: >show terminal

show terminal

Negation: # no terminal exec-timeout

2.8.39 # terminal historysize

Syntax: # terminal history size <0-32>

Parameters:

<0-32>: Specify the current history size. "0" means to disable.

Explanation: Set up terminal history size.

Show: >show terminal

show terminal

Negation: # no terminal history size

2.8.40 # terminal length

Syntax: # terminal length <0 or 3-512>

Parameters:

<0 or 3-512>: Specify the lines displayed on the screen. "0" means no pausing.

Explanation: Set up terminal length.

Show: >show terminal

show terminal

Negation: # no terminal length

2.8.41 # terminal width

Syntax: # terminal width <0 or 40-512>

Parameters:

<0 or 40-512>: Specify the width displayed on the screen. "0" means unlimited width.

Explanation: Set up terminal display width.

Show: ›show terminal

show terminal

Negation: # no terminal width

2.8.42 # no port-security shutdown

Syntax: # no port-security shutdown [interface (<port_type>[<v_port_type_list>])]

Explanation: Reopen ports that are shutdown or disabled by Port Security function.

Parameters:

[interface (<port_type>[<v_port_type_list>])]: Specify the port type and port numbers that you want to reopen.

2.8.43 show commands

In Exec mode, "show" commands can be issued to display current status or settings of a certain command. They will be introduced in Section 3.9 "Commands in Config Mode".

2.9 Commands in Config Mode

2.9.1 (config)# aaa authentication login

Syntax: (config)# aaa authentication login { console | telnet | ssh | http } { { local | radius | tacacs }

[{ local | radius | tacacs } [{ local | radius | tacacs }]] }

Explanation: Configure the authentication method for the client.

Parameters:

{ console | telnet | ssh | http }: Specify one of the authentication clients.

{ { local | radius | tacacs } [{ local | radius | tacacs } [{ local | radius | tacacs }]] }: Specify one of the authentication methods for the specified client. At least one method needs to be specified. Users can specify three methods at most.

local: Use the local user database on the switch for authentication.

radius: Use remote RADIUS server(s) for authentication.

tacacs: Use remote TACACS+ server(s) for authentication.

NOTE: *Methods that involve remote servers will time out if the remote servers are offline. In this case the next method is tried. Each method is tried and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.*

Example: Set the Console client to use remote RADIUS server(s) for authentication.

```
# config t
(config)# aaa authentication login console radius
```

Negation: (config)# no aaa authentication login { console | telnet | ssh | http }

Show: # show aaa

2.9.2 (config)# access management

Syntax: (config)# access management <access_id> <access_vid> <start_addr> [to <end_addr>] { [web] [snmp] [telnet] | all }

Explanation: Create an access management rule.

Parameters:

<access_id: 1-16>: Specify an ID for this access management entry.

<access_vid>: Indicates the VLAN ID for the access management entry.

<start_addr> [to <end_addr>]: Indicate the starting and ending IP address for the access management entry.

{ [web] [snmp] [telnet] | all }: Specify matched hosts can access the switch from which interface.

Example: Allow IP 192.0.3.1 to 192.0.3.10 to access the device via Web, SNMP and Telnet.

```
# config t
(config)# access management 1 1 192.0.3.1 to 192.0.3.10 all
```

Negation: (config)# no access management

(config)# no access management <access_id>

Show: # show access management [statistics | <access_id_list>]

Clear: # clear access management statistics

2.9.3 (config)# access-list

(config)# access-list ace

Syntax: (config)# access-list ace <AceId : 1-256> [action {deny |filter |permit}] [dmac-type {any| broadcast |

multicast | unicast }] [frame-type {any | arp|etype|ipv4|ipv4-icmp|ipv4-tcp |ipv4-udp|ipv6|ipv6-icmp|ipv6-tcp |ipv6- udp}] [ingress {any | interface <PORT_TYPE> }] [logging] [mirror] [next { <AceId : 1-256>|last}] [policy <PolicyId : 0- 255>]

[rate-limiter {<RateLimiterId : 1-16>|disable}] [redirect {disable | interface <PORT_TYPE>}] [shutdown]

[tag{any|tagged|untagged}] [tag-priority {0-1 | 0-3 | 2-3 | 4-5 | 4-7 | 6-7 | <TagPriority : 0-7> |any}] [vid { <Vid : 1-4095>|any}]

Explanation: Configure an access control list.

Parameters:

<AceId : 1-256>: Specify access control list ID that applies to this rule.

[action {deny | filter | permit}]: Specify the action that applies to this rule.

[dmac-type {any| broadcast | multicast | unicast }]: Specify destination MAC type that applies to this rule.

[frame-type {any| arp|etype |ipv4|ipv4-icmp |ipv4-tcp|ipv4-udp|ipv6|ipv6-icmp|ipv6-tcp|ipv6-udp}]: Specify the frame type that applies to this rule.

[ingress {any | interface <PORT_TYPE> }]: Specify the ingress port.

[logging]: Enable logging function.

[mirror]: Enable the function of mirroring frames to destination mirror port.

[next{<AceId:1-256>|last}]: Insert the currentACEID before the next ACEID or put the ACEID to the last one.

[policy <PolicyId : 0-255>]: Specify the policy ID.

[rate-limiter {<RateLimiterId : 1-16>|disable}]: Specify the rate limit ID or disable this function.

[redirect {disable | interface <PORT_TYPE>}]: Redirect frames to a specific port or disable this function.

[shutdown]: Enable shutdownfunction.

[tag {any|tagged|untagged}]: Specify whether frames should be tagged or untagged.

[tag-priority {0-1 | 0-3 | 2-3 | 4-5 | 4-7 | 6-7 | <TagPriority : 0-7> |any}]: Specify the priority value.

[vid { <Vid : 1-4095>|any}]: Specify the VLAN ID.

Show: #show access-list [interface[(<port_type>[<v_port_type_list>])]][rate-limiter[<rate_limiter_list>]] [ace statistics [<ace_list>]]

Negation: (config)# no access-list ace <ace_list>

Clear: # clear access-list ace statistics

(config)# access-list ace update

Syntax: (config)#access-list ace update <AceId:1-256> [action{deny|filter|permit}] [dmac-type{any| broadcast| multicast | unicast }] [frame-type {any| arp|etype|ipv4|ipv4-icmp|ipv4-tcp |ipv4-udp|ipv6|ipv6-icmp|ipv6-tcp |ipv6- udp}] [ingress{any| interface<PORT_TYPE>}] [logging][mirror] [next{<AceId:1-256>|last}] [policy<PolicyId :0- 255>] [rate-limiter {<RateLimiterId : 1-16>|disable}] [redirect {disable | interface <PORT_TYPE>}]

[shutdown] [tag{any|tagged|untagged}] [tag-priority {0-1 | 0-3 | 2-3 | 4-5 | 4-7 | 6-7 | <TagPriority : 0-7> |any}] [vid { <Vid : 1- 4095>|any}]

Explanation: Update an access control list.

Parameters:

<AceId : 1-256>: Specify access control list ID that applies to this rule.

[action {deny | filter | permit}]: Specify the action that applies to this rule.

[dmac-type {any| broadcast | multicast | unicast }]: Specify destination MAC type that applies to this rule.

[frame-type {any| arp|etype |ipv4|ipv4-icmp |ipv4-tcp|ipv4-udp|ipv6|ipv6-icmp|ipv6-tcp|ipv6-udp}]: Specify the frame type that applies to this rule.

[ingress {any | interface <PORT_TYPE> }]: Specify the ingress port.

[logging]: Enable logging function.

[mirror]: Enable the function of mirroring frames to destination mirror port.

[next{<AceId:1-256>|last}]: Insert the current ACEID before the next ACEID or put the ACE ID to the last one.

[policy <PolicyId : 0-255>]: Specify the policy ID.

[rate-limiter {<RateLimiterId : 1-16>|disable}]: Specify the rate limit ID or disable this function.

[redirect {disable| interface <PORT_TYPE>}]: Redirect frames to a specific port or disable this function.

[shutdown]: Enable shutdown function.

[tag {any|tagged|untagged}]: Specify whether frames should be tagged or untagged.

[tag-priority {0-1 | 0-3 | 2-3 | 4-5 | 4-7 | 6-7 | <TagPriority : 0-7> |any}]: Specify the priority value.

[vid { <Vid : 1-4095>|any}]: Specify the VLAN ID.

Show: #show access-list [interface[(<port_type>[<v_port_type_list>])]] [rate-limiter[<rate_limiter_list>]] [ace statistics [<ace_list>]]

Negation: (config)# no access-list ace <ace_list>

(config)# access-list rate-limiter

Syntax: (config)# access-list rate-limiter [<rate_limiter_list>] { pps <pps_rate> |100pps <pps100_rate> |kpps <kpps_rate> | 100kbps <kpbs100_rate> }

Explanation: Configure rate limiter that applies to each rate limit ID.

Parameters:

[<rate_limiter_list>]: Specify the "rate limit ID", "100kbps" or "pps". The allowed rate limit ID range is from1~16.

{ pps <pps_rate> | 100pps <pps100_rate> | kpps <kpps_rate> | 100kbps <kpbs100_rate> }: Specify the rate limit rate.

Show: # show access-list rate-limiter [<RateLimiterList : 1~16>]

(config-if)# access-list action

Syntax: (config-if)# access-list action { permit|deny}

Explanation: Configure a specific port's action option.

Parameters:

{ permit|deny}: Permit or deny frames on a specific port.

Show: # show access-list [interface [(<port_type> [<v_port_type_list>])]]

(config-if)# access-list logging

Syntax: (config-if)# access-list logging

Explanation: Enable a specific port's logging function.

Show: # show access-list [interface [(<port_type> [<v_port_type_list>])]]

Negation: (config-if)# no access-list logging

(config-if)# access-listmirror

Syntax: (config-if)# access-list mirror

Explanation: Enable a specific port's frames to be mirrored to a destination port.

Show: # show access-list [interface [(<port_type> [<v_port_type_list>])]]

Negation: (config-if)# no access-list mirror

(config-if)# access-list policy

Syntax: (config-if)# access-list policy <policy_id>

Parameters:

<policy_id:0-255>: Specify a policy ID that applies to this specific port.

Explanation: Apply a policy ID to a specific port.

Show: # show access-list [interface [(<port_type> [<v_port_type_list>])]]

Negation: (config-if)# no access-list policy

(config-if)# access-list port-state

Syntax: (config-if)# access-list port-state

Explanation: Enable a specific port ' s port state.

Negation: (config-if)# no access-list port-state

(config-if)# access-list rate-limiter

Syntax: (config-if)# access-list rate-limiter <rate_limiter_id>

Parameters:

<rate_limiter_id:1-16>: Specify a rate limiter ID to a specific port.

Explanation: Apply a rate limiter ID to a specific port.

Negation: (config-if)# no access-list rate-limiter

(config-if)# access-list shutdown

Syntax: (config-if)# access-list shutdown

Explanation: Shutdown this port when specified rules are matched.

Negation: (config-if)# no access-list shutdown

(config-if)# access-list { redirect | port-copy }

Syntax: (config-if)# access-list { redirect | port-copy } interface { <port_type> <port_type_id> | (<port_type> [<port_type_list>]) }

Parameters:

{ redirect | port-copy }: Redirect or copy this port's frames to the specified port.

interface{<port_type><port_type_id>|(<port_type>[<port_type_list>])}: Specifytheredirectorcopyport type and port list.

Explanation: Redirect or copy this port's frames to the specified port.

Negation: (config-if)# no access-list { redirect | port-copy }

2.9.4 (config)# aggregation

(config)# aggregation mode

Syntax: (config)# aggregation mode { [smac] [dmac] [ip] [port] }

Explanation: Configure aggregation mode.

Parameters:

[smac]: All traffic from the same Source MAC address is output on the same link in a trunk.

[dmac]: All traffic with the same Destination MAC address is output on the same link in a trunk.

[ip]: All traffic with the same source and destination IP address is output on the same link in a trunk.

[port]: All traffic with the same source and destination TCP/UDP port number is output on the same link in a trunk.

Negation: (config)# no aggregation mode

Show: # show aggregation [mode]

(config-if)# aggregation group

Syntax: (config-if)# aggregation group <unit>

Explanation: Add this specific interface to the specified aggregation group.

Parameters:

<unit>: Specify the aggregation group ID.

Negation: (config-if)# no aggregation group

Show: # show aggregation [mode]

2.9.5 (config)# banner

(config)# banner [motd] <banner>

Syntax: (config)# banner [motd] <banner>

Parameters:

[motd]: Type inthe message ofthe day.

Explanation: Configure the message of theday.

Negation: (config)# no banner [motd]

(config)# banner exec <banner>

Syntax: (config)# banner exec <banner>

Explanation: Display the configured message when successfully entering Exec mode.

Negation: (config)# no banner exec

(config)# banner login<banner>

Syntax: (config)# banner login <banner>

Explanation: Display the configured message when prompted for login ID and password.

Negation: (config)# no banner login

2.9.6 (config)# clock

(config)# clock summer-time <word16> date

Syntax: clock summer-time <word16> date [<start_month_var> <start_date_var> <start_year_var> <start_hour_var> <end_month_var> <end_date_var> <end_year_var> <end_hour_var> [<offset_var>]]

Explanation: Configure daylight saving time. This is used to set the clock forward or backward according to the

configurationsset fora definedDaylightSavingTimeduration. "Recurring " commandis usedto repeatthe configuration every year.

Parameters:

summer-time <word16>: Specify a description for this day-light setting.

date [<start_month_var> <start_date_var> <start_year_var> <start_hour_var> <end_month_var> <end_date_var> <end_year_var> <end_hour_var> [<offset_var>]]

<start_month_var:1-12>: Specify the starting month.

<start_date_var: 1-31>: Specify the starting day.

<start_year_var:2000-2097>: Specify the starting year.

<start_hour_var: hh:mm>: Specify the time to start.

<end_month_var:1-12>: Specify the ending month.

<end_date_var: 1-31>: Specify the ending day.

<end_year_var:2000-2097>: Specify the ending year.

<end_hour_var: hh:mm>: Specify the time to start.

[<offset_var: 1-1440>]: Specify the number of minutes to add during Daylight Saving Time. The allowed range is 1 to 1440.

Negation: (config)# no clock summer-time

Show: > show clock

> show clock detail

showclock

show clock detail

(config)# clock summer-time <word16> recurring

Syntax: (config)# clock summer-time <word16> recurring [<start_week_var> <start_day_var> <start_month_var> <start_hour_var> <end_week_var> <end_day_var> <end_month_var> <end_hour_var> [<offset_var>]]

Explanation: Configure daylight saving time. This is used to set the clock forward or backward according to the configurationsset fora definedDaylight SavingTimeduration. "Recurring " commandis usedto repeatthe configuration every year.

Parameters:

summer-time <word16>: Specify a description for this day-light setting.

recurring [<start_week_var> <start_day_var> <start_month_var> <start_hour_var> <end_week_var> <end_day_var> <end_month_var> <end_hour_var> [<offset_var>]]

<start_week_var:1-5>: Specify the starting week.

<start_day_var: 1-31>: Specify the starting day.

<start_month_var:1- 12>: Specify the starting month.

<start_hour_var: hh:mm>: Specify the time to start.

<end_week_var:1-5>: Specify the ending week.

<end_day_var: 1-31>: Specify the ending day.

<end_month_var: 1-12>: Specify the ending month.

<end_hour_var: hh:mm>: Specify the time to end.

[<offset_var: 1-1440>]: Specify the number of minutes to add during Daylight Saving Time. The allowed range is 1 to 1440.

Negation: (config)# no clock summer-time

Show: # show clock

show clock detail

(config)# clock timezone

Syntax: (config)# clock timezone <word> <-23-23> [<0-59>]

Explanation: Configure a timezone used in the switch.

Parameters:

<word16>: Specify the name of the timezone.

<-23-23>: Hours offset from UTC.

[<0-59>]: Minutes offset from UTC.

Negation: (config)# no clock timezone

Show: # show clock

show clock detail

2.9.7 (config)# default access-list rate-limiter

Syntax: (config)# default access-list rate-limiter [<rate_limiter_list>]

Explanation: To default the specified rate-limiter ID.

Parameters:

[<rate_limiter_list: 1-16>]: Specify a rate limiter ID.

Example: To default rate-limiter 1.

```
# config t
 (config)#  default access-list rate-limiter 1
```

2.9.8 (config)# dot1x

(config)# dot1x system-auth-control

Syntax: (config)# dot1x system-auth-control

Explanation: To enable 802.1x service.

Example: Enable 802.1x service.

```
# config t
(config)# dot1x system-auth-control
```

Negation: (config)# no dot1x system-auth-control

Show: > show dot1x status [interface(<port_type> [<v_port_type_list>])][brief]

show dot1x status [interface (<port_type> [<v_port_type_list>])] [brief]

(config)# dot1x re-authentication

Syntax: (config)# dot1x re-authentication

Explanation: Set clients to be re-authenticated after an interval set in "Re-authenticate" field. Re-autentication can be used to detect if a new device is attached to a switch port.

Example: Enable re-authentication function.

```
# config t
(config)# dot1x re-authentication
```

Negation: (config)# no dot1x re-authentication

Show: > show dot1x status [interface (<port_type> [<v_port_type_list>])] [brief]

show dot1x status [interface (<port_type> [<v_port_type_list>])] [brief]

(config)# dot1x authentication timer re-authenticate

Syntax: (config)# dot1x authentication timer re-authenticate <1-3600>

Explanation: Specify the time interval for a connected device to be re-authenticated. By default, the re-authenticated period is set to 3600 seconds. The allowed range is 1 - 3600 seconds.

Parameters:

<1-3600>: Specify a re-authentication value between 1 and 3600.

Example: Set re-authentication timer to 100.

```
# config t
 (config)# dot1x authentication timer re-authenticate 100
```

Negation: (config)# no dot1x authentication timer re-authenticate

(config)# dot1x timeouttx-period

Syntax: (config)# dot1x timeout tx-period <v_1_to_65535>

Explanation: Specify the time that the switch waits for a supplicant response during an authentication session before

transmitting a Request Identify EAPOL packet. By default, it is set to 30 seconds.

Parameters:

<v_1_to_65535>: Specify a timeout value between 1 and 65535 (seconds).

Example: Set EAPOL timeout to 30 seconds.

```
# config t
(config)# dot1x timeout tx-period 30
```

Negation: (config)# no dot1x timeout tx-period

(config)#dot1x authentication timer inactivity

Syntax: (config)# dot1x authentication timer inactivity <10-1000000>

Explanation: Specify the period that is used to age out a client's allowed access to the switch via 802.1Xand MAC-based authentication. The default period is 300 seconds. The allowed range is 10 - 1000000 seconds.

Parameters:

<10-1000000>: Specify a value between 10 and 1000000 (seconds).

Example: Set the aging time to 300 seconds.

```
# config t
(config)# dot1x authentication timer inactivity 300
```

Negation: (config)# no dot1x authentication timer inactivity

(config)# dot1xtimeout quiet-period

Syntax: (config)# dot1x timeout quiet-period <v_10_to_1000000>

Explanation: The time afteranEAP Failure indication or RADIUS timeout that aclient is not allowed access. This setting applies to ports running Single 802.1X, Multi 802.1X, or MAC-based authentication. By default, hold time is set to 10 seconds. The allowed range is 10 - 1000000 seconds.

Parameters:

<10-1000000>: Specify a value between 10 and 1000000 (seconds).

Example: Set hold time to 30 seconds.

```
# config t
 (config)# dot1x timeout quiet-period 30
```

Negation: (config)# no dot1x timeout quiet-period

(config)# dot1x feature

Syntax: (config)# dot1x feature { [guest-vlan] [radius-qos] [radius-vlan] }

Explanation: Enable the specified feature.

Parameters:

{ [guest-vlan] [radius-qos] [radius-vlan] }:

[guest-vlan]: Enable guest VLAN. A Guest VLAN is a special VLAN typically with limited network access. When checked,theindividualports'dittosetting determineswhethertheport can be movedinto Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

[radius-qos]: Enable RADIUS assigned QoS.

[radius-vlan]: Enable RADIUS VLAN. RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature.

Example: Enable guest VLAN service.

```
# config t
(config)# dot1x feature guest-vlan
```

Negation: (config)# no dot1x feature { [guest-vlan] [radius-qos] [radius-vlan] }

(config)# dot1x guest-vlan

Syntax: (config)# dot1x guest-vlan <value> Explanation:Configurea guestVLANID. Parameters:

<value:1-4095>: Specify the guest VLAN ID. The allowed VLAN ID range is from 1 to 4095.

Negation: (config)# no dot1x guest-vlan

(config)# dot1x guest-vlan supplicant

Syntax: (config)# dot1x guest-vlan supplicant

Explanation: Enable GuestVLANsupplicantfunction. The switch remembers ifanEAPOLframe has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, itwill first check if this option is enabled or disabled. When enabled, the switch does not maintain the EAPOL packet history and allows clients that fail authentication to access the guest VLAN, regardless ofwhether EAPOL packets had been detected on the interface. Clients that fail authentication can access the guest VLAN.

Negation: (config)# no dot1x guest-vlan supplicant

(config)# dot1x max-requth-req

Syntax: (config)# dot1x max-reauth-req <value>

Explanation: The maximum number of times the switch transmits an EAPOL Request Identity frame without receiving a response before adding a port to the Guest VLAN. The value can only be changed when the Guest VLAN option is globally enabled. The range is 1 - 255.

Parameters:

<value:1-255>: Specify a value between 1 and 255.

Negation: (config)# no dot1x max-reauth-req

(config-if)# dot1x port-control

Syntax: (config-if)# dot1x port-control {force-authorized |force-unauthorized |auto |single |multi | mac-based }

Parameters:

{force-authorized | force-unauthorized | auto | single | multi | mac-based }: Specify one of the authentication modes on the selected interfaces. This setting works only when NAS is globally enabled. The following modes are available:

force-authorized: In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.

force unauthorized: In this mode, the switchwill send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.

auto (Port-Based 802.1X): This mode requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.

single (802.1X): In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the "Port Security" module is used to secure a supplicant's MAC address once successfully authenticated.

multi (802.1X): In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the "Port Security" module.

mac-based: Unlike port-based 802.1X, MAC-based authentication do not transmit or receive EAPOL frames. In MAC-based authentication, the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

Example: Set Gigabit Ethernt port 1-10's admin state to "auto"

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# dot1x port-control auto
```

Negation: (config-if)# no dot1x port-control

(config-if)# dot1x guest-vlan

Syntax: (config-if)# dot1x guest-vlan

Explanation: Enable the guest VLAN on the selected interfaces.

Example: Enable guest VLAN on port 1-10.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# dot1x guest-vlan
```

Negation: (config-if)# no dot1x guest-vlan

(config-if)# dot1x radius-qos

Syntax: (config-if)# dot1x radius-qos

Explanation: Enable RADIUS Assigned QoS on the selected interfaces.

Example: Enable RADIUS Assigned QoS on port 1-10.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# dot1x radius-qos
```

Negation: (config-if)# no dot1x radius-qos

(config-if)# dot1x radius-vlan

Syntax: (config-if)# dot1x radius-vlan

Explanation: Enable RADIUS Assigned VLAN on the selected interfaces.

Example: Enable RADIUS Assigned VLAN on port 1-10.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# dot1x radius-vlan
```

Negation: (config-if)# no dot1x radius-vlan

(config-if)# dot1x re-authenticate

Syntax: (config-if)# dot1x re-authenticate

Explanation: Schedules reauthentication to whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately. This command only has effectfor successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

Show: >show dot1x statistics { eapol | radius | all } [interface (<port_type> [<v_port_type_list>])] # show dot1x statistics { eapol | radius | all } [interface (<port_type> [<v_port_type_list>])]

2.9.9 (config-if)# duplex

Syntax: (config-if)# duplex { half | full | auto [half | full] }

Explanation: Configure port ' s duplex mode.

Parameters:

{ half | full | auto [half | full] }: specify the duplex mode for this specific interface.

Example: Set port 1 ' s duplex mode to auto.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# duplex auto
```

Negation: (config-if)# no duplex

Show: > show interface (<port_type> [<v_port_type_list>])

status # show interface (<port_type>

[<v_port_type_list>]) status

2.9.10 (config)# enable

(config)# enable password

Syntax: (config)# enable password <password>

Explanation: Configure enable password.

Parameters:

password <password>: Specify the enable mode password.

(config)# enable password level

Syntax: (config)# enable password [level <priv: 1-15>]<password>

Explanation: Configure enable password and privilege level.

Parameters:

[level <priv: 1-15>]: Specify the privilege level for this password.

<password>: Specify the enable mode password.

Negation: (config)# no enable password [level <priv>]

(config)# enable secret

Syntax: (config)# enable secret { 0 | 5 } [level <priv: 1-15>] <password>

Parameters:

{ 0 | 5 } : Specify " 0 " todenote unencryptedsecret(cleartext). Specify " 5 " todenoteencryptedsecret

(MD5). [level <priv: 1-15>]: Specify the privilege level for this password.

<password>: Specify the enable mode password.

Explanation: Configure enable secret password and privilege level.

Negation: (config)# no enable secret { [0 | 5] } [level <priv>]

2.9.11 (config)# erps

(config)# erps <group> guard <guard_time_ms>

Syntax: (config)# erps <group> guard <guard_time_ms>

Explanation: Configure the specified group's guard time. **Parameters:**

<group: 1-64>: Specify a group number. The allowed range is from 1 to 64.

<guard_time_ms: 10-2000>: Specify the guard time. The allowed range is 10 to 2000 ms.

Negation: (config)# no erps <group> guard

Negation: # show erps [<groups>] [detail | statistics]

(config)# erps <group> holdoff <holdoff_time_ms>

Syntax: (config)# erps <group> holdoff <holdoff_time_ms>

Parameters:

<group: 1-64>: Specify a group number. The allowed range is from 1 to 64.

<holdoff_time_ms: 0- 10000>: Specify the holdoff time. The allowed range is 0 to 10000 ms.

Explanation: Configure the specified group's holdoff time.

Negation: (config)# no erps <group> holdoff

Negation: # show erps [<groups>] [detail | statistics]

(config)# erps <group> major port0 interface port1 interface <port_type> <port1> [interconnect]

Syntax: (config)# erps <group> major port0 interface <port_type> <port0> port1 interface <port_type> <port1> [interconnect]

Explanation: Create an ERPS instance.

Parameters:

<group: 1-64>: Specify a group number. The allowed range is from 1 to 64.

<port_type><port0>:SpecifyPort0 ' sport typeandport number. Port0 is also knownas Eport(Eastport) which is used by some of the other vendors.

<port_type> <port1>: Specify Port 1 ' sport type and port number. Port 1 is also known as W port (Westport)

which is used bysome ofthe other vendors.When this portis interconnected with theothersub-ring, "0" is used in this field to indicate that no west port is associated with this instance.

[interconnect]: Specify this parameter if this is an interconnected node for this instance.

Show: # show erps [<groups>] [detail | statistics]

(config)# erps <group> mep port0 sf <p0_sf> aps <p0_aps> port1 sf <p1_sf> aps <p1_aps>

Syntax: (config)# erps <group> mep port0 sf <p0_sf> aps <p0_aps> port1 sf <p1_sf> aps <p1_aps>

Explanation: Configure the specified group's MEP & APS settings.

Parameters:

<group: 1-64>: Specify a group number. The allowed range is from 1 to 64.

<p0_sf>: This is also known as East Signal FailAPS MEP. Assign the East Signal Fail reporting MEPinthisfield.

<p0_aps>: Specify the East APS PDU handling MEP.

<p1_sf>: This is also known as West Signal Fail APS MEP. When interconnected with the other sub-ring, "0" is used in this field to indicate that no west SF MEP is associated with this instance. Assign the West Signal Fail reporting MEP in this field.

<p1_aps>: Specify theWestAPSPDU handling MEP. When interconnected with the other sub-ring, "0" is used in this field to indicate that no west APS MEP is associated with this instance.

Negation: (config)# no erps <group> mep

Show: # show erps [<groups>] [detail | statistics]

(config)# erps <group> revertive <wtr_time_minutes>

Syntax: (config)# erps <group> revertive <wtr_time_minutes>

Explanation: Configure theWait-to-Restore timer in revertive mode.

Parameters:

<group: 1-64>: Specify a group number. The allowed range is from 1 to 64.

<wtr_time_minutes>: Specify Wait-to-Restore timer in minutes. The allowed range is from 1 to 12 minutes.

Negation: (config)# no erps <group> revertive

Show: # show erps [<groups>] [detail | statistics]

(config)# erps <group> rpl { owner | neighbor } { port0 | port1 }

Syntax: (config)# erps <group> rpl { owner | neighbor } { port0 | port1 }

Explanation: Specify the Ethernet ring port on the local node as the RPL (Ring Protection Link) owner or neighbor.

Parameters:

<group: 1-64>: Specify a group number. The allowed range is from 1 to 64.

{ owner | neighbor }: Specify the ring port is a owner or neighbor. RPL (Ring Protection Link) is responsible for blocking traffic over the RPL so that no loops are formed in the Ethernet traffic.

{ port0 | port1 }: Specify the port applies to this rule.

Negation: (config)# no erps <group> rpl

Show: # show erps [<groups>] [detail | statistics]

(config)# erps <group> sub port0 interface<port_type> <port0> {{ port1 interface

<port_type> <port1> } | { interconnect <major_ring_id> [virtual-channel]} }

Syntax: (config)# erps <group> sub port0 interface <port_type> <port0> { { port1 interface <port_type> <port1> } | { interconnect <major_ring_id> [virtual-channel] } }

Explanation: Create a profile and configure the Sub ERPS interface port 0, port 1.

Parameters:

<group: 1-64>: Specify a group number. The allowed range is from 1 to 64.

<port_type> <port0>: Specify sub port's port type and port number.

{{port1interface<port_type><port1>}|{interconnect<major_ring_id>[virtual-channel]}}:SpecifyPort 1's port type and port numbr or specify major ring's group ID.

Negation: (config)# no erps <group>

Show: # show erps [<groups>] [detail | statistics]

(config)# erps <group>topology-change propagate

Syntax: (config)# erps <group> topology-change propagate

Parameters:

<group: 1-64>: Specify a group number. The allowed range is from 1 to 64.

Explanation: Allow topology change notification propagation.

Negation: (config)# no erps <group> topology-change propagate

Show: # show erps [<groups>] [detail | statistics]

(config)# erps <group> version { 1 | 2 }

Syntax: (config)# erps <group> version { 1 | 2 }

Explanation: Configure ERPS version for a specific profile.

Parameters:

<group: 1-64>: Specify a group number. The allowed range is from 1 to 64.

{ 1 | 2 }: Specify ERPS version 1 or 2.

Negation: (config)# no erps <group> version

Show: # show erps [<groups>] [detail | statistics]

(config)# erps <group> vlan { none | [add | remove] <vlans> }

Syntax: (config)# erps <group> vlan { none | [add | remove] <vlans> }

Explanation: Configure VLANs for a specific ERPS profile.

Parameters:

<group: 1-64>: Specify a group number. The allowed range is from 1 to 64.

{ none | [add | remove] <vlans> } : Specify an option.

none: Do not include any VLANs.

[add | remove] <vlans>: Add or remove a specific VLAN.

Negation: (config)# no erps <group> vlan

Show: # show erps [<groups>] [detail | statistics]

2.9.12 (config-if)# excessive-restart

Syntax: (config-if)# excessive-restart

Explanation: Restartbackoffalgorithm after 16 collisions(No excessive-restart means discard frames after 16 collisions.)

Negation: (config-if)# no excessive-restart

Show: > show interface (<port_type> [<v_port_type_list>]) status

show interface (<port_type> [<v_port_type_list>]) status

2.9.13 (config-if)# flowcontrol { on | off }

Syntax: (config-if)# flowcontrol { on | off }

Explanation: Enable or disable flow confrol for this specific interface.

Parameters:

{ on | off }: Enable or disable flow control.

Negation: (config-if)# no flowcontrol

Show: > show interface (<port_type> [<v_port_type_list>]) status

show interface (<port_type> [<v_port_type_list>]) status

2.9.14 (config)# green-ethernet

(config)# green-ethernet ledinterval

Syntax: (config)# green-ethernet led interval <v_0_to_24> intensity <v_0_to_100>

Explanation: Configure the LED time interval and LED light intensity to reduce power consumption.

Parameters:

led interval <v_0_to_24>: Specify LEDtime interval. The first value is the starting time. The second one is the ending time. The allowed value is from 0 to 24.

intensity <v_0_to_100>: LED intensity. The value is from 0 to 100.

Example: LED intensity reduces to 80% during 9:00 and 18:00.

```
                    function for optimized
# config t
(config)# green-ethernet led interval 9-18 intensity 80
```

Negation: (config)# no green-ethernet led interval <0~24>

(config)# green-ethernetled on-event

Syntax: (config)# green-ethernet led on-event { [link-change <v_0_to_65535>] [error]}

Explanation: The switch will bring LED intensity to 100% for the specified period in the event ofany error (such as link down).

Parameters:

[link-change <v_0_to_65535>]: Specify how long LED intensity 100% lasts when errors occur. The allowed value is from 0 to 65535.

[error]: Bring LED intensity to 100% in the event of errors.

Example: Bring LED intensity to 100% for 10 minutes when errors occur.

```
                    function for optimized
# config t
(config)# green-ethernet led on-event link-change 600 error
```

Negation: (config)# no green-ethernet led on-event [link-change] [error]

(config)# green-ethernet eee optimize-for-power

Syntax: (config)# green-ethernet eee optimize-for-power

Explanation: Enables the EEE function for this switch.

Example: Enable EEE function for optimized power.

```
# config t
 (config)# green-ethernet eee optimize-for-power
```

Negation: (config)# no green-ethernet eee optimize-for-power

show: # show green-ethernet [interface (<port_type> [<port_list>])]

show green-ethernet eee [interface (<port_type> [<port_list>])]

#showgreen-ethernet energy-detect[interface(<port_type>[<port_list>])]

show green-ethernet short-reach [interface (<port_type> [<port_list>])]

(config-if)# green-ethernet eee

Syntax: (config-if)# green-ethernet eee

Explanation: Enable EEE (Energy-Efficient Ethernet) on the selected interface.

Negation: (config-if)# no green-ethernet eee

Show: # show green-ethernet eee [interface (<port_type> [<port_list>])]

(config-if)# green-ethernet urgent-queues

Syntax: (config-if)# green-ethernet eee urgent-queues [<urgent_queue_range_list>]

Explanation: It is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.

Queues set will activate transmission offrames assoon as data is available. Otherwise the queue will postpone transmission until a burst of frames can be transmitted.

Parameters:

[<urgent_queue_range_list>]: Specify urgent queue range. The allowed range is from 1 to 8.

Negation: (config-if)# no green-ethernet eee urgent-queues [<urgent_queue_range_list>]

(config-if)# green-ethernet energy-detect

Syntax: (config-if)# green-ethernet energy-detect

Explanation: Enable power saving function for this specific interface when there is no link partner.

Negation: (config-if)# no green-ethernet energy-detect

Show: # show green-ethernet energy-detect [interface (<port_type> [<port_list>])]

(config-if)# green-ethernet short-reach

Syntax: (config-if)# green-ethernet short-reach

Explanation: Enable power saving for ports which is connect to link partner with short cable.

Negation: (config-if)# no green-ethernet short-reach

Show: # show green-ethernet short-reach [interface (<port_type> [<port_list>])]

2.9.15 (config)# gvrp

(config)# gvrp

Syntax: (config)# gvrp

Explanation: Globally enable GVRP function.

Example: Globally enable GVRP function.

```
# config t
(config)# gvrp
(config)#
```

Negation: (config)# no gvrp

(config)# gvrp max-vlans

Syntax: (config)# gvrp max-vlans <maxvlans>

Explanation: Set up the maximum number of VLANs can be learned via GVRP.

Parameters:

<maxvlans>: Specify the number of VLANs learned via GVRP.

Example: Set the maximum number of VLANs can be learned via GVRP to 20.

```
# config t
(config)# gvrp
(config)# gvrp max-vlans 20
```

Negation: (config)# no gvrp max-vlans <maxvlans>

(config)# gvrp time

Syntax: (config)# gvrp time { [join-time <jointime>] [leave-time <leavetime>] [leave-all-time <leavealltime>] }

Explanation: Set up the maximum number of VLANs can be learned via GVRP.

Parameters:

[join-time<jointime>]: Specify the amount of time in unitsof centi-seconds that PDUs are transmitted. The default value is 20 centi-seconds. The valid value is 1~20.

[leave-time<leavetime>]:Specify the amount of time in units of centi-seconds that the device waits before deleting the associated etry. The leave time is activated by a "Leave All-time" message sent/received and cancelled by the Join message. The default value is 60 centi-seconds.

NOTE: The "LeaveAll-time" parameter must be greater than the "Leave-time" parameter.

[leave-all-time <leavealltime>]: Specify the amount of time that "LeaveAll" PDUs are created. A LeaveAll PDU indicates thatall registrations are shortlyde-registered. Participants will need to rejoin in order to maintain registration. The valid value is 1000 to 5000 centi-seconds. The factory default 1000 centi-seconds.

NOTE: The "LeaveAll-time" parameter must be greater than the "Leave-time" parameter.

Negation: (config)# nogvrptime { [join-time <jointime>] [leave-time <leavetime>] [leave-all-time <leavealltime>] }

(config-if)# gvrp

Syntax: (config-if)# gvrp

Explanation: Enable GVRP function on the specified interfaces.

Example: Enable GVRP function on port 1~5.

```
# config t
(config)# interface GigabitEthernet 1/1-5
(config-if)# gvrp
(config-if)#
```

Negation: (config-if)# no gvrp

2.9.16 (config)# hostname

Syntax: (config)# hostname <WORD>

Explanation: Specify a descriptive name for this switch.

Parameters:

<WORD32>: Specify a descriptive name for this device. Indicate the hostname for this device. Alphabets (A-Z; a-z), digits(0-9) and minus sign(-) can be used. However, space characters are not allowed. The first character must be an alphabet character. The first and last character must not be a minus sign. The allowed string length is 0 – 255.

Example: Set the hostname to AccessSW.

```
# config t
(config)# hostname AccessSW
AccessSW(Config)#
```

Negation: (config)# no hostname

Show: > showversion

show version

2.9.17 (config)# interface

(config)# interface (<port_type> [<plist>])

Syntax: (config)# interface (<port_type> [<plist>])

Explanation: Enter Config Interface mode for this specific interface.

Parameters:

<port_type> [<plist>]: Specify the port type and port number.

Example: Enter Config Interface mode for Gigabit Ethernet port 1.

```
# config t
(config)#
(config)# interface GigabitEthernet 1/1
(config-if)#
```

Show: > show interface (<port_type> [<in_port_list>]) switchport [access | trunk | hybrid]
> show interface (<port_type> [<v_port_type_list>]) capabilities

> show interface(<port_type>[<v_port_type_list>])statistics [{ packets |bytes |errors |discards|filtered| { priority [<priority_v_0_to_7>] } }] [{ up | down }]

> show interface (<port_type> [<v_port_type_list>]) status

> show interface vlan [<vlist>]

show interface (<port_type> [<in_port_list>]) switchport [access |trunk |hybrid]

show interface (<port_type> [<v_port_type_list>]) capabilities

#showinterface(<port_type>[<v_port_type_list>]) statistics [{ packets |bytes|errors |discards |filtered | { priority [<priority_v_0_to_7>] } }] [{ up | down }]

show interface (<port_type> [<v_port_type_list>]) status

show interface vlan [<vlist>]

Clear: # clear statistics { [interface] (<port_type> [<v_port_type_list>]) }

(config)# interface vlan

Syntax: (config)# interface vlan <vlist>

Explanation: Enter Config Interface VLAN mode for this specific interface.

Example: Enter Config Interface VLAN 1 for port 1.

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

2.9.18 (config)# ip

(config)# ip arp inspection

Syntax: (config)# ip arp inspection

Explanation: Enable ARP inspection function.

Negation: (config)# no ip arp inspection

Show:>show ip arp inspection[interface(<port_type>[<in_port_type_list>])|vlan

<in_vlan_list>] #show ip arp inspection[interface(<port_type>[<in_port_type_list>]) | vlan <in_vlan_list>]

Clear: # clear ip arp

(config)# ip arp inspection entry interface

Syntax: (config)#iparp inspection entry interface<port_type> <in_port_type_id><vlan_var><mac_var><ipv4_var>

Explanation: Create ARP static entry.

Parameters:

<port_type> <in_port_type_id>: Specify the port type and port number.

<vlan_var>: Specify a configured VLAN ID.

<mac_var>: Specify an allowed source MAC address in ARP request packets.

<ipv4_var>: Specify an allowed source IP address in ARP request packets.

Negation: (config)# no ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>

Show: # show ip arp inspection entry [dhcp-snooping | static] [interface (<port_type> [<in_port_type_list>])]

Clear: # clear ip arp

(config)# ip arp inspection translate

Syntax: (config)# ip arp inspection translate [interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>]

Explanation: Translate the dynamic entry to static one.

Parameters:

<port_type> <in_port_type_id>: Specify the port type and port number.

<vlan_var>: Specify a configured VLAN ID.

<mac_var>: Specify an allowed source MAC address in ARP request packets.

<ipv4_var>: Specify an allowed source IP address in ARP request packets.

Show: # show ip arp inspection entry [dhcp-snooping | static] [interface (<port_type> [<in_port_type_list>])]

(config)# ip arp inspection vlan

Syntax: (config)# ip arp inspection vlan <in_vlan_list>

Explanation: Specify ARP inspection is enabled on which VLAN.

Parameters:

<in_vlan_list>: Specify a list of VLAN ID to be used for ARP inspection.

Negation: (config)# no ip arp inspection vlan <in_vlan_list>

Show: <show ip arp

#show ip arp

Clear: # clear ip arp

(config)# ip arp inspection vlan <in_vlan_list> logging

Syntax: (config)# ip arp inspection vlan <in_vlan_list> logging { deny | permit | all }

Explanation: Enable log function.

Parameters:

{ deny | permit | all }: Specify one of the log types.

Deny: Log denied entries.

Permit: Log permitted entries.

All: Log all entries.

Negation: (config)# no ip arp inspection vlan <in_vlan_list> logging

Show: <show ip arp

#show ip arp

Clear: # clear ip arp

(config)# ip dhcp relay

Syntax: (config)# ip dhcp relay

Explanation: Enable DHCP relay function.

Example: Enable DHCP relay function.

```
# config t
(config)# ip dhcp relay
```

Negation: (config)# no ip dhcp relay

Show: >show ip dhcp relay [statistics]

show ip dhcp relay [statistics]

Clear: # clear ip dhcp relay statistics

(config)# ip dhcp relay information option

Syntax: (config)# ip dhcp relay information option

Explanation: Enable DHCP Relay option82 function. Please note that "Relay Mode" must be enabled before this function is able to take effect.

Example: Enable DHCP Relay option 82 function

```
# config t
(config)# ip dhcp relay information option
```

Negation: (config)# no ip dhcp relay information option

(config)# ip dhcp relay information policy {drop | keep |replace}

Syntax: (config)# ip dhcp relay information policy { drop | keep | replace }

Explanation: Specify DHCP Relay information policy action.

Parameters:

{ drop | keep | replace }: Specify one of the relay information policy options.

drop: Drop the packet when it receives a DHCP message that already contains relay information.

keep: Keep the client's DHCP information.

replace: Replace the DHCP client packet information with the switch's relay information. This is the default setting.

Example: Keep the client's DHCP information.

```
# config t
(config)# ip dhcp relay information policy keep
```

Negation: (config)# no ip dhcp relay information policy

(config)# ip dhcp snooping

Syntax: (config)# ip dhcp snooping

Explanation: Enable DHCP snooping function globally. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.

Example: Enable DHCP snooping function.

```
# config t
(config)# ip dhcp snooping
```

Negation: (config)# no ip dhcp snooping

Show: >show ipdhcpsnooping [interface(<port_type>[<in_port_list>])]

#show ip dhcp snooping [interface (<port_type>[<in_port_list>])]

show ip dhcp snooping table

Clear: # clear ip dhcp snooping statistics [interface (<port_type> [<in_port_list>])]

(config)# ip dns proxy

Syntax: (config)# ip dns proxy

Explanation: Enable DNS (Domain Name System) proxy function.

function

```
# config t
(config)# ip dns proxy
```

Negation: (config)# no ip dns proxy

(config)# ip helper-address

Syntax: (config)# ip helper-address <v_ipv4_ucast>

Explanation: Configure DHCP Relay server IPv4address.

Parameters:

<v_ipv4_ucast>: Specify DHCP Relay server IPv4 address that is used by the switch's DHCP relay agent

Negation: (config)# no ip helper-address

(config)# ip http secure-server

Syntax: (config)# ip http secure-server

Explanation: Enablethe HTTPS operation mode. When thecurrentconnection isHTTPS and HTTPS modeoperation is disabled, web browser will automatically redirect to an HTTP connection.

Example: Enable the HTTPS operation mode.

```
# config t
(config)# ip http secure-server
```

Negation: (config)# no ip http secure-server

Show: # show ip http server secure status

(config)# ip http secure-redirect

Syntax: (config)# ip http secure-redirect

Explanation: Enable the HTTPS redirect mode operation. It applies only if HTTPS mode is "Enabled". Automatically redirects HTTP ofweb browserto an HTTPS connection when both HTTPS mode andAutomatic Redirect are enabled.

Example: Enable HTTPs automatic redirect mode.

```
# config t
(config)# ip http secure-redirect
```

Negation: (config)# no ip http secure-redirect

Show: # show ip http server secure status

(config)# ip igmp host-proxy

Syntax: (config)# ip igmp host-proxy [leave-proxy]

Explanation: When enabled, the switch suppresses leave messages unless received from the last member port in

the group. IGMP leave proxy suppresses all unnecessary IGMP leave messages so that a non-querier switch forwards an IGMP leave packet only when the last dynamic member port leaves a multicast group.

Parameters:

[leave-proxy]: The parameter is optional. Enable leave-proxy function.

Negation: (config)# no ip igmp host-proxy [leave-proxy]

Show: # show ip igmp snooping detail

(config)# ip igmp snooping

Syntax: (config)# ip igmp snooping

Explanation: Globally enable IGMP Snooping feature. When enabled, this device will monitor network traffic and determine which hosts will receive multicast traffic. The switch can passively monitor or snoop on IGMP Query and Report packets transferred between IP multicast routers and IP multicast service subscribers to identify the multicast group members. The switch simply monitors the IGMP packets passing through it, picks out the group registration information and configures the multicast filters accordingly.

Negation: (config)# no ip igmp snooping

Show: # show ipigmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

Clear: # clear ip igmp snooping [vlan <v_vlan_list>] statistics

(config)# ip igmp snooping vlan

Syntax: (config)# ipigmpsnooping vlan<v_vlan_list>

Explanation: Enable IGMP function for specific VLANs.

Parameters:

<v_vlan_list>: Specify valid IGMP VLANs.

Negation: (config)# no ip igmp snooping vlan [<v_vlan_list>]

Show: # show ip igmp snooping

Clear: # clear ip igmp snooping [vlan <v_vlan_list>] statistics

(config)# ip igmpssm-range

Syntax: (config)# ip igmp ssm-range <v_ipv4_mcast> <ipv4_prefix_length>

Explanation: SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

Parameters:

<v_ipv4_mcast>: Specify valid IPv4 multicast address.

<ipv4_prefix_length>: Specify the prefix length ranging from 4 to 32.

Negation: (config)# no ip igmp ssm-range

(config)# ip igmp unknown-flooding

Syntax: (config)# ip igmp unknown-flooding

Explanation: Set forwarding mode for unregistered (not-joined) IP multicast traffic. Select the checkbox to flood traffic.

Negation: (config)# no ip igmp unknown-flooding

(config)# ip name-server

Syntax: (config)# ip name-server { <v_ipv4_ucast> | dhcp [interface vlan <v_vlan_id>] }

Explanation: Set up DNS IP address manually or obtain DNS IP address via specific VLAN DHCP server.

Parameters:

<v_ipv4_ucast>: Manually specify unicast IPv4 name server address.

dhcp [interface vlan <v_vlan_id>]: Configure DNS IP address via specific VLAN DHCP server.

Negation: (config)# no ip name-server

Show: >showip name-server

show ip name-server

(config)# ip route

Syntax: (config)# ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>

Explanation: Configure a static IP route.

Parameters:

<v_ipv4_addr>: Specify IPv4 address. The IP route is the destination IP network or host address of this route. Valid format is dotted decimal notation.

<v_ipv4_netmask>: The route mask is a destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Only a default route will have a mask length of 0 (as it will match anything).

<v_ipv4_gw>: This is the IP address of the gateway. Valid format is dotted decimal notation. Gateway and Network must be of the same type.

Example: Add a new ip route with the following settings.

```
# config t
(config)# ip route 192.168.1.240 255.255.255.0 192.168.1.254
```

Negation: (config)# no ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>

Show: >show ip route # show ip route

(config)# ip routing

Syntax: (config)# ip routing

Explanation: Enable IPv4 and IPv6 routing.

Example: Enable IPv4 and IPv6 routing.

```
# config t
(config)# ip routing
```

Negation: (config)# no ip routing

Show: >show ip route

> show ipv6 route [interface vlan <vlan_list>] # show ip route

show ipv6 route [interface vlan<vlan_list>]

```
# show ip route
127.0.0.1 /32 via 127.0.0.1 <UP HOST>
224.0.0.0/4 via 127.0.0.1 <UP>
# show ipv6 route interface vlan 1
::1/128 via ::1 <UP HOST>
```

(config)# ip source binding interface

Syntax: (config)# ip source binding interface <port_type> <in_port_type_id> <vlan_var> <ipv4_var> <mask_var>

Explanation: Create a static entry.

Parameters:

<port_type> <in_port_type_id>: Specify a port type and port number to which a static entry is bound.

<vlan_var>: Specify VLAN ID that has been configured.

<ipv4_var>: Specify a valid IPv4 address.

<mask_var>: Specify the subnet mask for the entered IP address.

Negation: (config)# no ip source binding interface <port_type> <in_port_type_id> <vlan_var> <ipv4_var> <mask_var>

Show: # show ip source binding [dhcp-snooping | static] [interface (<port_type> [<in_port_type_list>])]

```
# config t
```

(config)# ip ssh

Syntax: (config)# ip ssh **Explanation:** Enable SSH mode. **Example:** Enable SSH mode.

Negation: (config)# no ip ssh

Show: # show ip ssh

```
# config t
```

NOTE: SSHis preferred to Telnet, unless the management network is trusted. Telnet passes authentication credentials in plain text, making those credentials susceptible to packet capture and analysis. SSH provides a secure authentication method. TheSSHinthis device uses version 2 ofSSHprotocol.

(config)# ip verify source

Syntax: (config)# ip verify source Explanation: Enable IP source guard function. Negation: (config)# no ip verify source Show:>show ip verifysource [interface(<port_type>[<in_port_type_list>])] # show ip verify source [interface (<port_type> [<in_port_type_list>])]

(config)# ip verify source translate

Syntax: (config)# ip verify source translate

Explanation: Translate Dynamic entries to Static ones.

(config-if)# ip arp inspection check-vlan

Syntax: (config-if)# ip arp inspection check-vlan

Explanation: Enable check vlan function.

Negation: (config-if)# no ip arp inspection check-vlan

(config-if)# ip arp inspection logging

Syntax: (config-if)# ip arp inspection logging { deny | permit | all }

Explanation: Enable log function on a specific interface.

Parameters:

{ deny | permit | all }: Specify one of the log types.

Deny: Log denied entries. **Permit:** Log permitted entries. **All**: Log all entries.

Negation: (config-if)# no ip arp inspection logging

(config-if)# ip arp inspection trust

Syntax: (config-if)# ip arp inspection trust

Explanation: Enable trust state on the selected interfaces.

Negation: (config-if)# no ip arp inspection trust

(config-if)# ip dhcp snooping trust

Syntax: (config-if)# ip dhcp snooping trust

Explanation: Set this interface to DHCP Snooping trusted port.

Negation: (config-if)# no ip dhcp snooping trust

Show: >show ipdhcp snooping [interface(<port_type>[<in_port_list>])] # show ip dhcp snooping [interface

(<port_type> [<in_port_list>])]

(config-if)# ip igmp snooping filter

Syntax: (config-if)# ip igmp snooping filter <profile_name>

Explanation: Use this command to filter specific multicast traffic on a per port basis.

Parameters:

<profile_name>: Specify the configured multicast groups that are denied on a port. When a certain multicast group is selected on a port, IGMP join reports received on a port are dropped.

Negation: (config-if)# no ip igmp snooping filter

Show: > show ipigmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

show ipigmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

(config-if)# ip igmp snooping immediate-leave

Syntax: (config-if)# ip igmp snooping immediate-leave

Explanation: Enable fast leave function on a specific port. When a leave packet is received, the switch immediately removes it from a multicast service without sending an IGMP group-specific (GS) queryto that interface.

Negation: (config-if)# no ip igmp snooping immediate-leave

Show: > show ipigmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

show ipigmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

(config-if)# ip igmp snooping max-groups

Syntax: (config-if)# ip igmp snooping max-groups <throttling>

Explanation: Specify the maximum number of multicast groups that a port can join at the same time.

Parameters:

<throttling>: This field limits the maximum number of multicast groups that a port can join at the same time. When the maximum number is reached on a port, any new IGMP join reports will be dropped. By default, unlimited is selected. The allowed range can be specified is 1 to 10.

Negation: (config-if)# no ip igmp snooping max-groups

Show: > show ipigmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

show ipigmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

(config-if)# ip igmp snooping mrouter

Syntax: (config-if)# ip igmp snooping mrouter

Explanation: Set this interface to Router port. If IGMP snooping cannot locate the IGMP querier, you can

manually designate a port which is connected to a known IGMP querier (i.e., a multicast router/switch). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

Negation: (config-if)# no ip igmp snooping mrouter

Show:>show ip igmp snooping mrouter [detail] # show ip igmp snooping mrouter [detail]

(config-if)# ip verify source

Syntax: (config-if)# ip verify source

Explanation: Enable IP Source Guard on this interface

Negation: (config-if)# no ip verify source

Show:>show ipverifysource [interface(<port_type>[<in_port_type_list>])] # show ip verify source [interface (<port_type> [<in_port_type_list>])]

(config-if)# ip verify source limit

Syntax: (config-if)# ip verify source limit <0-2>

Explanation: Specify the maximum number of dynamic clients that can be learned on a port. The available options are 0, 1, 2. If the port mode is enabled and the maximum number of dynamic clients is equal 0, the switch will only forward IP packets that are matched in static entries for a given port.

Parameters:

<0-2>: Specify the maximum number of dynamic clients that can be learned on a port.

Negation: (config-if)# no ip verify source limit

Show:>show ipverifysource [interface(<port_type>[<in_port_type_list>])] # show ip verify source [interface (<port_type> [<in_port_type_list>])]

(config-if-vlan)# ip address

Syntax: (config-if-vlan)# ip address { { <address> <netmask> } | { dhcp [fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]] } } **Explanation:** Configure IPv4 address for this VLAN interface. **Parameters:**

<address> <netmask>: Specify IPv4 address and subnet mask.

dhcp [fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]]: Use DHCP server to automatically assign IP address.

fallback <fallback_address> <fallback_netmask>: specify Fallback IP address and subnet mask.

timeout <fallback_timeout>: Specify Fallback timeout value.

Negation: (config-if-vlan)# no ip address

Show: > show ip interface brief # show ip interface brief

(config-if-vlan)# ip igmp snooping

Syntax: (config-if-vlan)# ip igmp snooping

Explanation: Eanble IGMP Snooping on this specific VLAN.

Negation: (config-if-vlan)# no ip igmp snooping

Show: >show ip statistics[system][interfacevlan<v_vlan_list>][icmp][icmp-msg <type>] # show ip statistics [system] [interface vlan<v_vlan_list>] [icmp] [icmp-msg <type>]

(config-if-vlan)# ip igmp snooping compatibility

Syntax: (config-if-vlan)# ip igmp snooping compatibility { auto | v1 | v2 | v3 }

Explanation: Configure IGMP Snooping version used for this specific VLAN.

Parameters:

{ auto |v1 | v2 | v3}: Specify one ofthe IGMP Snooping options. **auto:** Compatible withVersion 1, Version 2, and Version 3. **v1:** Compatible with IGMP version 1.

v2: Compatible with IGMP version 2.

v3: Compatible with IGMP version 3.

Negation: (config-if-vlan)# no ip igmp snooping compatibility

(config-if-vlan)# ipigmp snooping last-member-query-interval

Syntax: (config-if-vlan)# ip igmp snooping last-member-query-interval <ipmc_lmqi>

Explanation: LMQI stands for Last Member Query Interval and is to configure the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The allowed range is 0~31744 tenths of a second.

Parameters:

<ipmc_lmqi: 0-31744>: Specify LMQI (Last Member Query Interval) value.

Negation: (config-if-vlan)# no ip igmp snooping last-member-query-interval

(config-if-vlan)# ip igmp snooping priority

Syntax: (config-if-vlan)# ip igmp snooping priority <cos_priority>

Explanation: Specify the priority for transmitting IGMP/MLD control frames. By default, priority is set to 0. Allowed priority values is 0 -7.

Parameters:

<cos_priority: 0-7>: Specify COS for this specific VLAN. The valid range is 0 to 7.

Negation: (config-if-vlan)# no ip igmp snooping priority

(config-if-vlan)# ip igmp snooping querier address

Syntax: (config-if-vlan)# ip igmp snooping querier address <v_ipv4_ucast>

Explanation: Specify IGMP Snooping querier IP address.

Parameters:

<v_ipv4_ucast>: Specify IGMP Snooping querier unicast IP address.

Negation: (config-if-vlan)# no ip igmp snooping querier address

(config-if-vlan)# ip igmp snooping querier election

Syntax: (config-if-vlan)# ip igmp snooping querier election

Explanation: Enable IGMP Snooping querier election function.

Negation: (config-if-vlan)# no ipigmp snooping querier election

(config-if-vlan)# ip igmp snooping query-interval

Syntax: (config-if-vlan)# ip igmp snooping query-interval <ipmc_qi>

Explanation: Specify IPMC Query interval value.

Parameters:

<ipmc_qi: 1-31744>: Specify IPMC Query interval value. The valid value is 1~31744.

Negation: (config-if-vlan)# no ip igmp snooping query-interval

(config-if-vlan)# ipigmp snooping query-max-response-time

Syntax: (config-if-vlan)# ip igmp snooping query-max-response-time <ipmc_qri>

Explanation: Specify IPMC Query Response time value.

Parameters:

<ipmc_qri>: Specify IPMC Query Response time value. The valid value is 1~31744.

Negation: (config-if-vlan)# no ip igmp snooping query-max-response-time

(config-if-vlan)# ip igmp snooping robustness-variable

Syntax: (config-if-vlan)# ip igmp snooping robustness-variable <ipmc_rv>

Explanation: The robustness variable (RV) allows tuning for the expected packet loss on a subnet. If a subnet is susceptible to packet loss, this value can be increased. The RV value must not be zero and should not be one. The value should be 2 or greater. By default, it is set to 2.

Parameters:

<ipmc_rv: 1-255>: Specify IPMC Robustness Variable value. The valid value is 1~255.

Negation: (config-if-vlan)# no ip igmp snooping robustness-variable

(config-if-vlan)# ipigmp snooping unsolicited-report-interval

Syntax: (config-if-vlan)# ip igmp snooping unsolicited-report-interval <ipmc_uri>

Explanation: The Unsolicited Report Interval is the amount of time that the upstream interface should transmit unsolicited IGMP reports when report suppression/proxy reporting is enabled. The allowed range for URI is 0 -31744 seconds.

Parameters:

<ipmc_uri: 0-31744>: Specify Unsolicited Report Interval value. The valid value is 0~31744.

Negation: (config-if-vlan)# no ip igmp snooping unsolicited-report-interval

(config-if-vlan)# ipv6 address

Syntax: (config-if-vlan)# ipv6 address <subnet>

Explanation: Configure IPv6 address for this VLAN interface.

Parameters:

<subnet>: Specify IPv6 address in x:x:x:x::x/<0-128> format.

Negation: (config-if-vlan)# no ipv6 address [<ipv6_subnet>]

Show: >show ip interface brief

>show ipv6 interface [vlan <v_vlan_list> { brief | statistics }] # show ip interface brief

show ipv6 interface [vlan <v_vlan_list> { brief | statistics }]

(config-if-vlan)# ipv6 mld snooping

Syntax: (config-if-vlan)# ipv6 mld snooping

Explanation: Eanble MLD (Multicast Listener Discovery) Snooping on this specific VLAN.

Negation: (config-if-vlan)# no ipv6 mld snooping

Show: >show ipv6 statistics[system][interfacevlan<v_vlan_list>][icmp][icmp-msg <type>] #show ipv6 statistics[system][interface vlan <v_vlan_list>][icmp] [icmp-msg <type>]

(config-if-vlan)# ipv6 mld snooping compatibility

Syntax: (config-if-vlan)#ipv6mldsnooping compatibility{auto|v1 |v2 }

Explanation: Configure MLD Snooping version used for this specific VLAN.

Parameters:

{ auto | v1 | v2 | v3 }: Specify one of the MLD Snooping options.

auto: Compatible with Version 1, Version 2.

v1: Compatible with MLD version 1.

v2: Compatible with MLD version 2.

Negation: (config-if-vlan)# no ipv6 mld snooping compatibility

(config-if-vlan)# ipv6 mld snooping last-member-query-interval

Syntax: (config-if-vlan)# ipv6 mld snooping last-member-query-interval <ipmc_lmqi>

Explanation: LMQI stands for Last Member Query Interval and is to configure the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The allowed range is 0~31744 tenths of a second.

Parameters:

<ipmc_lmqi: 0-31744>: Specify LMQI (Last Member Query Interval) value.

Negation: (config-if-vlan)# no ipv6 mld snooping last-member-query-interval

(config-if-vlan)# ipv6 mld snooping priority <cos_priority>

Syntax: (config-if-vlan)# ipv6 mld snooping priority <cos_priority>

Explanation: Specify the priority for transmitting IGMP/MLD control frames. By default, priority is set to 0. Allowed priority values is 0 -7.

Parameters:

<cos_priority: 0-7>: Specify COS for this specific VLAN. The valid range is 0 to 7.

Negation: (config-if-vlan)# no ipv6 mld snooping priority

(config-if-vlan)# ipv6 mld snooping querier election

Syntax: (config-if-vlan)# ipv6 mld snooping querier election

Explanation: Enable MLD Snooping querier election function.

Negation: (config-if-vlan)# no ipv6 mld snooping querier election

(config-if-vlan)# ipv6 mld snooping query-interval <ipmc_qi>

Syntax: (config-if-vlan)# ipv6 mld snooping query-interval <ipmc_qi>

Explanation: Specify MLD Query interval value.

Parameters:

<ipmc_qi: 1-31744>: Specify IPMC Query interval value. The valid value is 1~31744.

Negation: (config-if-vlan)# no ipv6 mld snooping query-interval

(config-if-vlan)# ipv6 mldsnooping query-max-response-time <ipmc_qri>

Syntax: (config-if-vlan)# ipv6 mld snooping query-max-response-time <ipmc_qri>

Explanation: Specify MLD Query Response time value.

Parameters:

<ipmc_qri>: Specify MLD Query Response time value. The valid value is 1~31744.

Negation: (config-if-vlan)# no ipv6 mld snooping query-max-response-time

(config-if-vlan)# ipv6 mld snooping robustness-variable <ipmc_rv>

Syntax: (config-if-vlan)# ipv6 mld snooping robustness-variable <ipmc_rv>

Explanation: The robustness variable (RV) allows tuning for the expected packet loss on a subnet. If a subnet is susceptible to packet loss, this value can be increased. The RV value must not be zero and should not be one. The value should be 2 or greater. By default, it is set to 2.

Parameters:

<ipmc_rv: 1-255>: Specify IPMC Robustness Variable value. The valid value is 1~255.

Negation: (config-if-vlan)# no ipv6 mld snooping robustness-variable

(config-if-vlan)# ipv6 mldsnooping unsolicited-report-interval <ipmc_uri>

Syntax: (config-if-vlan)# ipv6 mld snooping unsolicited-report-interval <ipmc_uri>

Explanation: The Unsolicited Report Interval is the amount of time that the upstream interface should transmit unsolicited IGMP reports when report suppression proxy reporting is enabled. The allowed range for URI is 0 -31744 seconds.

Parameters:

<ipmc_uri: 0-31744>: Specify Unsolicited Report Interval value. The valid value is 0~31744.

Negation: (config-if-vlan)# no ipv6 mld snooping unsolicited-report-interval

2.9.19 (config)# ipmc

(config)# ipmc profile

Syntax: (config)# ipmc profile

Explanation: Enable IPMC (IP multicast) profile globally.

Negation: (config)# no ipmc profile

Show: # show ipmc profile

(config)# ipmc profile <profile_name>

Syntax: (config)# ipmc profile <profile_name>

Parameters:

<profile_name: word16>: Specify the desired profile name in 16 characters. When entered is pressed, the command will change to (config-ipmc-profile)#.

Explanation: Set up an IPMC profile.

Example: Create an IPMC profile named "goldpass".

```
# config t
(config)# ipmc profile goldpass
(config-ipmc-profile)#
```

Negation: (config)# no ipmc profile <profile_name>

Show: # show ipmc profile [<profile_name>] [detail]

(config)# ipmc range

Syntax: (config)# ipmc range <entry_name> { <v_ipv4_mcast> [<v_ipv4_mcast_1>] | <v_ipv6_mcast> [<v_ipv6_mcast_1>] }

Explanation: Specify the multicast IP range. The available IP range is from 224.0.0.0~239.255.255.255.

Parameters:

<entry_name>: The name used in specifying the address range.

{ <v_ipv4_mcast> [<v_ipv4_mcast_1>] | <v_ipv6_mcast> [<v_ipv6_mcast_1>] }: Specify the multicast IP range. The available IP range is from 224.0.0.0~239.255.255.255.

Negation: (config)# no no ipmc range <entry_name>

Show: # show ipmc profile [<profile_name>] [detail]

(config-ipmc-profile)# default range

Syntax: (config-ipmc-profile)# default range <entry_name>

Parameters:

<entry_name: word16>: Specify an entry name in 16 characters for this IPMC profile.

Explanation: To set default IPMC Profile Rule for a specific IPMC Profile.

Example: To default IPMC Profile Rule (Entry 1) for specific IPMC Profile.

```
# config t
(config)# ipmc profile goldpass
(config-ipmc-profile)# default range 1
```

Negation: (config-ipmc-profile)# no range <entry_name>

Show: # show ipmc profile

#show ipmc profile [<profile_name>] [detail]

(config-ipmc-profile)# description

Syntax: (config-ipmc-profile)# description <profile_desc>

Parameters:

<profile_desc: line 64>: Additional description for the designated profile in 64 characters.

Explanation: Specify descriptive information for the designated profile.

Example: Provide descriptive information for IPMC profile goldpass.

```
# config t
(config)# ipmc profile goldpass
(config-ipmc-profile)# description 1stclasscustomer
```

Negation: (config-ipmc-profile)# no description

Show: # show ipmc profile

#show ipmc profile [<profile_name>] [detail]

(config-ipmc-profile)# range

Syntax: (config-ipmc-profile)# range <entry_name> { permit | deny } [log] [next <next_entry>]

Parameters:

<entry_name>: Specify an entry name.

{ permit | deny }: Specify the action taken upon receiving the Join/Report frame that has the group address matches the address range of the rule.

Permit: Group address matches the range specified in the rule will be learned.

Deny: Group address matches the range specified in the rule will be dropped. [log]: Log when matching
[next <next_entry>]: Specify next entry used in profile

Explanation: To set action of an entry for a specific IPMC profile.

Negation: (config-ipmc-profile)# no range<entry_name>

Show: # show ipmc profile

#show ipmc profile [<profile_name>] [detail]

2.9.20 (config)# ipv6 mldhost-proxy

(config)# ipv6 mldhost-proxy

Syntax: (config)# ipv6 mldhost-proxy

Explanation: Enable IPv6 MLD proxy. When MLD proxy is enabled, the switch exchanges MLD messages with the router on its upstream interface, and performs the host portion of the MLD task on the upstream interface as follows:

When queried, it sends multicast listener reports to the group.

When a host joins a multicast group to which no other host belongs, it sends unsolicited multicast listener reports to that group.

When the last host in a particular multicast group leaves, it sends an unsolicited multicast listener done report to the all-routers address (FF02::2) for MLDv1.

Example: Enable IPv6 MLD Proxy.

```
# config t
(config)# ipv6 mld host-proxy
(config)#
```

Negation: (config)# no ipv6 mldhost-proxy

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type>

[<v_port_type_list>])] [sfm-information]] [detail]

show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

(config)# ipv6 mld host-proxy leave-proxy

Syntax: (config)# ipv6 mld host-proxy leave-proxy

Explanation: Enable IPv6 MLD leave proxy. To prevent multicast router from becoming overloaded with leave messages, MLD snooping suppresses leave messages unless received from the last member port in the group. When the switch acts as the querier, the leave proxy feature will not function.

Example: Enable IPv6 MLD leave proxy.

```
# config t
(config)# ipv6 mld host-proxy leave-proxy
(config)#
```

Negation: (config)# no ipv6 mld host-proxy leave-proxy

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type>

[<v_port_type_list>])] [sfm-information]] [detail]

show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

(config)# ipv6 mld snooping

Syntax: (config)# ipv6 mld snooping

Explanation: Enable MLD Snooping feature globally. When enabled, this device will monitor network traffic and determine which hosts would like to receive multicast traffic. The switch can passively monitor or snoop on MLD Listener Query and Report packets transferred between IP multicast routers and IP multicast service subscribers to identify the multicast group members. The switch simply monitors the IGMP packets passing through it, picks out the group registration information and configures the multicast filters accordingly.

Example: Enable IPv6 MLD snooping.

```
# config t
(config)# ipv6 mld snooping
(config)#
```

Negation: (config)# no ipv6 mld snooping

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type>

[<v_port_type_list>])] [sfm-information]] [detail]

show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

(config)# ipv6 mld snooping vlan

Syntax: (config)# ipv6 mld snooping vlan <v_vlan_list>

Parameters:

<v_vlan_list>: Specify VLAN ID for MLD.

Negation: (config)# no ipv6 mld snooping vlan [<v_vlan_list>]

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type>
[<v_port_type_list>])] [sfm-information]] [detail]

> show ipv6 mld snooping mrouter [detail]

show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

show ipv6 mld snooping mrouter [detail]

Clear: # clear ipv6 mld snooping [vlan <v_vlan_list>] statistics

(config)# ipv6 mld ssm-range

Syntax: (config)# ipv6 mld ssm-range <v_ipv6_mcast> <ipv6_prefix_length>

Parameters:

<v_ipv6_mcast>: Specify valid IPv6 mluticast address.

<ipv6_prefix_length>: Specify prefix length range from 8 to 128.

Explanation: Specify SSM (Source-Specific Multicast) Range. This setting allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

Example: Configure MLD SSM with the ff3e::7728/128 settings.

```
# config t
 (config)# ipv6 mld ssm-range ff3e::7728  128
```

Negation: (config)# no ipv6 mld ssm-range

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type>

[<v_port_type_list>])] [sfm-information]] [detail]

show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

(config)# ipv6 mld unknown-flooding

Syntax: (config)# ipv6 mldunknown-flooding

Explanation: Enable forwarding mode for unregistered (not-joined) IP multicast traffic.

Example: To flood unregistered IPv6 multicast traffic

```
# config t
```

Negation: (config)# no ipv6 mldunknown-flooding

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type>

[<v_port_type_list>])] [sfm-information]] [detail]

> show ipv6 mld snooping mrouter [detail]

show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

show ipv6 mld snooping mrouter [detail]

(config)# ipv6 route

Syntax: (configure)# ipv6 route <v_ipv6_subnet> { <v_ipv6_ucast> |interface vlan <v_vlan_id>

<v_ipv6_addr> }

Parameters:

<v_ipv6_subnet>: Specify IPv6 route address.

{ <v_ipv6_ucast> | interface vlan <v_vlan_id> <v_ipv6_addr> }: Specify one ofthe options. This could be either IPv6 next hop unicast address or an interface.

Explanation: Configure a static IPv6 route.

Negation: (config)# no ipv6 route <v_ipv6_subnet> { <v_ipv6_ucast> |interface vlan <v_vlan_id> <v_ipv6_addr> }

Show: # show ipv6 route [interface vlan <v_vlan_list>]

(config-if)# ipv6 mld snooping filter

Syntax: (config-if)# ipv6 mld snooping filter <profile_name>

Explanation: Use this command to filter specific multicast traffic on a per port basis.

Parameters:

<profile_name>: Specify the configured multicast groups that are denied on a port. When a certain multicast group is selected on a port, IGMP join reports received on a port are dropped.

Negation: (config-if)# no ipv6 mld snooping filter

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type>

[<v_port_type_list>])] [sfm-information]] [detail]

(config-if)# ipv6 mld snooping immediate-leave

Syntax: (config-if)# ipv6 igmp snooping immediate-leave

Explanation: Enable fast leave function on a specific port. When a leave packet is received, the switch immediately removes it from a multicast service without sending an IGMP group-specific (GS) query to that interface.

Negation: (config-if)# no ipv6 mld snooping immediate-leave

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

(config-if)# ipv6 mld snooping max-groups

Syntax: (config-if)# ip igmp snooping max-groups <throttling>

Explanation: Specify the maximum number of multicast groups that a port can join at the same time.

Parameters:

<throttling>: This field limits the maximum number of multicast groups that a port can join at the same time. When the maximum number is reached on a port, any new IGMP join reports will be dropped. By default, unlimited is selected. The allowed range can be specified is 1 to 10.

Negation: (config-if)# no ipv6 mld snooping max-groups

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

3. 9.20.11 (config-if)# ipv6 mld snooping mrouter

Syntax: (config-if)# ipv6 mld snooping mrouter

Explanation: Set this interface to Router port. If IGMP snooping cannot locate the IGMP querier, you can manually designate a port which is connected to a known IGMP querier (i.e., a multicast router/switch). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

Negation: (config-if)# no ipv6 mld snooping mrouter

Show: > show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type>

[<v_port_type_list>])] [sfm-information]] [detail]

> show ipv6 mld snooping mrouter [detail]

show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail]

show ipv6 mld snooping mrouter [detail]

2.9.21(config)# lacp

(config)# lacp system-priority

Syntax: (configure)# lacp system-priority <v_1_to_65535>

Parameters:

<v_1_to_65535>: The priority of the port. The allowed value range is from 1 to 65535.

Explanation: Configure system priority for LACP function. The lower number means greater priority. This priority value controls which ports will be active and which ones will be in a backup role.

Example: Set LACP system priority value to 100.

```
# config t
(config)# lacp system-priority 100
```

Negation: (config)# no lacp system-priority <v_1_to_65535>

Show: # show lacp { internal | statistics | system-id | neighbour }

(config-if)# lacp

Syntax: (config-if)# lacp

Explanation: Enable LACP on this interface.

Example: Enable LACP on port **1.**

```
# config t
(config)# interface GigabitEthernet 1/1
(config-if)# lacp
(config-if)#
```

Negation: (config-if)# no lacp

Show: # show lacp { internal | statistics | system-id | neighbour }

Clear: # clear lacp statistics

(config-if)# lacp key

Syntax: (config-if)# lacp key { <v_1_to_65535> | auto }

Explanation: Configure a LACP key for this interface.

Parameters:

{ <v_1_to_65535> | auto }: Specify a LACP key for this interface. The "auto" setting sets the key as appropriate by the physical link speed. If you want a user-defined key value, enter a value between 1 and 65535. Ports in an aggregated link group must have the same LACP port Key. In order to allow a port to join an aggregated group, the port Key must be set to the same value.

Negation: (config-if)# no lacp key { <v_1_to_65535> | auto }

Show: # show lacp { internal | statistics | system-id | neighbour }

(config-if)# lacp port-priority <v_1_to_65535>

Syntax:(config-if)#lacpport-priority <v_1_to_65535>

Explanation: Configure a LACPkey forthis interface.

Parameters:

<v_1_to_65535>}: Specify a LACP port priority forthis interface. The lower number means greater priority. This priority value controls which ports will be active and which ones will be in a backup role.

Negation: (config-if)# no lacp port-priority <v_1_to_65535>

Show: # show lacp { internal | statistics | system-id | neighbour }

(config-if)# lacp role { active | passive }

Syntax: (config-if)# lacp role { active lpassive } **Explanation:** Configure LACP role for this interface.

Parameters:

{ active | passive }: Specify either "Active" or "Passive" role depending on the device's capability of

negotiating and sending LACP control packets. Ports that are designated as "Active" are able to process and send LACP control frames. Hence, this allows LACP compliant devices to negotiate the aggregated like so that the group may

be changed dynamically as required. In order to add or remove ports from the group, at least one of the participating devices must set to "Active" LACP ports.

Negation: (config-if)# no lacp role { active | passive }

Show: # show lacp { internal | statistics | system-id | neighbour }

(config-if)# lacp timeout { fast | slow }

Syntax: (config-if)# lacp timeout { fast | slow }

Explanation: Configure timeout mode.

Parameters:

{ fast | slow }:TheTimeout controls the period between BPDU transmissions. Fastwilltransmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.

Negation: (config-if)# no lacp timeout { fast | slow }

Show: # show lacp { internal | statistics | system-id | neighbour }

2.9.22 (config)# line

(config)# line

Syntax: (configure)# line { <0~16> | console 0 | vty <0~15> }

Explanation: Enter the specific line. When Enter is pressed, the command line changes to "(config-

line)#" .

Parameters:

{ <0~16> | console 0 | vty <0~15> }: Specify one of the options.

<0~16> : List of line numbers.

console 0: Console line connection.

vty <0~15>: VTY lines are the Virtual Terminal lines of the device, used solely to control inbound Telnet connections. They are virtual, in the sense that they are a function of software - there is no hardware associated with them .

Example: Enter Console 0 mode.

```
# config t
(config)# line console 0
(config-line)#
```

Show:>show line[alive] # show line [alive]

(config-line)# do

Syntax: (config-line)# do <command> **Explanation:** To run EXEC. commands.

Parameters:

<command>: Enter the EXEC. command

Example: Show aaa settings.

```
# config t
(config)# line console 0
(config-line)# do show aaa
console  : local
telnet   : local
ssh      : local
http     : local
(config-line)#
```

3.9.21.3 (config-line)# editing

Syntax: (config-line)# editing

Explanation: Enable command line editing.

Negation: (config-line)# no editing

Show:>show line[alive] # show line [alive]

(config-line)# end

Syntax: (config-line)# end **Explanation:** Return to EXEC. mode. **Example:** Return to EXEC. mode.

```
# config t
(config)# line console 0
(config-line)# end
#
```

(config-line)# exec-banner

Syntax: (config-line)# exec-banner

Explanation: Enable the display of EXEC banner.

Example: Enable the display of EXEC banner.

```
# config t
(config)# line console 0
(config-line)# exec-banner
```

Negation: (config-line)# no exec-banner

Show:>show line[alive] # show line [alive]

(config-line)# exec-timeout

Syntax: (config-line)# exec-timeout <min> [<sec>]

Parameters:

<min>: Specify timeout in minutes. The allowed range is 0 to 1440. [<sec>]: Specify timeout in seconds. The allowed range is 0 to 3600.

Negation: (config-line)# no exec-timeout

Show:>show line[alive] # show line [alive]

(config-line)# exit

Syntax: (config-line)# exit **Explanation:** Return to previous mode. **Example:** Return to previous mode.

```
# config t
(config)# line console 0
(config-line)# exit
```

Example: Enable IPv6 MLD
(config-line)# help

Syntax: (config-line)# help

Explanation: Show the Help explanation.

Example: Show Help explanation.

Example: Enable IPv6 MLD proxy.

```
# config t
(config)# line console 0
(config-line)# help
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
and you want to know what Parameters match the input
    (e.g. 'show pr?'.)
```

(config-line)# history size

Syntax: (config-line)# history size <history_size>

Explanation: Control how many history commands are displayed.

Parameters:

<history_size>: The allowed range is 0 to 32. 0 means "disable".

Example: Set history size to 10.

```
# config t
(config)# line console 0
(config-line)# history size 10
```

Negation: (config-line)# no history size

Show:>show line[alive] # show line [alive]

(config-line)# length

Syntax: (config-line)# length <length>

Explanation: Configure the number of lines displayed on the screen.

Parameters:

<length>: Specify the number of lines displayed on the screen. The allowed range is 3 to 512. Specify "0" for no pausing.

Example: Display 20 lines on the screen.

```
# config t
(config)# line console 0
(config-line)# length 20
(config-line)#
```

Negation: (config-line)# no length

Show:>show line[alive] # show line [alive]

(config-line)# location

Syntax: (config-line)# location <location>

Explanation: Configure the descriptive location of this device.

Parameters:

<location>: Location description for the terminal. The characters allowed are 32.

Example: Configure the location "cabinet5a".

```
# config t
(config)# line console 0
(config-line)# location cabinet5a
(config-line)#
```

Negation: (config-line)# no location

Show:>show line[alive] # show line [alive]

(config-line)# motd-banner

Syntax: (config-line)# motd-banner

Explanation: Enable the display of motd (message of the day) banner.

Example: Enable motd banner.

```
# config t
(config)# line console 0
(config-line)# motd-banner
(config-line)#
```

Negation: (config-line)# no motd-banner

Show:>show line [alive] # show line [alive]

(config-line)# privilege level

Syntax: (config-line)# privilege level <privileged_level> **Explanation**: Configure the privilege level for the terminal line.
Parameters:

<privileged_level>: Privilege level for the terminal line. The allowed range is 0 to 15.

Example: Change the privilege level to 5 for vty 1.

```
# config t
(config)# line vty 1
(config-line)# privilege level 5
(config-line)#
```

Negation: (config-line)# no privilege level

Show:>show line[alive] # show line [alive]

(config-line)#width

Syntax:(config-line)#width<width>

Explanation: Configure the width of the terminal line.

Parameters:

<width>: Specify the width of the terminal line. The allowed range is 40 to 512. Specify "0" for unlimited width.

Example: Change of width of vty 1 to 60.

```
# config t
(config)# line vty 1
(config-line)# width 60
(config-line)#
```

Negation: (config-line)# no width

Show:>show line[alive] # show line [alive]

2.9.23 (config)# lldp

(config)# lldp holdtime

Syntax: (config)# lldp holdtime <val>

Explanation: This setting defines how long LLDP frames are considered valid and is used to compute the TTL. The default is 4.

Parameters:

<val>: Specify the holdtime value. The allowed value is 2 to 10.

Example: Set the holdtime to 5.

```
# config t
(config)# lldp holdtime 5
```

Negation: (config)# no lldp holdtime

(config)# lldp reinit

Syntax: (config)# lldp reinit <val>

Explanation: Configure a delay between the shutdown frame and a new LLDP initialization.

Parameters:

<val>: Specify a value between 1 and 10 (seconds).

Example: Set the LLDP re-initiation value to 3.

```
# config t
(config)# lldp reinit 3
```

Negation: (config)# no lldp reinit

(config)# lldptimer

Syntax: (config)# lldp timer <val>

Explanation: Configure the interval between LLDP frames are sent to its neighbors for updated discovery information. The default is 30 seconds.

Parameters:

<val>: Specify a value between 5 and 32768 (seconds).

Example: Set the LLDP timer value to 35.

```
# config t
(config)# lldp timer 35
```

Negation: (config)# no lldp timer

(config)# lldp transmission-delay

Syntax: (config)# lldp transmission-delay <val>

Parameters:

<val>: Specify a value between 1 and 8192 (seconds).

Explanation: Configure a delay between the LLDP frames that contain changed configurations. Tx Delay cannot be larger than 1/4 of the Tx interval value.

Example: Set the LLDP transmission delay value to 2.

```
# config t
(config)# lldp transmission-delay 2
```

Negation: (config)# no lldp transmission-delay

(config)# lldp meddatum

Syntax: (config)# lldp med datum {wgs84 | nad83-navd88 | nad83-mllw}

Explanation: The Map Datum is used for the coordinates given in above options.

Parameters:

{ wgs84 | nad83-navd88 | nad83-mllw }: Specify one of the options.

WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.

NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).

NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Example: Set the map datum to wgs84.

```
# config t
(config)# lldp med datum wgs84
```

Negation: (config)# no lldp med datum

(config)# lldp medfast

Syntax: (config)# lldp med fast <v_1_to_10>

Explanation: Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy. With this in mind, LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. With Fast start repeat count it is possible to specify the number of times the fast start transmission is repeated. The recommended value is 4 times, giving that 4 LLDP frames with a 1 second interval will be transmitted, when a LLDP frame with new information is received. It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including between Network Connectivity Devices, or to other types of links.

Parameters:

<v_1_to_10>: Specify a valid value between 1 and 10.

Example: Set the value to 5.

```
# config t
(config)# lldp med fast 5
```

Negation: (config)# no lldp med fast

(config)# lldp med location-tlv altitude

Syntax: (config)# lldp med location-tlv altitude { meters | floors } <v_word11>

Explanation: Altitude SHOULD be normalized to within -32767 to 32767 with a maximum of 4 digits. It is possible to select between two altitude types (floors or meters). "meters" means meters of Altitude defined by the vertical datum specified; while, "floors" means altitude in a form more relevant in buildings which have different floor-to-floor dimensions.

Parameters:

{ meters | floors }: Specify one of the options.

<v_word11>: Specify a value for the specified option.

Example: Set the altitude value to "floors 10".

```
          the holdtime to
# config t

(config)# lldp med location-tlv altitude floors 10
```

Negation: (config)# no lldp med location-tlv altitude

(config)# lldp med location-tlv civic-addr

Syntax: (config)# 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 }

<v_string250>

Explanation: Configure civic address information.

Parameters:

{ 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 }: Specify one of the options.

country: The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.

state: National subdivisions (state, canton, region, province, prefecture).

county: County, parish, gun (Japan), district.

city: City, township, shi (Japan) - Example: Copenhagen.

district: City division, borough, city district, ward, chou (Japan).

block: Neighbourhood, block.

street: Street - Example: Poppelvej.

leading-street-direction: Example: N.

trailings-street-suffix: Example: SW.

street-suffix: Ave, Platz.

house-no: Specify housenumber.

house-no-suffix: Example: A, 1/2.

landmark: Landmark or vanity address - Example: Columbia University.

additional-info: Example: South Wing.

Name: Example: Flemming Jahn.

zip-code: Postal/zip code - Example: 2791.

building: Building (structure). Example:Low Library.

apartment: Unit (Apartment, suite). Example: Apt 42.

floor: Example: 4.

room-number: Room number - Example: 450F.

place-type: Example: Office.

postal-community-name: Example: Leonia.

p-o-box: Example: 12345.

additional code: Example: 1320300003.

Example: Set the country code to "UK".

```
the holdtime to
# config t
(config)# lldp med location-tlv civic-addr country UK
```

Negation: (config)# no lldpmedlocation-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 }

(config)# lldp med location-tlv elin-addr

Syntax: (config)# lldp med location-tlv elin-addr <v_word25>

Explanation: Configure a value for Emergency Location Information.

Parameters:

<v_word25>: A value for Emergency Location Information (ELIN).

Example: Set the emergency location information to "911".

```
# config t
(config)# lldp med location-tlv elin-addr 911
```

Negation: (config)# no lldp med location-tlv elin-addr

(config)# lldp med location-tlv latitude

Syntax: (config)# lldp med location-tlv latitude { north | south } <v_word8>

Explanation: Configure a value for latitude. Latitude value should be between 0 and 90.

Parameters:

{ north | south }: Specify one of the options, either north or south.

<v_word8>: Specify latitude value for the selected option.

Example: Set the north latitude to 5.

```
# config t
(config)# lldp med location-tlv latitude north 5
```

Negation: (config)# no lldp med location-tlv latitude

(config)# lldp med location-tlv longitude

Syntax: (config)# lldp med location-tlv longitude { west | east } <v_word9>

Explanation: Configure a value for longitude. Longitude value should be between 0 and 180.

Parameters:

{ west | east }: Specify one of the options, either west or east.

<v_word9>: Specify longitude value for the selected option.

Example: Set the west longitude to 90.
Example: Setthe holdtime to5.

```
# config t
(config)# lldp med location-tlv longitude west 90
```

Negation: (config)# no lldp med location-tlv longitude

(config)# lldp med media-vlan-policy

Syntax: (config)# lldp med media-vlan-policy <policy_index> { voice | voice-signaling | guest-voice-signaling | guest-voice | softphone-voice | video-conferencing | streaming-video | video-signaling } { tagged <v_vlan_id> | untagged } [l2-priority <v_0_to_7>] [dscp <v_0_to_63>]

Explanation: Configure a LLDP MED policy ID for a service.

Parameters:

<policy_index>: Specify a policy ID. The valid range is from 0 to 31.

{ voice | voice-signaling | guest-voice-signaling | guest-voice | softphone-voice | video-conferencing | streaming- video | video-signaling }: Specify one of the services for this policy ID.

{ tagged <v_vlan_id> | untagged }: Specify whether this service is tagged or untagged. When "tagged" is specified, a VLAN ID should be provided.

[l2-priority <v_0_to_7>]: Specify a value for L2 priority. The valid value is from 0 to 7. [dscp <v_0_to_63>]: Specify a value for DSCP. The valid value is from 0 to 63.

Example: Create a policy ID 1 for tagged Voice VLAN.

```
# config t
(config)# lldp med media-vlan-policy 1 voice tagged 100 l2-priority 7 DSCP 63
```

Negation: (config)# no lldp med media-vlan-policy <policies_list>

Show: > show lldp med media-vlan-policy [<v_0_to_31>]

show lldp med media-vlan-policy [<v_0_to_31>]

(config-if)# lldp cdp-aware

Syntax: (config-if)# lldp cdp-aware

Explanation: Configures if the interface shall be CDP aware (CDP discovery information is added to the LLDP neighbor table).

Example: Setthe holdtime to5.

Example: Set interface 1 to CDP aware.

```
# config t
(config)# interface GigabitEthernet 1/1
(config-if)# lldp cdp-aware
```

Negation: (config-if)# no lldp cdp-aware

Show: > show lldp neighbors [interface (<port_type> [<v_port_type_list>])] # show lldp neighbors [interface (<port_type> [<v_port_type_list>])]

(config-if)# lldp med media-vlan policy-list

Syntax: (config-if)# lldp med media-vlan policy-list <v_range_list>

Explanation: To apply MED Media-VLAN policy of LLDP on this interface.

Parameters:

<v_range_list>: Assign a policy to this interface.

Negation: (config-if)# no lldp med media-vlan policy-list <v_range_list>

Show: >show lldpmed media-vlan-policy [<v_0_to_31>] # show lldp med media-vlan-policy [<v_0_to_31>]

(config-if)# lldp medtransmit-tlv

Syntax: (config-if)# lldp med transmit-tlv [capabilities] [location] [network-policy]

Explanation: To configure LLDP-MED TLV Type for specific interface.

Parameters:

[capabilities]: Enable transmission ofthe optional capabilities TLV. [location]: Enable transmission ofthe optional location TLV.

[network-policy]: Enable transmission of the optional network policy TLV.

Negation: (config-if)# no lldp med transmit-tlv [capabilities] [location] [network-policy]

Show: >show lldpmed media-vlan-policy [<v_0_to_31>] # show lldp med media-vlan-policy [<v_0_to_31>]

(config-if)# lldp receive

Syntax: (config-if)# lldp receive

Explanation: The switch will analyze LLDP information received from neighbours.

Negation: (config-if)# no lldp receive

Show: > show lldp statistics [interface (<port_type> [<v_port_type_list>])] # show lldp statistics[interface (<port_type>[<v_port_type_list>])]

(config-if)# lldptlv-select

Syntax: (config-if)# lldptlv-select { management-address | port-description | system-capabilities | system-description

| system-name }

Explanation: To configure LLDP-MED TLV attributes for specific interface.

Parameters:

{ management-address | port-description | system-capabilities | system-description | system-name }: Specify a LLDP TLV attribute. LLDP uses several attributes to discover neighbour devices. These attributes contains type, length, and value descriptions and are referred to TLVs. Details such as port description, system name, system description, system capabilities, management address can be sent from this device.

Negation: (config-if)# no lldptlv-select { management-address | port-description | system-capabilities | system-description | system-name }

Show: > show lldp neighbors [interface (<port_type> [<v_port_type_list>])] #show lldp neighbors [interface (<port_type> [<v_port_type_list>])]

(config-if)# lldp transmit

Syntax: (config-if)# lldp transmit

Explanation: To configure LLDP Tx only mode for specific interface

Negation: (config-if)# no lldp transmit

Show: # show lldp statistics [interface (<port_type> [<v_port_type_list>])]

2.9.24 (config)# logging

(config)# logging on

Syntax: (config)# logging on

Explanation: This sets the server mode operation. When the mode of operation is enabled (on), the syslog message will send out to syslog server (at the server address). The syslog protocol is based on UDP communication and received on UDP port 514. Syslog server will not send acknowledgments back to the sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out, even if the syslog server does not exist. When the mode of operation is disabled, no syslog packets are sent out.

Example: Enable log server operation.

```
# config t
 (config)# logging on
```

Negation: (config)# no logging on

Show: # show logging

Clear: # clear logging [info] [warning] [error] [switch <switch_list>]

(config)# logging host

Syntax: (config)# logging host { <v_ipv4_ucast> | <v_word45> }

Parameters:

{ <hostname> | <ipv4_ucast> }: Specify one of the options. The hostname is the domain name of the log server; while the latter is IPv4 address of the log server.

Explanation: Configure log server address.

Example: Use IPv4 address to configure log server.

```
# config t
 (config)# logging host 192.168.1.253
```

Negation: (config)# no logging host

Show: # show logging

show logging <logging_id: 1-4294967295> # show logging [info] [warning] [error]

(config)# logging level

Syntax: (config)# logging level { info | warning | error }

Explanation: Configure what kind of messages will send to syslog server.

Parameters:

{ info | warning | error }: Specify one of the log message options.

Info: Send information, warnings and errors.

Warning: Send warnings and errors.

Error: Send errors only.

Example: Send error messages to log server.

```
# config t
 (config)# logging level error
```

Show: # show logging

show logging <logging_id: 1-4294967295> # show logging [info] [warning] [error]

2.9.25 (config)# loop-protect

(config)# loop-protect

Syntax: (config)# loop-protect

Explanation: Enable loop protection function.

Example: Enable loop protection function.

```
# config t
 (config)# loop-protect
```

Negation: (config)# no loop-protect

Show: # show loop-protect [interface (<port_type> [<plist>])]

(config)# loop-protect shutdown-time

Syntax: (config)# loop-protect shutdown-time <t>

Explanation: Configure the period for which a port will be kept disabled.

Parameters:

<t: 0-604800>: Specify a shutdown time value. The valid values are from 0 to 604800 seconds. 0 means that a port is kept disabled until next device restart.

Example: Set the shutdown time value to 180 seconds.

```
# config t
(config)# loop-protect shutdown-time 180
```

Negation: (config)# no loop-protect shutdown-time

Show: # show loop-protect [interface (<port_type> [<plist>])]

(config)# loop-protect transmit-time

Syntax: (config)# loop-protect transmit-time <t>

Explanation: Configure the interval between each loop protection PDU sent on each port.

Parameters:

<t: 1-10>: Specify a transmit time value. The valid values are from 1 to 10 seconds.

Example: Set the transmit time value to 5 seconds.

```
# config t
(config)# loop-protect transmit-time 5
```

Negation: (config)# no loop-protect transmit-time

Show: # show loop-protect [interface (<port_type> [<plist>])]

(config-if)# loop-protect

Syntax: (config-if)# loop-protect

Explanation: Enable loop protection function on this interface.

Negation: (config-if)# no loop-protect

Show: # show loop-protect [interface (<port_type> [<plist>])]

(config-if)# loop-protect action

Syntax: (config-if)# loop-protect action { [shutdown] [log] }

Explanation: Configure the action taken when loops are detected on a port.

Parameters:

{ [shutdown] [log] }: When a loop is detected on a port, the loop protection will immediately take appropriate actions. Actions will betaken include "Shutdown Port", "Shutdown Port and Log" or "Log Only".

Negation: (config-if)# no loop-protect action

Show: # show loop-protect [interface (<port_type> [<plist>])]

(config-if)# loop-protect tx-mode

Syntax: (config-if)# loop-protect tx-mode

Explanation: Enable a port to actively generate loop protection PDUs.

Negation: (config-if)# no loop-protect tx-mode

Show: # show loop-protect [interface (<port_type> [<plist>])]

2.9.26 (config)# mac

(config)# mac address-table aging-time

Syntax: (config)# mac address-table aging-time <v_0_10_to_1000000>

Explanation: Configure the aging time for a learned MAC to be appeared in MAC learning table.

Parameters:

<v_0_10_to_1000000>: Specify an aging time value for MAC address table. The valid values are from 10 to 1000000 (seconds). Using "0" to disable aging time function.

Example: Set the aging time to 600 seconds.

```
# config t
 (config)# mac address-table aging-time 600
```

Negation: (config)# no mac address-table aging-time

(config)# no mac address-table aging-time <v_0_10_to_1000000>

Show: > show mac address-table [conf | static | aging-time | { { learning | count } [interface

(<port_type>

[<v_port_type_list>])]}|{address<v_mac_addr>[vlan<v_vlan_id>]}| vlan<v_vlan_id_1> |interface

(<port_type> [<v_port_type_list_1>])]

show mac address-table [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>])]}|{address<v_mac_addr>[vlan<v_vlan_id>]} |vlan<v_vlan_id_1> |interface

(<port_type> [<v_port_type_list_1>])]

show mac address-table aging-time

(config)# mac address-table static

Syntax: (config)# mac address-table static <v_mac_addr> vlan <v_vlan_id> interface (<port_type> [<v_port_type_list>])

Explanation: Configure the static MAC address mapping table.

Parameters:

<v_mac_addr>: Specify MAC address in "xx:xx:xx:xx:xx:xx" format. vlan <v_vlan_id>: Specify the VLAN ID for this entry.

interface (<port_type> [<v_port_type_list>]): Specify the interface port type and the port number.

Example: Add a static MAC address "11:11:22:22:33:33" to MAC address table.

```
# config t
 (config)# mac address-table static 11:11:22:22:33:33 vlan 1 interface
GigabitEthernet 1/1-10
```

Negation: (config)#no macaddress-table static<v_mac_addr> vlan<v_vlan_id> interface(<port_type> [<v_port_type_list>])

Show: > show mac address-table [conf | static | aging-time |{ { learning | count } [interface

(<port_type>

[<v_port_type_list>])]}|{address<v_mac_addr>[vlan<v_vlan_id>]} |vlan<v_vlan_id_1> |interface

(<port_type> [<v_port_type_list_1>])]

show mac address-table [conf | static | aging-time |{ { learning | count } [interface (<port_type> [<v_port_type_list>])]}|{address<v_mac_addr>[vlan<v_vlan_id>] }| vlan<v_vlan_id_1> |interface

(<port_type> [<v_port_type_list_1>])]

Clear: # clear mac address-table

(config-if)# macaddress-table learning

Syntax: (config)# mac address-table learning [secure]

Explanation: Set this interface to secure mode.

Parameters:

[secure]: Only static MAC entries listed in "Static MAC Table Configuration" are learned. Others will be dropped.

NOTE: *Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.*

Negation: (config-if)# no mac address-table learning [secure]

Show: > show mac address-table [conf | static | aging-time |{ { learning | count } [interface
(<port_type>

[<v_port_type_list>])]} |{address<v_mac_addr>[vlan<v_vlan_id>]}| vlan<v_vlan_id_1> |interface
(<port_type> [<v_port_type_list_1>])]

show mac address-table [conf | static | aging-time |{ { learning | count } [interface (<port_type> [<v_port_type_list>])]} |{address<v_mac_addr>[vlan<v_vlan_id>]}| vlan<v_vlan_id_1> |interface

(<port_type> [<v_port_type_list_1>])]

Clear: # clear mac address-table

2.9.27 (config-if)# media-type

Syntax: (config-if)# media-type { rj45 | sfp | dual }

Explanation: Configure the media type supported for this specific interface.

Parameters:

{ rj45 | sfp | dual }: The options are RJ-45, SFP, or dual (both RJ-45 & SFP are supported.).

Negation: (config-if)# no media-type

2.9.28 (config-if)# mtu

Syntax: (config-if)# mtu <max_length>

Explanation: Configure the maximum transmission unit for this specific interface.

Parameters:

<max_length: 1518-9600>}: Specify the MTU. The range is 1518 to 9600 bytes.

Negation: (config-if)# no mtu

Show: # show interface (<port_type> [<v_port_type_list>]) status

2.9.29 (config)# mep

(config)# mep <inst>

Syntax: (config)# mep <inst> [mip] { up | down } domain { port | evc | vlan } [vid <vid>] flow <flow> level <level> interface < port_ type> < port>

Explanation: Create a MEP instance.

Parameters:

<inst>: Specify an instance ID number.

[mip]: Mip (Maintenance Entity Intermediate Point) mode.

{ up | down }: Specify the traffic direction either Ingress or Egress for monitoring on a residence port.
domain { port | evc | vlan }: Specify a domain option.

Port: This is a MEP in the Port Domain. 'Flow Instance' is a Port. (CURRENTLY, Port is available for use.)

Evc: This is a MEP in the EVC Domain. 'Flow Instance' is a EVC. The EVC must be created.

VLAN: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN. The VLAN must be created.

[vid< vid>]: AC-tag orS-tag(dependingonVLANporttype)isaddedwiththisVID. Entering "0" means notag will be added.

flow <flow>: TheMEP related tothisflow. level <level>:TheMGP level ofthis MEP.

interface <port_type> <port>: Specify a port number that you want to moinitor.

Negation: (config)# no mep <inst>

Show: # show mep [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck] [detail]

(config)# mep <inst> ais

Syntax: (config)# mep <inst> ais [frls | frlm] [protect]

Explanation: To configure AIS of a MEP instance.

Parameters:

<inst>: Specify an instance ID number.

ais [fr1s | fr1m]: Ais stands for Alarm Indication Signal. "fr1s" means that frame rate is 1f/s. "fr1m" means that frame rate is 1f/min.

[protect]: The AIS can be used for protection. At the point of state change three AIS PDUs are transmitted as fast as possible.

Negation: (config)# no mep <inst> ais

Show: # show mep [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck] [detail]

(config)# mep <inst> aps

Syntax: (config)# mep <inst> aps <prio> [multi | uni] { laps | { raps [octet <octet>] } }

Explanation: Configure APS of a MEP instance.

Parameters:

<inst>: Specify an instance ID number.

aps <prio>: The priority to be inserted as PCP bits in TAG (if any). [multi | uni]: Specify an option.

multi: OAM PDU is transmitted with multicast MAC. Must be "multi" in case of RAPS (Ring Automatic Protection Switching Protocol).

uni: OAM PDU is transmitted with unicast MAC. The MAC is taken from peer MEP MAC database. This option is only possible in case of LAPS (Linear Automatic Protection Switching Protocol).

{ laps | { raps [octet <octet>] } }: Specify an option.

laps: APS PDU is transmitted as L-APS (this is for ELPS).

raps: APS PDU is transmitted as R-APS (this is for ERPS).

octet: This is the last octet of the transmitted and expected RAPS multi-cast MAC. In G.8031 (03/2010) a RAPS multi-cast MAC is defined as 01-19-A7-00-00-XX. In current standard the value for this last octet is '01' and the usage of other values is for further study.

Negation: (config)# no mep <inst> aps

Show: # show mep [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck] [detail]

(config)# mep <inst> cc

Syntax: (config)# mep <inst> cc <prio> [fr300s | fr100s | fr10s | fr1s | fr6m | fr1m | fr6h]

Explanation: Configure Continuity Check of a MEP instance.

Parameters:

<inst>: Specify an instance ID number. cc: Continuity Check

<prio: 0-7>: The priority to be inserted as PCP bits in TAG (if any).

[fr300s | fr100s | fr10s | fr1s | fr6m | fr1m | fr6h]: The frame rate is 300 f/s, 100 f/s, 10 f/s, 1 f/s, 6 f/min, 1 f/min, 6 f/hour.

Negation: (config)# no mep <inst> cc

Show: # show mep [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck] [detail]

(config)# mep <inst> client domain

Syntax: (config)# mep <inst> client domain { evc | vlan }

Explanation: Configureclientdomainofa MEPinstance.

Parameters:

<inst>: Specify an instance ID number. cc: Continuity Check

{ evc | vlan }: The client layer domain. Options available are EVC and VLAN domain.

Show: # show mep [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck] [detail]

(config)# mep <inst> client flow

Syntax: (config)# mep <inst> client flow <cflow> level <level> [ais-prio [<aisprio> | ais-highest]] [lck-prio

[<lck pri 0 >
|lck -high est]]

Explanation: Configure the priority to be used when transmitting AIS in each client flow.

Parameters:

<inst>: Specify an instance ID number.

client flow <cflow: unit>: The client layer flow number. level <level: 0-7>: The MEG level value.

[ais-prio [<aisprio:0-7> | ais-highest]]: Configure AIS injection priority. Specify either 0-7 or the highest possible number.

[lck-prio [<lckprio: 0-7> | lck-highest]]: Configure LCK injection priority. Specify either 0-7 or the highest possible number.

Negation: (config)# no mep <inst> client-flow { <cflow> | all }

Show: # show mep [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck] [detail]

(config)# mep <inst>dm

Syntax: (config)# mep <inst> dm <prio> [multi | { uni mep-id <mepid> }] [single | dual] [rdtrp | flow] interval

<interval> last-n <lastn>

Explanation: To configure Delay Measurement of a MEP.

Parameters:

<inst>: Specify an instance ID number.

dm <prio: 0-7>: Configure Delay Measurement (DM) priority value. Priority in case of tagged OAM. In the

EVC domain this is the COS-ID.

[multi | { uni mep-id <mepid> }]: Specify multicast or unicast MEP ID.

[single | dual]: One-Way or Two-Way Delay Measurement implemented on 1DM or DMM/DMR, respectively. [rdtrp | flow]: Specify one value.

rdtrp: The frame delay calculated by the transmitting and receiving timestamps of initiators. Frame Delay = RxTimeb-TxTimeStampf.

Flow: The frame delay calculated by the transmitting and receiving timestamps of initiators and remotes. Frame Delay = (RxTimeb-TxTimeStampf)-(TxTimeStampb-RxTimeStampf).

interval <interval>: Interval between PDU transmission in 10ms. Min value is 10. last-n <lastn>: The last N dalays used for average last N calculation. Min value is 10.

Negation: (config)# no mep <inst> dm

Show: # show mep [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck] [detail]

Clear: # clear mep <inst> { lm | dm |tst }

(config)# mep <inst> dm ns

Syntax: (config)# mep <inst> dm ns

Explanation: Configure Delay Measurement (nanosecond) of a MEP.

Parameters:

<inst>: Specify an instance ID number.

Negation: (config)# no mep <inst> dm ns

Show: # show mep [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck] [detail]

Clear: # clear mep <inst> { lm | dm |tst }

(config)# mep <inst> dm overflow-reset

Syntax: (config)# mep <inst> dm overflow-reset

Explanation: Reset all Delay Measurement results on total delay counter overflow.

Parameters:

<inst>: Specify an instance ID number.

Negation: (config)# no mep <inst> dm overflow-reset

Show: # show mep [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck] [detail]

Clear: # clear mep <inst> { lm | dm |tst }

(config)# mep <inst> dm proprietary

Syntax: (config)# mep <inst> dm proprietary **Explanation:** Use proprietary Delay Measurement.

Parameters:

<inst>: Specify an instance ID number.

Negation: (config)# no mep <inst> dm proprietary

Show: # show mep [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck] [detail]

Clear: # clear mep <inst> { lm | dm |tst }

(config)# mep <inst> dm syncronized

Syntax: (config)# mep <inst> dm syncronized **Explanation:** Configure time sync of Delay Measurement.

Parameters:

<inst>: Specify an instance ID number.

Negation: (config)# no mep <inst> dm syncronized

Show: # show mep [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck] [detail]

Clear: # clear mep <inst> { lm | dm |tst }

(config)# mep <inst>lb

Syntax: (config)# mep <inst> lb <prio> [dei] [multi |{ uni {{ mep-id <mepid> } |{ mac <mac>}}}] count <count> size <size> interval <interval>

Explanation: Configure loopback of a MEP.

Parameters:

<inst>: Specify an instance ID number.

lb <prio: 0-7>: Configure loopback priority. The priority to be inserted as PCP bits in TAG (if any). [dei]: The DEI to be inserted as PCP bits in TAG (if any).

[multi | { uni { { mep-id <mepid> } | { mac <mac> } } }]: Specify LBM PDU to be transmitted as unicast or multicast. The unicast MAC will be configured through 'Peer MEP' or 'Unicast Peer MAC'. To-wards MIP only unicast Loop Back is possible.

count <count>: The number of LBM PDU to be sent.

size <size>: The number of bytes in the LBM PDU Data Pattern TLV. interval <interval>: The number of bytes in the LBM PDU Data Pattern TLV.

Negation: (config)# no mep <inst> lb

Show: # show mep [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck] [detail]

(config)# mep <inst> lck

Syntax: (config)# mep <inst> lck [frls | frlm]

Explanation: Configure Locked Frame Rate of a MEP.

Parameters:

<inst>: Specify an instance ID number.

[fr1s | fr1m]: Frame rate is 1f/s or 1f/min.

Negation: (config)# no mep <inst> lck

Show: # show mep [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck] [detail]

(config)# mep <inst>level

Syntax: (config)# mep <inst> level <level>

Explanation: Configure MEG level of a MEP.

Parameters:

<inst>: Specify an instance ID number.

<level:0-7>: The MEG level value.

Show: # show mep [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck] [detail]

(config)# mep <inst>lm

Syntax: (config)# mep <inst> lm <prio> [multi | uni] [single | dual] [fr10s | fr1s | fr6m | fr1m | fr6h] [flr <flr>]

Explanation: Configure Locked Frame Rate of a MEP.

Parameters:

<inst>: Specify an instance ID number.

lm <prio: 0-7>: Configure loss measurement priority in case of tagged OAM. In the EVC domain this is the COS-ID.

[multi | uni]: multi OAM PDU is transmitted with multicast MAC. uni OAM PDU is transmitted with unicast MAC. The MAC is taken from peer MEP MAC database. In case of LM there is only one peer MEP.

[single | dual]: Dual ended LM is based on CCM PDU. Single ended LM is based on LMM/LMR PDU. [fr10s | fr1s | fr6m | fr1m | fr6h]: Specify a frame rate.

fr10s: Frame rate is 10f/s. fr1s: Frame rate is 1f/s. fr6m: Frame rate is 6f/min. fr1m: Frame rate is 1f/min. fr6h: Frame rate is 6f/hour.

[flr <flr: unit>]: The Frame Loss Ratio interval value.

Negation: (config)# no mep <inst> lm

Show: # show mep [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck] [detail]

Clear: # clear mep <inst> { lm | dm |tst }

(config)# mep <inst>lt

Syntax: (config)# mep <inst> lt <prio> { { mep-id <mepid> } | { mac <mac> } } ttl <ttl>

Explanation: Configure link trace of a MEP.

Parameters:

<inst>: Specify an instance ID number.

lt <prio: 0-7>: Configure link trace priority in case of tagged OAM. In the EVC domain this is the COS-ID.

{{ mep-id <mepid>} |{ mac <mac>}}: Specify Peer MEP-ID for Link Trace target unicast MAC or Link Trace target unicast MAC address.

ttl <ttl> Time to live value.

Negation: (config)# no mep <inst> lt

Show: # show mep [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck] [detail]

(config)# mep <inst>meg-id

Syntax: (config)# mep <inst> meg-id <megid> { itu | itu-cc | { ieee [name <name>] } }

Explanation: To configure MEG-ID format.

Parameters:

<inst>: Specify an instance ID number.

meg-id <megid>: Specify a MEG ID string. This is either the ITU MEG-ID or the IEEE Short MA, depending on the selected MEG-ID format. The ITU max. is 13 characters. The ITU-CC max. is 15 characters. The IEEE max. is 16 characters..

{ itu | itu-cc | { ieee [name <name>] } }: Specify a MEG-ID format.

itu: The MEG-ID has ITU format (ICC - UMC). The meg-id max. is 13 characters.

itu-cc: The MEG-ID has ITU Country Code format (CC - ICC - UMC). The meg-id max. is 15 characters.

ieee: The MEG-ID (Short MA Name) has IEEE Character String format. The meg-id max. is 16 characters.

name <name>: This is only relevant for IEEE.

(config)# mep <inst> peer-mep-id

Syntax: (config)# mep <inst> peer-mep-id <mepid> [mac <mac>]

Explanation: Configure peer MEP-ID of a MEP.

Parameters:

<inst>: Specifyan instance ID number.

peer-mep-id <mepid>: Configure the peer MEP-ID value. [mac <mac>]: The peer MAC address.
Negation: (config)# no mep <inst> peer-mep-id { <mepid> | all }

(config)# mep <inst> performance-monitoring

Syntax: (config)# mep <inst> performance-monitoring

Explanation: Enable perofmrance monitoring of MEP.

Parameters:

<inst>: Specify an instance ID number.

Negation: (config)#no mep<inst> performance-monitoring

(config)# mep <inst> tst

Syntax: (config)#mep <inst>tst<prio> [dei]mep-id<mepid> [sequence] [all-zero |all-one | one-zero]rate <rate> size <size>

Explanation: Enable test signal of MEP.

Parameters:

<inst>: Specify an instance ID number.

tst <prio: 0-7>: Configure the test signal priority in case of tagged OAM. In the EVC domain this is the COS-ID. [dei]: Drop Eligible Indicator in case of tagged OAM.

mep-id <mepid>: Configure Peer MEP-ID value for unicast TST. The MAC is taken from peer MEP MAC database. [sequence]: Enable sequence number in TST PDU.

[all-zero | all-one | one-zero]: Specify an option.

all-zero: Test pattern is set to all zero.

all-one: Test pattern is set to all one.

one-zero: Testpattern is set to 10101010. rate <rate>: Transmission rate value.

size <size>: Frame size value.

Show: # show mep [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck] [detail]

Clear: # clear mep <inst> { lm | dm |tst }

(config)# mep <inst> tst rx

Syntax: (config)# mep <inst> tst rx

Explanation: Enable test signal RX transmission of MEP.

Parameters:

<inst>: Specify an instance ID number.

Negation: (config)# no mep <inst> tst rx

Show: # show mep [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck] [detail]

Clear: # clear mep <inst> { lm | dm |tst }

(config)# mep <inst> tst rx

Syntax: (config)# mep <inst> tst tx

Explanation: Enable test signal TX transmission of MEP.

Parameters:

<inst>: Specify an instance ID number.

Negation: (config)# no mep <inst> tst tx

Show: # show mep [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck] [detail]

Clear: # clear mep <inst> { lm | dm |tst }

(config)# mep <inst> vid

Syntax:(config)#mep <inst>vid<vid>

Explanation: To configure VID of MEP.

Parameters:

<inst>: Specify an instance ID number.

<vid>: The MEP VID value.

Negation: (config)# no mep <inst> vid

Show: # show mep [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck] [detail]

(config)# mep <inst> voe

Syntax: (config)# mep <inst> voe

Explanation: MEP is VOE based.

Parameters:

<inst>: Specify an instance ID number.

Negation: (config)# no mep <inst> voe

Show: # show mep [<inst>] [peer | cc | lm | dm | lt | lb | tst | aps | client | ais | lck] [detail]

2.9.30 (config)# monitor

(config)# monitor destination interface

Syntax: (config)# monitor destination interface <port_type> <in_port_type>

Explanation: Configure which port traffic should be mirrored to.

Parameters:

<port_type>: Specify the interface type.

<in_port_type>: Specify the port number.

Example: Set the traffic to be mirrored to Gigabit Ethernet port 10.

```
# config t
(config)# monitor destination interface gigabitethernet 1/10
```

Negation: (config)# no monitor destination

(config)# monitor source

Syntax: (config)# monitor source{ [interface (<port_type>) [<v_port_type_list>]]} |{ cpu [<cpu_switch_range>] } { both | rx | tx }

Explanation: Configure which source ports ' RX or TX traffic should be mirrored to the destination port.

Parameters:

{ [interface (<port_type>) [<v_port_type_list>]]}: Specify one of the options. * means all interfaces.

{ both | rx | tx }: Specify which direction of traffic should be mirrored to the destination port. "both" means both received and transmitted traffic. "rx" means received traffic. "tx" means transmitted traffic.

Example: Set port 1 to 5 ' s RX traffic to be mirrored to the destination port.

```
# config t
(config)# monitor source interface GigabitEthernet 1/1-5 rx
```

Negation: (config)#no monitorsource{{interface(<port_type>[<v_port_type_list>])}|{cpu [<cpu_switch_range>] } }

2.9.31 (config)# ntp

(config)# ntp

Syntax: (config)# ntp

Explanation: Enable NTP function.

Example: Enable NTP function.

```
# config t
(config)# ntp
```

Negation: (config)# no ntp

Show: # show ntp status

(config)# ntp server

Syntax: (config)# ntp server <index_var> ip-address { <ipv4_var> | <ipv6_var> | <name_var> }

Explanation: Configure a list of NTP server ' s address.

Parameters:

< index_var: 1-5>: Specify the index number of NTP server. The allowed range is from 1 to 5. The NTP servers are tried in numeric order. If 'Server 1' is unavailable, the NTP client will try to contact 'Server 2'.

{ <ipv4_var> | <ipv6_var> | <name_var> }: Specify one of the three options.

<ipv4_var>: IPv4 address.

<ipv6_var>: IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special

syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once.

<name_var>: The domain name for NTP server.

Example: Set the NTP server 1 to 192.168.1.253.

```
# config t
(config)# ntp server 1 ip-address 192.168.1.253
```

Negation: (config)# no ntp server <index_var>

Show: # show ntp status

2.9.32 (config)# poe(For PoE ModelsOnly)
(config)# poe management mode

Syntax: (config)# poe management mode { allocation-consumption | allocation-reserved-power }

Explanation: Power over Ethernet (PoE) commands are used to set the maximum PoE power provided to a port, the maximum power budget for the switch (power available to all RJ-45 ports), the port PoE operating mode, power allocation priority, and the maximum power allocated to each port. If the power demand from devices connected to the switch exceeds the power budget, the switch uses port power priority settings to limit the supplied power.

Parameters:

consumption & reserved power mode: "consumption" & "reserved-power" mode decide how ports are shut down.

consumption: When this mode is used, ports are shutdown in the event of the following situations.

When the actual power consumption for all ports exceeds the amount ofpower supply can deliver.

When the actual power consumption for a given port exceeds the reserved power for that port.

Ports are shutdown according to their port priority. If two ports have the same priority, the port with the higher port number is shutdown.

reserved-power: When this mode is selected, ports are shutdown when total reserved power exceeds the amount of power thatthepower supply can deliver. In this mode,ifthe PD(Powered Device) keeps requesting more power than available from the power supply, then the port power is not turned on.

allocation : These modes are used to set up how attached PD may reserve power:

allocation: The amount of power reserved for each is specified in "Maximum Power [W]" field.

NOTE:*Ifportsusemorepower than thepower reservedfor them,theywillbeshutdown.*

Negation: (config)# no poe management mode

Show:>show poe [interface (<port_type>[<v_port_type_list>])] # show poe [interface (<port_type> [<v_port_type_list>])]

(config)# poe supply

Syntax: (config)# poe supply <v_1_to_600>

Explanation: Configure the maximum power supply that the device can deliver.

Parameters:

<v_1_to_600>: Specify maximum power supply that the device can deliver.

Negation: (config)# no poe supply

2.9.33 (config)# port-security

(config)# port-security

Syntax: (config)# port-security

Explanation: Enable port security function globally.

Example: Enable port security function globally.

```
# config t
(config)# port-security
```

Negation: (config)# no port-security

Show: > show port-security switch [interface (<port_type> [<v_port_type_list>])] # show port-security switch [interface (<port_type> [<v_port_type_list>])]

(config)# port-security aging

Syntax: (config)# port-security aging

Explanation: Enable port security aging function. If enabled, secured MAC addresses are subject to aging as discussed in "Aging time" command. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Example: Enable port security aging function.

```
# config t
(config)# port-security aging
```

Negation: (config)# no port-security aging

Show: >show port-securityport[interface(<port_type>[<v_port_type_list>])] # show port-security port [interface (<port_type> [<v_port_type_list>])]

(config)# port-security aging time

Syntax: (config)# port-security aging time <v_10_to_10000000>

Explanation: Configure a desired aging time value. If "Aging" is enabled, secured MAC addresses are subject to aging as discussed this command. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames

are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Parameters:

<v_10_to_10000000>: Specify the aging time value. The allowed range is between 10 and 10,000,000 seconds.

Example: Set the aging time value to 1800 seconds.

```
# config t
(config)# port-security aging time 1800
```

Negation: (config)# no port-security aging time

Show:>show port-security port [interface (<port_type> [<v_port_type_list>])] # show port-security port [interface (<port_type> [<v_port_type_list>])]

(config-if)# port-security

Syntax: (configt-if)# port-security

Explanation: Enable the port security function on the selected ports.

Example: Enable Gigabit Ethernet port 1-10's port security function.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# port-security
```

Negation: (configt-if)# no port-security

Show: > show port-security switch [interface (<port_type> [<v_port_type_list>])] # show port-security switch [interface (<port_type> [<v_port_type_list>])]

(config-if)# port-security maximum

Syntax: (configt-if)# port-security maximum [<v_1_to_1024>]

Explanation: The maximum number of MAC addresses that can be secured on this port. The number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken.

Parameters:

[<v_1_to_1024>]: Specify a value between 1 and 1024.

Example: Limit Gigabit Ethernet port 1-10's MAC addresses can be learnt to 5.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# port-security maximum 5
```

Negation: (configt-if)# no port-security maximum

Show:>show port-security port [interface (<port_type> [<v_port_type_list>])] # show port-security port [interface (<port_type> [<v_port_type_list>])]

(config-if)# port-security violation

Syntax: (configt-if)# port-security violation { protect | trap | trap-shutdown | shutdown }

Explanation: If the limit is exceeded, the specified action will take effect.

Parameters:

{ protect | trap | trap-shutdown | shutdown }: Specify one of the actions taken when the limit is exceeded.

protect: Do not allow more than the specified limit of MAC addresses to access on a port. No action is further taken.

trap: If Limit + 1 MAC addresses are seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit is exceeded.

trap-shutdown: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will betaken.

shutdown: If Limit + 1 MACaddresses is seen on the port, shutdown the port. This implies that all secured MAC addresses will be removed from the port, and no new addresses will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shutdown. There are three ways to re-open the port:

Boot the switch

Disable and re-enable Limit Control on the port or the switch

Click the "Reopen" button

Example: Send a SNMP trap when the limit is exceeded.

```
# config t
(config)# interface gigabitethernet 1/1-10
(config-if)# port-security violation trap
```

Negation: (configt-if)# no port-security violation

Show:>show port-securityport[interface(<port_type>[<v_port_type_list>])] # show port-security port [interface (<port_type> [<v_port_type_list>])]

2.9.34 (config)# privilege

Syntax: (config)# privilege { exec | configure | config-vlan | line | interface | if-vlan | ipmc-profile | snmps-host | stp-aggr | dhcp-pool | rfc2544 -profile } level <privilege> <cmd>

Explanation: This command is used to change the privilege level of commands available in Configuration mode.

Parameters:

{ exec | configure | config-vlan | line | interface | if-vlan | ipmc-profile | snmps-host | stp-aggr | dhcp-pool | rfc2544-profile }: Specify the group command that you want to configure.

level <privilege>: Specify the privilege level. The allowed range is 0 to 15.

<cmd>: Initial valid words and literals of the command to modify, in 128 characters.

Example: The following example sets the privilege level to 15 for any Exec mode (user or privileged) command that start with the letter "v"

```
# config t
(config)# privilege exec level 15 host
```

Negation: (config)# no privilege { exec | configure | config-vlan | line | interface | if-vlan | ipmc-profile | snmps-host | stp-aggr | dhcp-pool | rfc2544-profile } level <0-15> <cmd>

Show: >show privilege # show privilege

2.9.35 (config)# qos

(config)# qos map cos-dscp

Syntax: (config)#qos map cos-dscp <cos> dpl <dpl> dscp { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23

| af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

Parameters:

cos-dscp <cos>: Map COS to DSCP. Indicate the Class of Service level. The allowed range is 0 to 7. A CoS class of 0 has the lowest priority, while 7 has the highest priority.

dpl <dpl>: Specify the Drop Precedence Level. The allowed range is 0 to 7.

dscp { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }: Specify one of the DSCP values

<dscp_num: 0-63>: The allowed number is from 0 to 63. be: Default PHB (DSCP 0) for best effort traffic.

af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43: Assured Forwarding PHB AF 11 (DSCP 10), 12 (DSCP 12), 13 (DSCP 14), 21 (DSCP 18), 22 (DSCP 20), 23 (DSCP 22), 31 (DSCP 26), 32 (DSCP 28), 33 (DSCP 30), 41 (DSCP 34), 42 (DSCP 36).

cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7: Class selector PHB CS1 precedence 1 (DSCP 8), CS2 precedence 2 (DSCP 16), CS3 precedence 3 (DSCP 24), CS4 precedence 4 (DSCP 32), CS5 precedence 5 (DSCP 40), CS6 precedence 6 (DSCP 48), CS7 precedence 7 (DSCP 56).

ef: Expedited Forwarding PHB (DSCP 46).

va: Voice Admit PHB (DSCP 44).

Explanation: Configure the COS-DSCP mapping.

Example: The following example sets DPL to 4, DSCP to cs4.

```
# config t
(config)# qos map cos-dscp 4 dpl 4 dscp cs4
```

Negation: (config)# no qos map cos-dscp <cos> dpl <dpl>

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

(config)# qos mapdscp-classify

Syntax: (config)# qos map dscp-classify { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

Parameters:

dscp-classify { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43

| cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }: Specify one of the DSCP values.

<dscp_num: 0-63>: The allowed number is from 0 to 63.

be: Default PHB (DSCP 0) for best effort traffic.

af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43: Assured Forwarding PHB AF 11 (DSCP 10), 12 (DSCP 12), 13 (DSCP 14), 21 (DSCP 18), 22 (DSCP 20), 23 (DSCP 22), 31 (DSCP 26), 32 (DSCP 28), 33 (DSCP 30), 41 (DSCP 34), 42 (DSCP 36).

cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7: Class selector PHB CS1 precedence 1 (DSCP 8), CS2 precedence 2 (DSCP 16), CS3 precedence 3 (DSCP 24), CS4 precedence 4 (DSCP 32), CS5 precedence 5 (DSCP 40), CS6 precedence 6 (DSCP 48), CS7 precedence 7 (DSCP 56).

ef: Expedited Forwarding PHB (DSCP 46).

va: Voice Admit PHB (DSCP 44).

Explanation: Configure the DSCP Ingress classification.

Example: The following example sets DSCP Ingress classification to cs4.

```
# config t
(config)# qos map dscp-classify cs4
```

Negation: (config)# no qos map dscp-classify { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

(config)# qos mapdscp-cos

Syntax: (config)# qos map dscp-cos { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } cos <cos> dpl <dpl>

Explanation: Configure the DSCP-based QoS Ingress classification.

Parameters:

dscp-cos { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }: Specify one of the DSCP values.

<dscp_num: 0-63>: The allowed number is from 0 to 63.

be: Default PHB (DSCP 0) for best effort traffic.

af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43: Assured Forwarding PHB AF 11 (DSCP 10), 12 (DSCP 12), 13 (DSCP 14), 21 (DSCP 18), 22 (DSCP 20), 23 (DSCP 22), 31 (DSCP 26), 32 (DSCP 28), 33 (DSCP 30), 41 (DSCP 34), 42 (DSCP 36).

cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7: Classselector PHB CS1 precedence 1 (DSCP 8), CS2 precedence 2 (DSCP 16), CS3 precedence 3 (DSCP 24), CS4 precedence 4 (DSCP 32), CS5 precedence 5 (DSCP 40), CS6

precedence 6 (DSCP 48), CS7 precedence 7 (DSCP 56).

ef: Expedited Forwarding PHB (DSCP 46).

va: Voice Admit PHB (DSCP 44).

cos <cos>: Indicate the Class of Service level. The allowed range is 0 to 7. A CoS class of 0 has the lowest priority, while 7 has the highest priority.

dpl <dpl>: Specify the Drop Precedence Level. The allowed range is 0 to 7.

Negation: (config)# no qos map dscp-cos { <dscp_num> |{ be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

(config)# qos mapdscp-egress-translation

Syntax: (config)# qos map dscp-egress-translation { <dscp_num> |{ be | af11 | af12 | af13 | af21 | af22 | af23 | af31

| af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 |ef|va }}to {<dscp_num_tr>|{be|

af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 |ef | va } }

Explanation: Configure the DSCP Egress Mapping Table.

Parameters:

dscp-egress-translation { <dscp_num> |{ be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }: Specify one of the DSCP values.

<dscp_num: 0-63>: The allowed number is from 0 to 63.

be: Default PHB (DSCP 0) for best effort traffic.

af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43: Assured Forwarding PHB AF 11 (DSCP 10), 12 (DSCP 12), 13 (DSCP 14), 21 (DSCP 18), 22 (DSCP 20), 23 (DSCP 22), 31 (DSCP 26), 32 (DSCP 28), 33 (DSCP 30), 41 (DSCP 34), 42 (DSCP 36).

cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7: Class selector PHB CS1 precedence 1 (DSCP 8), CS2 precedence 2 (DSCP 16), CS3 precedence 3 (DSCP 24), CS4 precedence 4 (DSCP 32), CS5 precedence 5 (DSCP 40), CS6 precedence 6 (DSCP 48), CS7 precedence 7 (DSCP 56).

ef: Expedited Forwarding PHB (DSCP 46).

va: Voice Admit PHB (DSCP 44).

Example: The following example maps cs4 to cs5.

```
# config t
(config)# qos map dscp-egress-translation cs4 to cs5
```

Negation: (config)# no qos map dscp-egress-translation {<dscp_num> |{be |af11 | af12 | af13 | af21 | af22 | af23 |af31 | af32 | af33 |af41 | af42 |af43 | cs1 | cs2 | cs3 |cs4 | cs5 | cs6 | cs7 | ef |va }} <dpl>

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

(config)# qos mapdscp-ingress-translation

Syntax: (config)# qos map dscp-ingress-translation { <dscp_num> |{ be |af11 |af12 |af13 |af21 |af22 |

af23 |af31
| af32| af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 |ef|va}}to{<dscp_num_tr>|{be|

af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 |ef | va } }

Explanation: Configure the DSCP Ingress Mapping Table.

Parameters:

dscp-ingress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }: Specify one of the DSCP values.

<dscp_num: 0-63>: The allowed number is from 0 to 63.

be: Default PHB (DSCP 0) for best effort traffic.

af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43: Assured Forwarding PHBAF 11 (DSCP 10), 12 (DSCP 12), 13 (DSCP14), 21 (DSCP 18), 22 (DSCP 20), 23 (DSCP 22), 31 (DSCP26), 32 (DSCP 28), 33 (DSCP 30), 41 (DSCP 34), 42 (DSCP 36).

cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7: Classselector PHBCS1precedence 1(DSCP8), CS2precedence 2 (DSCP16), CS3 precedence 3 (DSCP24), CS4precedence 4(DSCP32), CS5 precedence 5 (DSCP40), CS6 precedence 6 (DSCP 48), CS7 precedence 7 (DSCP 56).

ef: Expedited Forwarding PHB (DSCP 46).

va: Voice Admit PHB (DSCP 44).

Example: The following example maps cs4 to cs5.

```
# config t
(config)# qos map dscp-ingress-translation cs4 to cs5
```

Negation: (config)# no qos mapdscp-ingress-translation {<dscp_num> |{be |af11 |af12 |af13 | af21 | af22 | af23
| af31 | af32 | af33 | af41 |af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef |va} }

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

(config)# qos qce refresh

Syntax: (config)# qos qce refresh **Explanation:** To refresh QCE. **Example:** Refresh QCE.

```
# config t
 (config)# qos qce refresh
```

(config)# qos qce update

Syntax: (config)# qos qce { [update] } <qce_id> [{ next <qce_id_next> } | last] [interface (<port_type> [<port_list>])] [smac { <smac> | <smac_24> | any }] [dmac { <dmac> | unicast | multicast | broadcast | any }] [tag

{ [type { untagged | tagged | c-tagged | s-tagged | any }] [vid { <ot_vid> | any }] [pcp { <ot_pcp> | any }] [dei

{ <ot_dei> | any }] }*1] [inner-tag { [type { untagged | tagged | c-tagged | s-tagged | any }] [vid { <it_vid> | any }] [pcp { <it_pcp> | any }] [dei { <it_dei> | any }] }*1] [frame-type { any | { etype [{ <etype_type> |

any }] } | { llc

[dsap { <llc_dsap> | any }] [ssap { <llc_ssap> | any }] [control { <llc_control> | any }] } | { snap

[{ <snap_data> | any }] } | { ipv4 [proto { <pr4> | tcp | udp | any }] [sip { <sip4> | any }] [dip { <dip4> | any }] [dscp { <dscp4> | { 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 }] [sport { <sp4> | any }] [dport { <dp4> | any }] } | { ipv6 [proto { <pr6> | tcp | udp | any }] [sip { <sip6> | any }] [dip { <dip6> | any }] [dscp { <dscp6> | { be | af11 | af12 |

af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any }] [sport { <sp6> | any }] [dport { <dp6> | any }] }] [action { [cos { <action_cos> | default }] [dpl

{ <action_dpl> |

default }] [pcp-dei { <action_pcp> <action_dei> | default }] [dscp { <action_dscp_dscp> | { be | af11 | af12 |

af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | default }] [policy { <action_policy> | default }] }*1]

Explanation: To update the QCE.

Parameters:

{ [update] }: Update the QCE.

<qce_id>: Specify the QCE ID.

[{ next <qce_id_next> } | last]: Put this QCE next to the specified one or to the last one.

[interface (<port_type> [<port_list>])]: Specify port type and port number that apply to this updated QCE rule.
[smac { <smac> | <smac_24> | any }]: Set up the matched SMAC.

[dmac { <dmac> | unicast | multicast | broadcast | any }]: Set up the matached DMAC.

[tag { [type { untagged | tagged | c-tagged | s-tagged | any }]: Setup the matched tag type. [vid { <ot_vid> | any }]: Specify a specific VID or VID range or specify "any" to allow any VIDs.

[pcp { <ot_pcp> | any }]: Specify a specific PCP or PCP range or specify "any" to allow any PCP values. [dei { <ot_dei> | any }] }]: Specify a specific DEI or specify "any" to allow any DEI.

[frame-type { any | { etype [{ <etype_type> | any }] } | { llc [dsap { <llc_dsap> | any }] [ssap { <llc_ssap> | any }] [control { <llc_control> | any }] } | { snap [{ <snap_data> | any }] } | { ipv4 [proto { <pr4> | tcp | udp |

any}] [sip{ <sip4>| any}][dip{ <dip4> |any}][d scp{ <dscp4> | { be | af1 1 | af12 | af1 3 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2| cs3| cs4 | cs5| cs6 | cs7 | ef | va}| any}][fr agment{yes | no | any }] [sport{ <sp4> | any }] [dport{ <dp4> | any }] } | { ipv6 [proto{ <pr6 > | tcp | udp | any }]

[sip

{ <sip6> I any }] [dip { <dip6> I any }] [dscp { <dscp6> I { be I af11 I af12 I af13 I af21 I af22 I af23 I af31 I af32 I af33 I af41 I af42 I af43 I cs1 I cs2 I cs3 I cs4 I cs5 I cs6 I cs7 I ef I va } I any }] [sport { <sp6> I any }] [dport

{ <dp6> I any }] } }]: Specify the frame type that applies to this QCE rule.

any: By default, any is used which means that all types of frames are allowed.

etype: This option can only be used to filter Ethernet II formatted packets. (Options: Any, Specific – 600-ffff hex; Default: ffff). Note that 800 (IPv4) and 86DD (IPv6) are excluded. A detailed listing of Ethernet protocol

types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).

llc: LLC refers to Link Logical Control and further provides three options.

dsap: DSAP stands for Destination Service Access Point address. By default, any is used. Specify "any" or indicate a value (0x00 to 0xFF).

ssap: SSAP stands for Source Service Access Point address. By default, any is used. Specify "any" or indicate a value (0x00-0xFF).

control: Control field may contain command, response, or sequence information depending on whether the

LLC frame type is Unnumbered, Supervisory, or Information. By default, any is used. Specify "any" or indicate a value (0x00 to 0xFF).

snap: SubNetwork Access Protocol can be distinguished by an OUI and a Protocol ID. (Options for PID: Any, Specific (0x00-0xffff); Default: Any) If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type

(EtherType) field value for the protocol running on top of SNAP. If the OUI is that of a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other

words, if value of the OUI field is 00-00-00, then value of the PID will be etherType (0x0600-0xffff), and if value of the OUI isother than 00-00-00, then valid value of the PID will be any value from 0x0000 to 0xffff.

ipv4:

proto: IPv4 frame type includes Any, TCP, UDP, Other. If "TCP" or "UDP" is specified, you might further define Sport (Source port number) and Dport (Destination port number).

sip: Specify source IP type. By default, any is used. Indicate self-defined source IP and submask format. The address and mask must be in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When the mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero

dscp: By default, any is used. Indicate a DSCP value or a range of DSCP value.

fragment: By default, any is used. Datagrams sometimes may be fragmented to ensure they can pass through a network device that uses a maximum transfer unit smaller than the original packet's size.

ipv6:

proto: IPv6 protocol includes Any, TCP, UDP, Other. If "TCP" or "UDP" is specified, you may need to further define Sport (Source port number) and Dport (Destination port number).

sip: Specify source IP type. By default, any is used. You can also indicate self-defined source IP and submask format.

dscp: By default, any is used. You can also indicate a DSCP value or a range of DSCP value.

[action { [cos { <action_cos> | default }]: Specify the classification action taken on ingress frame if the parameters match the frame's content. If a frame matches the QCE, it will be put in the queue

corresponding to the specified QoS class or placed in a queue based on basic classification rules.

[dpl { <action_dpl> | default }]: If a frame matches the QCE, the drop precedence level will be set to the specified value or left unchanged.

[pcp-dei { <action_pcp> <action_dei> | default }]: If a frame matches the QCE, the PCP or DEI value will be set to the specified one.

[dscp { <action_dscp_dscp> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | default }] [policy { <action_policy> | default }] }*1]: If a frame matches the QCE, the DSCP value will be set to the specified one.

Negation: (config)# no qos qce <qce_id_range>

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

(config)# qos storm

Syntax: (config)# qos storm { unicast | multicast | broadcast } { { <rate> [kfps] } | { 1024 kfps } }

Explanation: Configure broadcast storm control rate for QoS

Parameters:

{ unicast | multicast | broadcast }: Specify the storm type that you want to configure.

{ { <rate> [kfps] } | { 1024 kfps } }: User-define storm frame rate or set storm rate to 1024 kfps.

Example: The following example sets broadcast storm control for QoS to 1024 kfps.

```
# config t
(config)# qos storm broadcast 1024 kfps
```

Negation: (config)# no qos storm { unicast | multicast | broadcast }

Show: # show qos storm

(config-if)# qoscos

Syntax: (config-if)# qos cos <cos>

Explanation: Configure CoS value on this selecte infterface.

Parameters:

<cos>: Specify COS value (1-7).

Negation: (config-if)# no qos cos

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } |wred |{ maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

(config-if)# qos dei

Syntax: (config-if)# qos dei <dei>

Explanation: Configure DEI (Drop Eligible Indicator) value on this selecte infterface.

Parameters:

<dei>: Specify DEI for untagged frames.

Negation: (config-if)# no qos dei

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

(config-if)# qosdpl

Syntax: (config-if)# qos dpl <dpl>

Explanation: Configure DPL value on this selecte infterface.

Parameters:

<dpl>: Specify the default Drop Precedence Level

Negation: (config-if)# no qos dpl

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

(config-if)# qosdscp-classify

Syntax: (config-if)# qos dscp-classify { zero | selected | any }

Explanation: Configure a classification method.

Parameters:

{ zero | selected | any }: Specify a classification method.

zero: Classify if incoming DSCP is 0.

selected: Classify only selected DSCP for which classification is enabled in DSCP Translation table

any: Classify all DSCP.

Negation: (config-if)# no qos dscp-classify

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

(config-if)# qosdscp-remark

Syntax: (config-if)# qos dscp-remark { rewrite | remap | remap-dp }

Explanation: Configure port egress rewriting of DSCP values.

Parameters:

{ rewrite | remap | remap-dp }: Specify an option.

rewrite: Rewrite DSCP field with classified DSCP value.

remap: Frame with DSCP from analyzer is remapped and remarked with the remapped DSCP value.

Depending on the frame's DP level, the remapped DSCP value is either taken from the DSCP Translation table, Egress Remap DP0 or DP1 field.

remap-dp: Frame with DSCP from analyzer is remapped and remarked with the remapped DSCP value. The remapped DSCP value is always taken from the DSCP Translation table, Egress Remap DP0 field.

Negation: (config-if)# no qos dscp-remark

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

(config-if)# qosdscp-translate

Syntax: (config-if)# qos dscp-translate

Explanation: Configure DSCP ingress translation of QoS for specific interface.

Negation: (config-if)# no qos dscp-translate

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

(config-if)# qos map cos-tag cos

Syntax: (config-if)# qos map cos-tag cos <cos> dpl <dpl> pcp <pcp> dei <dei>

Explanation: Configure (QoS class, DP level) to (PCP, DEI) Mapping of QoS for specific interface.

Parameters:

cos <cos: 0-7>: Specify a QoS class value. dpl <dpl:0-1>: Specify a DPL value (0 or 1).

pcp <pcp: 0-7>: Specify a PCP(Priority Code Point) value. dei <dei: 0-1>: Specify a DEI value (0 or 1).

Negation: (config-if)# no qos map cos-tag cos <cos> dpl <dpl>

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

(config-if)# qos map tag-cos pcp

Syntax: (config-if)# qos map tag-cos pcp <pcp> dei <dei> cos <cos> dpl <dpl>

Explanation: Configure (PCP, DEI) to (QoS class, DP level) Mapping of QoS for specific interface.

Parameters:

pcp <pcp: 0-7>: Specify a PCP (Priority Code Point) value. dei <dei: 0-1>: Specify a DEI value (0 or 1). cos <cos: 0-7>: Specify a QoS class value. dpl <dpl:0-1>: Specify a DPL value (0 or 1).

Negation: (config-if)# no qos map tag-cos pcp <pcp> dei <dei>

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

(config-if)# qos pcp

Syntax: (config-if)# qos pcp <pcp>

Explanation: Configure PCP value for specific interface.

Parameters:

pcp <pcp: 0-7>: Specify a PCP (Priority Code Point) value.

Negation: (config-if)# no qos pcp

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

(config-if)# qos policer

Syntax: (config-if)# qos policer <rate> [fps] [flowcontrol]

Explanation: Configure PCP value for specific interface.

Parameters:

<rate>: Indicate the rate for the policer. By default, 500kbps is used. The allowed range for kbps and fps is 100 to 1000000. The allowed range for Mbps and kfps is 1 to 3300Mbps.

[fps]: Rate is fps. By default, kbps is used.

[flowcontrol]: Enable Flow Control. If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames

Negation: (config-if)# no qos policer

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

(config-if)# qos queue-policer queue

Syntax: (config-if)# qos queue-policer queue <queue> <rate>

Explanation: Configure Ingress Queue Policers Rate of QoS for specific interface.

Parameters:

<queue: 0-7>: Specify a queue or a range.

<rate: 100-3300000>: Specify Policer rate in kbps.

Negation: (config-if)# no qos queue-policer queue <queue>

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

(config-if)# qos queue-shaper queue

Syntax: (config-if)# qos queue-shaper queue <queue> <rate> [excess]

Explanation: Configure Egress Queue Policers Rate of QoS for specific interface.

Parameters:

<queue: 0-7>: Specify a queue or a range.

<rate: 100-3300000>: Specify Policer rate in kbps. [excess]: Allow all excess bandwidth.

Negation: (config-if)# no qos queue-shaper queue <queue>

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

(config-if)# qos shaper

Syntax: (config-if)# qos shaper <rate>

Explanation: Configure Egress Queue Policers Rate of QoS for specific interface.

Parameters:

<rate: 100-3300000>: Specify Policer rate in kbps.

Negation: (config-if)# no qos shaper

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

(config-if)# qostag-remark

Syntax: (config-if)# qos tag-remark { pcp <pcp> dei <dei> | mapped }

Explanation: Configure the appropriate remarking mode used by this port.

Parameters:

{ pcp <pcp> dei <dei> | mapped }: Specify a remarking mode.

pcp <pcp> dei <dei>: Specify PCP and DEI value.

mapped: Use the mapping of the classified QoS class values and DP levels to PCP/DEI values.

Negation: (config-if)# no qos tag-remark

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

(config-if)# qos trust dscp

Syntax: (config-if)# qos trust dscp

Explanation: Enable DSCP Classification of QoS for specific interface.

Negation: (config-if)# no qos trust dscp

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

(config-if)# qos trust tag

Syntax: (config-if)# qos trust tag

Explanation: Enable VLAN tag Classification of QoS for specific interface.

Negation: (config-if)# no qos trust tag

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

(config-if)# qoswrr

Syntax: (config-if)# qos wrr <w0> <w1> <w2> <w3> <w4> <w5>

Explanation: Assign weight for QoS queueing method. WRR stands for Weighted Round Robin and uses default queue weights. The number of packets serviced during each visit to a queue depends on the percentages you configure for the queues.

Parameters:

<w0: 1-100>: Specify weight for queue 0.

<w1: 1-100>: Specify weight for queue 1.

<w2: 1-100>: Specify weight for queue 2.

<w3: 1-100>: Specify weight for queue 3.

<w4: 1-100>: Specify weight for queue 4.

<w5: 1-100>: Specify weight for queue 5.

Negation: (config-if)# no qos wrr

Show: # show qos

show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] } | storm | { qce [<qce>] }]

2.9.36 (config)# radius-server

(config)# radius-server attribute 32

Syntax: (config)# radius-server attribute 32 <id>

Explanation: Configure Radius attribute 32 string.

Parameters:

<id>: Specify Radius server identifier. The allowed characters are 1 to 253.

```
# config t
(config)# radius-server attribute 32 cabinet5aSW
```

Negation: (config)# no radius-server attribute 32

Show: # show radius-server [statistics]

(config)# radius-server attribute 4

Syntax: (config)# radius-server attribute 4 <ipv4>

Explanation: Configure NAS IPv4 address.

Parameters:

<ipv4>: Specify NAS IPv4 address.

Example: Set NAS IPv4 address to 100.1.1.25.

```
# config t
(config)# radius-server attribute 4 100.1.1.25
```

Negation: (config)# no radius-server attribute 4

Show: # show radius-server [statistics]

(config)# radius-server attribute 95

Syntax: (config)# radius-server attribute 95 <ipv6>

Explanation: Configure NAS IPv6 address.

Parameters:

<ipv6>: Specify NAS IPv6 address.

Negation: (config)# no radius-server attribute 95

Show: # show radius-server [statistics]

(config)# radius-server deadtime

Syntax: (config)# radius-server deadtime <minutes>

Explanation: Configure RADIUS server deadtime value. Deadtime is the period during which the switch will

not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually

trying to contact a server that it has already determined as dead.

Parameters:

<deadtime>: Specify RADIUS server deadtime value. The valid range is 1 to 1440 (minutes).

Example: Set RADIUS server to 60.

```
# config t
 (config)# radius-server deadtime 60
```

Negation: (config)# no radius-server deadtime

Show: # show radius-server [statistics]

(config)# radius-server host

Syntax: (config)# radius-server host <host_name> [auth-port <auth_port>] [acct-port <acct_port>] [timeout

<seconds>] [retransmit <retries>] [key <key>]

Explanation: This command is used to configure Radius server.

Parameters:

<host_name>: Specify the hostname or IP address for the radius server. The allowed characters are 1 to 255. [auth-port <auth_port>]: Specify the UDP port to be used on the RADIUS server for authentication.

[acct-port <acct_port>]: Specify the UDP port to be used on the RADIUS server for accounting.

[timeout <seconds>]: Specify a timeout value. If timeout value is specified here, it will replace the global timeout value. If you prefer to use the global value, leave this field blank.

[retransmit <retries>]: Specify a value for retransmit retry. If retransmit value is specified here, it will replace the global retransmit value. If you prefer to use the global value, leave this field blank.

[key <key>]: Specify a secret key. If secret key is specified here, it will replace the global secret key. If you prefer to use the global value, leave this field blank.

Negation: (config)# no radius-server host <host_name> [auth-port <auth_port>] [acct-port <acct_port>]

Show: # show radius-server [statistics]

(config)# radius-server key

Syntax: (config)# radius-server key <key>

Explanation: Configure RADIUS server key value. This key is shared between the RADIUS sever and the switch.

Parameters:

<key>: Specify RADIUS server secret key value. The valid range is 1 to 63.

Example: Set RADIUS server secret key to 803321

```
# config t
(config)# radius-server key 803321
```

Negation: (config)# no radius-server key

(config)# radius-server retransmit

Syntax: (config)# radius-server retransmit <retries>

Explanation: Configure the number of times to retransmit request packets to an authentication server that does not respond. If the server does not respond after the last retransmit is sent, the switch considers the authentication server is dead.

Parameters:

<retries>: Specify RADIUS server retransmit value. The valid range is 1 to 1000.

Example: Set RADIUS server retransmit value to 5

```
# config t
(config)# radius-server retransmit 5
```

Negation: (config)# no radius-server retransmit

Show: # show radius-server [statistics]

(config)# radius-servertimeout

Syntax: (config)# radius-server timeout <seconds>

Explanation: Configure the time the switch waits for a reply from an authentication server before it retransmits the request.

Parameters:

<seconds>: Specify RADIUS server timeout value. The valid range is 1 to 1000.

Example: Set RADIUS server timeout to 60

```
# config t
(config)# radius-server timeout 60
```

Negation: (config)# no radius-server timeout

Show: # show radius-server [statistics]

2.9.37 (config)# rmon

(config)# rmon alarm

Syntax: (config)# rmon alarm <id> <oid_str> <interval> { absolute | delta } rising-threshold <rising_threshold> [<rising_event_id>] falling-threshold <falling_threshold> [<falling_event_id>] { [rising | falling | both] }

Syntax: (config)# rmon alarm <id> { ifInOctets | ifInUcastPkts | ifInNUcastPkts | ifInDiscards | ifInErrors | ifInUnknownProtos | ifOutOctets | ifOutUcastPkts | ifOutNUcastPkts | ifOutDiscards | ifOutErrors } <ifIndex>

<interval> { absolute | delta } rising-threshold <rising_threshold> [<rising_event_id>] falling-threshold <falling_threshold> [<falling_event_id>] { [rising | falling | both] }

Explanation: Configure RMON alarm settings. RMON Alarm configuration defines specific criteria that will generate response events. It can be set to test data over any specified time interval and can monitor absolute or changing values. Alarms can also be set to respond to rising or falling thresholds.

Parameters:

<id>: Indicates the index of the entry. The range is from 1 to 65535.

<oid_str>: The object number of the MIB variable to be sampled. Only variables of the type ifEntry.n.n may be sampled. Possible variables are ifInOctets, ifInUcastPkts, ifInNUcastPkts, ifOutDiscards, ifErrors, ifInUnknownProtos, ifOutOctets, ifOutUcastPkts, ifOutNUcastPkts, ifOutDiscards, ifOutErrors.

<interval>: The polling interval for sampling and comparing the rising and falling threshold. The range is from 1to 2^31 (2147483647) seconds.

{ absolute | delta }: Test for absolute or relative change in the specified variable.

Absolute: The variable is compared to the thresholds at the end of the sampling period.

Delta: The last sample is subtracted from the current value and the difference is compared to the thresholds.

rising-threshold <rising_threshold>: If the current value is greater than the rising threshold and the last sample value is less than this threshold, then an alarm will be triggered. After a rising event has been generated, another such event will not be generated until the sampled value has fallen below the rising threshold, reaches the falling threshold, and again moves back up to the rising threshold. The threshold range is -2147483647 to 2147483647.

[<rising_event_id>]: Indicates the rising index of an event. The range is 1 - 65535.

falling-threshold <falling_threshold>: If the current value is less than the falling threshold, and the last sample value was greater than this threshold, then an alarm will be generated. After a falling event has been generated, another such event will not be generated until the sampled value has risen above the falling threshold, reaches the rising threshold, and again moves back down to the failing threshold. (Range: -2147483647 to 2147483647)

[<falling_event_id>]: Indicates the falling index of an event. The range is 0 - 65535.

{ [rising | falling | both] }: Specify a method that is used to sample the selected variable and calculate the value to be compared against the thresholds.

rising: Trigger alarm when the first value is larger than the rising threshold.

falling: Trigger alarm when the first value is less than the falling threshold.

both: Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold.

Negation: (config)# no rmon alarm <id>

Show: # show rmon alarm [<id_list>] # show rmon history [<id_list>]

show rmon statistics [<id_list>]

3.9.41.2(config)# rmon event

Syntax: (config)# rmon event <id> [log] [trap <community>] { [description <description>] }

Explanation: Configure RMON Event settings.

Parameters:

<id>: Specify an ID index. The range is 1 - 65535.

[log]: When the event is triggered, a RMON log entry will be generated.

[trap <community>]: A password-like community string sent with the trap. Although the community string can be set on this configuration page, it is recommended that it be defined on the SNMP trap configuration page prior to configuring it here. The allowed characters are 0 - 127.

{ [description <description>] }: Enter a descriptive comment for this entry.

Negation: (config)# no rmon event <id>

Show: # show rmon alarm [<id_list>] # show rmon history [<id_list>]

(config-if)# rmon collection history

Syntax: (config-if)# rmon collection history <id> [buckets <buckets>] [interval <interval>]

Explanation: RMON History Configuration is to collect statistics on a physical interface to monitor network utilization, packet types, and errors. A RMON historical record can be used to monitor intermittent problems.

Parameters:

<id>: Specify an ID index. The range is 1~65535.

[buckets <buckets>]: The number of buckets requested for this entry. The allowed range is 1~65535.

[interval <interval>]: Indicates the polling interval. By default, 1800 seconds is specified. The allowed range is 1~3600 seconds.

Negation: (config-if)# no rmon collection history <id>

Show: # show rmon history [<id_list>]

(config-if)# rmon collectionstats

Syntax: (config-if)# rmon collection stats <id>

Explanation: Configure RMON Statistics table using this command.

Parameters:

<id>: Specify an ID index. The range is 1~65535.

Negation: (config-if)# no rmon collection stats <id>

Show: # show rmon statistics [<id_list>]

2.9.38 (config)# spanning-tree

(config)# spanning-tree aggregation

Syntax: (config)# spanning-tree aggregation

Explanation: Enable aggregation mode of Spanning Tree.

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

Show: # show spanning-tree

(config-stp-aggr)# spanning-tree

Syntax: (config-stp-aggr)# spanning-tree

Explanation: Enable Spanning Tree under aggregation mode.

Negation: (config-stp-aggr)# no spanning-tree

Show: # show spanning-tree

(config-stp-aggr)# spanning-tree auto-edge

Syntax: (config-stp-aggr)# spanning-tree auto-edge

Explanation: Enable auto edge function. When enabled, a port is automatically determined to beat the edge of the network when it receives no BPDUs.

Negation: (config-stp-aggr)# no spanning-tree auto-edge

Show: # show spanning-tree

(config-stp-aggr)# spanning-tree bpdu-guard

Syntax: (config-stp-aggr)# spanning-tree bpdu-guard

Explanation: Enable BPDU guard function. This feature protects ports from receiving BPDUs. It can prevent loops by shutting down a port when a BPDU is received instead of putting it into the spanning tree discarding state. If enabled, the port will disable itself upon receiving valid BPDU's.

Negation: (config-stp-aggr)# no spanning-tree bpdu-guard

Show: # show spanning-tree

(config-stp-aggr)# spanning-tree edge

Syntax: (config-stp-aggr)# spanning-tree edge

Explanation: If an interface is attached to end nodes, you can set it to "Edge".

Negation: (config-stp-aggr)# no spanning-tree edge

Show: # show spanning-tree

(config-stp-aggr)# spanning-tree link-type

Syntax: (config-stp-aggr)# spanning-tree link-type { point-to-point | shared | auto }

Explanation: Configure the link type attached to an interface.

Parameters:

{ point-to-point | shared | auto }: Select the link type attached to an interface.

point-to-point: It is a point-to-point connection.

shared: It is a shared medium connection

auto: The switch automatically determines whether the interface is attached to a point-to-point link or shared medium.

Negation: (config-stp-aggr)# no spanning-tree link-type

Show: # show spanning-tree

(config-stp-aggr)# spanning-tree mst <instance> cost

Syntax: (config-stp-aggr)# spanning-tree mst <instance> cost { <cost> | auto }

Explanation: Configure MSTI and its ' path cost value.

Parameters:

mst <instance: 0-15>: Specify MST instance number. Specify "0" to denote CIST. Specify "1-15" to denote MSTI 1- 15.

cost { <cost> | auto }: Specify a Path cost value that is used to determine the best path between devices.

Valid values are 1 to 200000000. If "auto" mode is specified, the system automatically detects the speed and duplex mode to decide the path cost. Please note that path cost takes precedence over port priority.

Negation: (config-stp-aggr)# no spanning-tree mst <instance> cost

Show: # show spanning-tree

(config-stp-aggr)# spanning-tree mst <instance> port-priority

Syntax: (config-stp-aggr)# spanning-tree mst <instance> port-priority <prio>

Explanation: Configure MSTI and its ' port priority.

Parameters:

mst <instance: 0-15>: Specify MST instance number. Specify "0" to denote CIST. Specify "1-15" to denote MSTI 1- 15.

port-priority <prio>: Specify a port priority value.

Negation: (config-stp-aggr)# no spanning-tree mst <instance> port-priority

Show: # show spanning-tree

(config-stp-aggr)# spanning-tree restricted-role

Syntax: (config-stp-aggr)# spanning-tree restricted-role

Explanation: Enable restricted role function. If enabled, this 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.

Negation: (config-stp-aggr)# no spanning-tree restricted-role

Show: # show spanning-tree

(config-stp-aggr)# spanning-tree restricted-tcn

Syntax: (config-stp-aggr)# spanning-tree restricted-tcn

Explanation: Enable restricted TCN function. If enabled, this causes the port not to propagate received topology change notifications and topology changes to other ports.

Negation: (config-stp-aggr)# no spanning-tree restricted-tcn

Show: # show spanning-tree

(config)# spanning-tree edge bpdu-filter

Syntax: (config)# spanning-tree edge bpdu-filter

Explanation: Enable edge BPDU filtering function. The purpose of Port BPDU Filtering is to prevent the switch from sending BPDU frames on ports that are connected to end devices.

Example: Enable edge BPDU filtering function.

```
# config t
(config)# spanning-tree edge bpdu-filter
```

Negation: (config)# no spanning-tree edge bpdu-filter

Show: # show spanning-tree

(config)# spanning-tree edge bpdu-guard

Syntax: (config)# spanning-tree edge bpdu-guard

Explanation: Enable edge BPDU guard function. Edge ports generally connect directly to PC, file servers or printers. Therefore, edge ports are configured to allow rapid transition. Under normal situations, edge ports should not receive configuration BPDUs. However, if they do, this probably is due to malicious attacks or

mis-settings. When edge ports receive configuration BPDUs, they will be automatically set to non-edge ports and start a new spanning tree calculation process.

BPDU Guard is therefore used to prevent the device from suffering malicious attacks. With this function enabled, when edge ports receive configuration BPDUs, STP disables those affected edge ports. After a period of recovery time, those disabled ports are re-activated.

Example: Enable edge BPDU guard function.

```
# config t
(config)#  spanning-tree edge bpdu-guard
```

Negation: (config)# no spanning-tree edge bpdu-guard

Show: # show spanning-tree

(config)# spanning-tree mode

Syntax: (config)# spanning-tree mode { stp | rstp | mstp }

Parameters:

{ stp | rstp | mstp }: Specify one of the STP protocol versions.

Explanation: Configure the desired STP protocol version.

Example: Set the spanning tree mode to MSTP.

```
# config t
(config)# spanning-tree mode mstp
```

Negation: (config)# no spanning-tree mode

Show: # show spanning-tree

(config)# spanning-tree mst <instance> priority <prio>

Syntax: (config)# spanning-tree mst <instance> priority <prio>

Parameters:

<instance: 0-7>: Specify an instance ID. "0" means CIST. "1-7" means MSTI 1-7.

<prio: 0-61440>: Specify a priority value.

Explanation: Specify an appropriate priority for a MSTI instance. Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the root device.

However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Note that lower numeric values indicate higher priority. The bridge priority plus the MSTI instance number, concatenated with the 6- byte MAC address of the switch forms a Bridge Identifier.

Example: Map MST Instance 1 to priority 61440.

```
# config t
(config)# spanning-tree mst 1 priority 61440
```

Negation: (config)# no spanning-tree mst <instance> priority

Show: # show spanning-tree

(config)# spanning-tree mst <instance> vlan <v_vlan_list>

Syntax: (config)# spanning-tree mst <instance> vlan <v_vlan_list>

Parameters:

<instance: 0-7>: Specify an instance ID. "0" means CIST. "1-7" means MSTI 1-7.

<v_vlan_list>: Specify a list of VLANs for the specified MST instance. Separate VLANs with a comma and use hyphen to denote a range of VLANs. (Example: 2,5,20-40)

Explanation: Specify VLANs mapped to a certain MSTI. Both a single VLAN and a range of VLANs are allowed.

Example: Map MST Instance 1 to VLAN 90 and VLAN 101-105.

```
# config t
(config)# spanning-tree mst 1 vlan 90,101-105
```

Negation: (config)# no spanning-tree mst <instance> vlan

(config)# spanning-tree mst forward-time

Syntax: (config)# spanning-tree mst forward-time <fwdtime>

Parameters:

<fwdtime: 4-30>: Specify forward delay value between 4 and 30 (seconds).

Explanation: Fort STP bridges, the Forward Delay is the time spent in each Listening and Learning state before the Forwarding state is entered. This delay occurs when a new bridge comes onto a network.

Example: Set the forward delay to 15 seconds.

```
# config t
(config)# spanning-tree mst forward-time 15
```

Negation: (config)# no spanning-tree mst forward-time

Show: # show spanning-tree

(config)# spanning-treemst max-age

Syntax: (config)# spanning-tree mst max-age <maxage> [forward-time <fwdtime>]

Parameters:

<maxage: 6-40>: Specify the max age value. The valid range is from 6 to 40.

[forward-time <fwdtime>]: Fort STP bridges, the Forward Delay is the time spent in each Listening and Learning state before the Forwarding state is entered. This delay occurs when a new bridge comes onto a network. Valid values are 4-30 seconds.

Explanation: If another switch in the spanning tree does not send out a hello packet for a period of time, it is considered to be disconnected. Valid values are 6 to 40 seconds, and Max Age values must be smaller than or equal to (Forward Delay-1)*2.

Example: Set the max age to 20 seconds.

```
# config t
(config)# spanning-tree mst max-age 20
```

Negation: (config)# no spanning-tree mst max-age

Show: # show spanning-tree

(config)# spanning-tree mst max-hops

Syntax: (config)# spanning-tree mst max-hops <maxhops>

Parameters:

<maxhops>: Specify the maximum hop count value. The valid range is from 6 to 40.

Explanation: The maximum number of hops allowed for MST region before a BPDU is discarded. Each bridge decrements the hop count by one before passing on the BPDU. When the hop count reaches zero, the BPDU is discarded. The default hop count is 20. The allowed range is 6-40.

Example: Set the maximum hop count to 20.

```
# config t
(config)# spanning-tree mst max-hops 20
```

Negation: (config)# no spanning-tree mst max-hops

Show: # show spanning-tree

(config)# spanning-tree mst name

Syntax: (config)# spanning-tree mst name <name> revision <v_0_to_65535>

Parameters:

name <name>: Specify a name for this MSTI. By default, the switch's MAC address is used. The maximum length is 32 characters. In order to share spanning trees for MSTI, bridges must have the same configuration name and revision value.

revision <v_0_to_65535>: Specify a revision number for this MSTI. The allowed range is 0 - 65535.

Explanation: Configure a name and revision number for this MSTI.

Negation: (config)# no spanning-tree mst name

Show: # show spanning-tree

(config)# spanning-tree recovery interval

Syntax: (config)# spanning-tree recovery interval <interval>

Parameters:

<interval>: The time that has to pass before a port in the error-disabled state can be enabled. The allowed range is 30 – 86400 (seconds).

Explanation: When enabled, a port that is in the error-disabled state can automatically be enabled after a certain time.

Example: Set the spanning tree recovery interval to 50.

```
# config t
(config)# spanning-tree recovery interval 50
```

Negation: (config)# no spanning-tree recovery interval

Show: # show spanning-tree

(config)# spanning-tree transmit hold-count

Syntax: (config)# spanning-tree transmit hold-count <holdcount>

Parameters:

<holdcount:1-10>: Specify the transmit hold-count. The allowed transmit hold count is 1 to 10.

Explanation: The number of BPDU sent by a bridge port per second. When exceeded, transmission of the next BPDU will be delayed. By default, it is set to 6. The allowed transmit hold count is 1 to 10. Please note that increasing this value might have a significant impact on CPU utilization and decreasing this value might slow down convergence. It is recommended to remain Transmit Hold Count to the default setting.

Example: Set the spanning tree transmit hold-count to 6.

```
# config t
(config)# spanning-tree transmit hold-count 6
```

Negation: (config)# no spanning-tree transmit hold-count

Show: # show spanning-tree

(config-if)# spanning-tree

Syntax: (config-if)# spanning-tree

Explanation: Enable Spanning Tree on this interface.

Negation: (config-if)# no spanning-tree

Show: # show spanning-tree

(config-if)# spanning-tree auto-edge

Syntax: (config-if)# spanning-tree auto-edge

Explanation: Enable auto edge function on this interface. When enabled, a port is automatically determined to beat the edge of the network when it receives no BPDUs.

Negation: (config-if)# no spanning-tree auto-edge

Show: # show spanning-tree

(config-if)# spanning-tree bpdu-guard

Syntax: (config-if)# spanning-tree bpdu-guard

Explanation: Enable BPDU guard function on this interface. This feature protects ports from receiving

BPDUs. It can prevent loops by shutting down a port when a BPDU is received instead of putting it into the spanning tree discarding state. If enabled, the port will disable itself upon receiving valid BPDU's.

Negation: (config-if)# no spanning-tree bpdu-guard

Show: # show spanning-tree

(config-if)# spanning-tree edge

Syntax: (config-if)# spanning-tree edge

Explanation: If an interface is attached to end nodes, you can set it to "Edge".

Negation: (config-if)# no spanning-tree edge

Show: # show spanning-tree

(config-if)# spanning-tree link-type

Syntax: (config-if)# spanning-tree link-type { point-to-point | shared | auto }

Explanation: Configure the link type attached to an interface.

Parameters:

{ point-to-point | shared | auto }: Select the link type attached to an interface.

point-to-point: It is a point-to-point connection.

shared: It is a shared medium connection

auto: The switch automatically determines whether the interface is attached to a point-to-point link or shared medium.

Negation: (config-if)# no spanning-tree link-type

Show: # show spanning-tree

(config-if)# spanning-tree mst <instance> cost

Syntax: (config-if)# spanning-tree mst <instance> cost { <cost> | auto }

Explanation: Configure MSTI and its ' path cost value.

Parameters:

mst <instance: 0- 15>: Specify MST instance number. Specify "0" to denote CIST. Specify "1-15" to denote MSTI 1- 15.

cost { <cost> | auto }: Specify a Path cost value that is used to determine the best path between devices.

Valid values are 1 to 200000000. If "auto" mode is specified, the system automatically detects the speed and duplex mode to decide the path cost. Please note that path cost takes precedence over port priority.

Negation: (config-if)# no spanning-tree mst <instance> cost

Show: # show spanning-tree

(config-if)# spanning-tree mst <instance> port-priority

Syntax: (config-if)# spanning-tree mst <instance> port-priority <prio>

Explanation: Configure MSTI and its' port priority.

Parameters:

mst <instance: 0-15>: Specify MST instance number. Specify "0" to denote CIST. Specify "1-15" to denote MSTI 1- 15.

port-priority <prio>: Specify a port priority value.

Negation: (config-if)# no spanning-tree mst <instance> port-priority

Show: # show spanning-tree

(config-if)# spanning-tree restricted-role

Syntax: (config-if)# spanning-tree restricted-role

Explanation: Enable restricted role function. If enabled, this 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.

Negation: (config-if)# no spanning-tree restricted-role

Show: # show spanning-tree

(config-if)# spanning-tree restricted-tcn

Syntax: (config-if)# spanning-tree restricted-tcn

Explanation: Enable restricted TCN function. If enabled, this causes the port not to propagate received topology change notifications and topology changes to other ports.

Negation: (config-if)# no spanning-tree restricted-tcn

Show: # show spanning-tree

2.9.39 (config-if)# speed

Syntax: (config-if)# speed { 1000 | 100 | 10 | auto { [10] [100] [1000] } }

Explanation: Configure port speed for this specific interface.

Negation: (config-if)# no speed

Show: # show interface (<port_type> [<v_port_type_list>]) status

2.9.40 (config)# switchport

(config)# switchport vlan mapping

Syntax: (config)# switchport vlan mapping <group ID> <vlan_list> <translation_vlan>

Explanation: VLAN Translation is especially useful for users who want to translate the original VLAN ID to a new VLAN ID so as to exchange data across different VLANs and improve VLAN scaling. VLAN translation replaces an incoming C- VLAN tag with an S-VLAN tag instead of adding an additional tag. When configuring VLAN Translation, both ends of the link normally must be able to replace tags appropriately. In other words, both ends must be configured to translate the C-VLAN tag to S-VLAN tag and S-VLAN tag to C-VLAN tag appropriately in a network. Note that only access ports support VLAN translation. It is not recommended to configure VLAN Translation on trunk ports.

Parameters:

<group ID: 1-28>: Indicate the Group ID that applies to this translation rule.

<vlan_list>: Indicate the VLAN ID that will be mapped to a new VID.

<translation_vlan>: Indicate the new VID to which VID of ingress frames will be changed.

Example: Map the group ID 5 with VLAN ID 100 to be translated to 201.

```
# config t
(config)# switchport vlan mapping 5 100 201
```

Negation: (config)# no switchport vlan mapping <group> <v_vlan_id_from>

(config-if)# switchport accessvlan

Syntax: (config-if)# switchport access vlan <pvid> **Explanation:** Configure access VLAN ID for this interface.

Parameters:

<pvid>: Indicate the access VLAN ID (PVID) for this interface.

Example: Set the interface 1's access VLAN ID to 10.

```
# config t
(config)# interface GigabitEthernet 1/1
(config-if)# switchport access vlan 10
(config-if)#
```

Negation: (config-if)# no switchport access vlan

Show: # show vlan status

(config-if)# switchport forbiddenvlan

Syntax: (config-if)# switchport forbidden vlan { add | remove } <vlan_list>

Explanation: Add or remove a port from the forbidden VLAN list.

Parameters:

{ add | remove }: Add or remove this specific interface from the forbidden VLAN list.

<vlan_list>: Specify the VLAN ID.

Negation: (config-if)# no switchport access vlan

Show: > show switchport forbidden [{ vlan <vid> } | { name <name> }] # show switchport forbidden [{ vlan <vid> } | { name <name> }]

(config-if)# switchport hybrid acceptable-frame-type

Syntax: (config-if)# switchport hybrid acceptable-frame-type { all | tagged | untagged }

Explanation: Configure the accepted frame types. Available options include "all" (accept all frames), "tagged" (accept only tagged frames), "untagged" (accept only untagged frames). This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, frame type is set to All.

Parameters:

{ all | tagged | untagged }: Specify the frame type for this interface. Available options include "all" (accept all frames), "tagged" (accept only tagged frames), "untagged" (accept only untagged frames).

Negation: (config-if)# no switchport hybrid acceptable-frame-type

Show: # show vlan status

(config-if)# switchport hybrid allowed vlan

Syntax: (config-if)# switchport hybrid allowed vlan { all | none | [add | remove | except] <vlan_list> }

Explanation: Configure allowed VLANs when this interface is in hybrid mode.

Parameters:

{ all | none | [add | remove | except] <vlan_list> }: Specify one of the options.

all: All VLANs.

none: No VLANs.

add: Add VLANs to the current list.

remove: Remove VLANs from the current list

except: All VLANs except the following specified in <vlan_list>.

<vlan_list>: Specify the VLAN list.

Negation: (config-if)# no switchport hybrid allowed vlan

Show: # show vlan status

(config-if)# switchport hybrid egress-tag

Syntax: (config-if)# switchport hybrid egress-tag { none | all [except-native] }

Explanation: Determines egress tagging of a port.

Parameters:

{ none | all [except-native] }: Determines egress tagging of a port.

none: All VLANs are untagged.

all: All VLANs are tagged.

all [except-native]: All VLANs except the configured PVID will be tagged.

Negation: (config-if)# no switchport hybrid egress-tag

Show: # show vlan status

(config-if)# switchport hybrid ingress-filtering

Syntax: (config-if)# switchport hybrid ingress-filtering

Explanation: Enable ingress filtering function on this specific interface. If Ingress Filtering is enabled and the ingress port is not a member of a VLAN, the frame from the ingress port is discarded. By default, ingress filtering is disabled.

Negation: (config-if)# no switchport hybrid ingress-filtering

Show: # show vlan status

(config-if)# switchport hybrid native vlan

Syntax: (config-if)# switchport hybrid native vlan <pvid>

Explanation: Configures the VLAN identifier in Hybrid mode for the port. The allowed values are from 1 through 4095. The default value is 1.

Parameters:

<pvid>: Specify the port VLAN ID for this specific interface.

Negation: (config-if)# no switchport hybrid native vlan

Show: # show vlan status

(config-if)# switchport hybrid port-type

Syntax: (config-if)# switchport hybrid port-type { unaware | c-port | s-port | s-custom-port }

Explanation: Configures the port type in Hybrid mode for the port.

Parameters:

{ unaware | c-port | s-port | s-custom-port }: There are four port types available. Each port type's ingress and egress action is described in the following table.

Action Port Type	Ingress Action	Egress Action
Unaware	When a tagged frame is received on a port, If the tagged frame with TPID=0x8100, it becomes a double-tag frame and is forwarded. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of frame transmitted by Unaware port will be set to 0x8100. The final status of the frame after egressing are also affected byegress rule.
	When anuntagged frame is received on a port, a tag (PVID) is attached and then forwarded.	
C-port	When a tagged frame is received on a port, If a tagged frame with TIPID=0x8100, it is forwarded. If the TPID of tagged frame is not 0x8100	TheTPIDof frame transmittedbyC-port will be set to 0x8100.
	(ex. 0x88A8), it will be discarded.	
	When anuntagged frame is received on a port, a tag (PVID) is attached and then forwarded.	
S-port	When a tagged frame is received on a port, If a tagged frame with TPID=0x88A8, it is forwarded. If the TPID of tagged frame is not 0x88A8 (ex. 0x8810), it will be discarded.	The TPIDofframe transmitted byS-port will be set to 0x88A8
	When anuntagged frame is received on a port, a tag (PVID) is attached and then forwarded.	
S-custom port	When a tagged frame is received on a port, If a tagged frame with TPID=0x88A8, it is forwarded. If the TPID of tagged frame is not 0x88A8 (ex. 0x8810), it will be discarded.	The TIPID of frame transmitted by S-custom-port will be set to an self-customized value, which can be set by the user using the column of Ethertype for Custom S-ports.
	When anuntagged frame is received on a port, a tag (PVID) is attached and then forwarded.	

Negation: (config-if)# no switchport hybrid port-type

Show: # show vlan status

(config-if)# switchport mode

Syntax:(config-if)# switchport mode { access | trunk | hybrid }

Explanation: Configure VLAN mode for this specific interface.

Parameters:

{ access | trunk | hybrid }: Specify the VLAN mode.

Negation: (config-if)# no switchport mode

Show: # show vlan status

(config-if)# switchport trunk allowed vlan

Syntax: (config-if)# switchport trunk allowed vlan { all | none | [add | remove | except] <vlan_list> }

Explanation: Configure allowed VLANs when this interface is in trunk mode.

Parameters:

{ all | none | [add | remove | except] <vlan_list> }: Specify one of the options.

all: All VLANs.

none: No VLANs.

add: Add VLANs to the current list.

remove: Remove VLANs from the current list

except: All VLANs except the following specified in <vlan_list>.

<vlan_list>: Specify the VLAN list.

Negation: (config-if)# no switchport trunk allowed vlan

Show: # show vlan status

(config-if)# switchport trunk native vlan

Syntax: (config-if)# switchport trunk native vlan <pvid>

Explanation: Configure native VLAN ID in trunk mode for this specific interface.

Parameters:

<pvid>: Specify the port VLAN ID for this specific interface.

Negation: (config-if)# no switchport trunk native vlan

Show: # show running-config

(config-if)# switchport trunk vlan tag native

Syntax: (config-if)# switchport trunk vlan tag native

Explanation: Configure this specific interface to tag native VLAN traffic.

Negation: (config-if)# no switchport trunk vlan tag native

(config-if)# switchport vlan ip-subnet id

Syntax: (config-if)# switchport vlan ip-subnet id <vce_id> <ipv4> vlan <vid>

Explanation: IP Subnet-based VLAN configuration is to map untagged ingress frames to a specific VLAN if the source address is found in the IP subnet-to-VLAN mapping table. When IP subnet-based VLAN classification is enabled, the source address of untagged ingress frames are checked against the IP subnet-to-VLAN mapping table. If an entry is found for that subnet, these frames are assigned to the VLAN indicated in the entry. If no IP subnet is matched, the untagged frames are classified as belonging to the receiving port's VLAN ID (PVID).

Parameters:

<vce_id: 1-128>: Specify indexof the entry. Valid range is 1~128.

<ipv4>: Specify IP address and subnet mask. The format is xx.xx.xx.xx/mm.mm.mm.mm.

<vid>: Indicate the VLAN ID.

Negation: (config-if)# no switchport vlan ip-subnet id <vce_id_list>

Show: # show vlan ip-subnet [id <subnet_id>]

(config-if)# switchport vlan mac

Syntax: (config-if)# switchport vlan mac <mac_addr> vlan <vid>

Explanation: This command is to set up VLANs based on source MAC addresses. When ingress untagged frames are received by a port, source MAC address is processed to decide which VLAN these untagged frames belong. When source MAC addresses does not match the rules created, untagged frames are assigned to the receiving port's native VLAN ID (PVID).

Parameters:

<mac_addr>: Indicate the source MAC address. Please note that the source MAC address can only map to one VLAN ID.

vlan<vid>: Map this MAC address to the associated VLAN ID.

Negation: (config-if)# no switchport vlan mac <mac_addr> vlan <vid>

Show: # show vlan mac [address <mac_addr>]

(config-if)# switchport vlan mapping

Syntax: (config-if)# switchport vlan mapping <group>

Explanation: Configure group VLAN mapping table for this specific interface.

Parameters:

<group: 1-20>: Indicate the Group ID that applies to this rule.

Negation: (config-if)# no switchport vlan mapping

(config-if)# switchport vlan protocol group

Syntax: (config-if)# switchport vlan protocol group <grp_id> vlan <vid>

Explanation: Configure VLAN protocol group for this specific interface.

Parameters:

<grp_id: word 16>: Indicate the descriptive name for this entry. This field only allows 16 alphabet characters (a-z; A-z) or integers (0-9).

<vid>: Specify the VLAN ID that applies to this rule.

Negation: (config-if)# no switchport vlan protocol group <grp_id> vlan <vid>

Show: # show vlan protocol [eth2 { <etype> | arp | ip | ipx | at }] [snap { <oui> | rfc-1042 | snap-8021h } <pid>] [llc

<dsap> <ssap>]

2.9.41 (config)# tacacs-server

(config)# tacacs-server timeout

Syntax: (config)# tacacs-server timeout <seconds>

Explanation: The time the switch waits for a reply from a TACACS+ server before it retransmits the request.

Parameters:

<seconds:1-1000>: Specify a value for timeout. The allowed timeout range is between 1 and 1000.

Negation: (config)# no tacacs-server timeout

Show: # show tacacs-server

(config)# tacacs-server deadtime

Syntax: (config)# tacacs-server deadtime <minutes>

Explanation: Deadtime is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

Parameters:

<minutes:1-1440>: Specify a value for tacacs-server deadtime. The allowed deadtime range is between 1 to 1440 minutes.

Negation: (config)# no tacacs-server deadtime

Show: # show tacacs-server

(config)# tacacs-server key

Syntax: (config)# tacacs-server key <key>

Explanation: Specify the secret key up to 63 characters. This is shared between a TACACS+ sever and the switch.

Parameters:

<key:1-63>: Specify a shared secret key value.

Negation: (config)# no tacacs-server key

Show: # show tacacs-server

(config)# tacacs-server host

Syntax: (config)# tacacs-server host <host_name> [port <port>] [timeout <seconds>] [key <key>]

Explanation: Configure radius server settings.

Parameters:

<host_name>: Specify a hostname or IP address for the TACACS+ server.

[port <port>]: Specify the TCP port number to be used on a TACACS+ server for authentication.

[timeout <seconds>]: If timeout value is specified here, it will replace the global timeout value. If you prefer to use the global value, leave this field blank.

[key <key>]: If secret key is specified here, it will replace the global secret key. If you prefer to use the global value, leave this field blank.

Negation: (config)# no tacacs-server host <host_name> [port <port>]

Show: # show tacacs-server

2.9.42 (config)# upnp

(config)# upnp

Syntax: (config)# upnp

Explanation: Enable upnp operation.

Example: Enable upnp operation

```
# config t
(config)# upnp
(config)#
```

Negation: (config)# no upnp

Show: # show upnp

(config)# upnp advertising-duration

Syntax: (config)# upnp advertising-duration <v_100_to_86400>

Parameters:

<v_100_to_86400>: Specify the advertising duration. The allowed range is 100 to 86400 (seconds).

Explanation: This defines how often an UPnP advertisement is sent. The duration is carried in Simple

Service Discover Protocol (SSDP) packets which informs a control point how often it should receive a SSDP advertisement message from the switch. By default, the advertising duration is set to 100 seconds. However, due to the unreliable nature of UDP, it is recommended to set to the shorter duration since the shorter the duration, the fresher is UPnP status.

Example: Set the upnp advertising duration to 150 seconds.

```
# config t
(config)# upnp advertising-duration 150
```

Negation: (config)# no upnp advertising-duration

Show: # show upnp

(config)# upnp ttl

Syntax: (config)# upnp ttl <v_1_to_255>

Parameters:

<v_1_to_255>: Specify the ttl (time to live) value. The allowed range is 1 to 255.

Explanation: TTL (Time to live) is used to configure how many steps an UPnP advertisement can travel before it disappears.

Example: Set the upnp ttl value to 10.

```
# config t
(config)# upnp ttl 10
```

Negation: (config)# no upnp ttl

Show: # show upnp

2.9.43 (config)# username

(config)# username<username>privilege<priv>password encrypted

Syntax: (config)# username <username> privilege <priv> password encrypted <encry_password>

Explanation: By default, there is only one user, 'admin', assigned the highest privilege level of 15. Use this command to configure a new user account.

Parameters:

username <username: word31>: Specify a new username. The allowed characters are 31.

privilege <priv: 0-15>: Specify the privilege level for this new user account. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But other values need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance

(software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

password encrypted <encry_password: 4-44>: Specify the encrypted password for this new user account. The ENCRYPTED (hidden) user password. Notice the ENCRYPTED 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.

Example: Create the new user account with the following settings.

```
# config t
(config)# username mis4jack privilege 15 password encrypted jack30125
```

Negation: (config)# no username <username>

Show: >show users

#show users

(config)# username<username>privilege<priv>passwordnone

Syntax: (config)# username <username> privilege <priv> password none

Explanation: By default, there is only one user, 'admin', assigned the highest privilege level of 15. Use this command to configure a new user account without password

Parameters:

username <username: word31>: Specify a new username. The allowed characters are 31.

privilege <priv: 0-15>: Specify the privilege level for this new user account. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But other values need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance

(software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

password none: No password for this user account.

Example: Create the new user account with the following settings.

```
# config t
(config)# username mis4jack privilege 15 password none
```

Negation: (config)# no username <username>

Show: >show users

#show users

(config)# username<username>privilege<priv>password unencrypted

Syntax: (config)# username <username> privilege <priv> password unencrypted <password>

Explanation: By default, there is only one user, 'admin', assigned the highest privilege level of 15. Use this command to configure a new user account with unencrypted password.

Parameters:

username <username: word31>: Specify a new username. The allowed characters are 31.

privilege <priv: 0-15>: Specify the privilege level for this new user account. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But other values need to refer to each group privilege level. User's privilege should be same or greater than the

group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance

(software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

password unencrypted <password: line31>: Specify the unencrypted password for this user account. The

UNENCRYPTED (Plain Text) user password. Any printable characters including space is accepted.

Example: Create the new user account with the following settings.

```
# config t
(config)# username mis4jack privilege 15 password unencrypted jack30125
```

Negation: (config)# no username <username>

Show: >show users

#show users

2.9.44 (config)# vlan

(config)# vlan

Syntax: (config)# vlan <vlist> **Explanation:** Configure allowed VLANs. **Parameters:**

<vlist>: This shows the allowed access VLANs. This setting only affects ports set in "Access" mode. Ports in other modes are members of all VLANs specified in "Allowed VLANs" field. By default, only VLAN 1 is specified. More allowed access VLANs can be entered by specifying the individual VLAN ID separated by comma. If you want to specify a range, separate it by a dash. For example, 1, 5,10,12-15,100. Once Enter is pressed, the prompt changes to (config-vlan)#

Example: Add VID 1,5,10,12-15,100 to the allowed VLAN list.

```
# config t
(config)# vlan 1,510,12-15,100
(config-vlan)#
```

Negation: (config)# no vlan { { ethertype s-custom-port } | <vlan_list> }

(config)# vlan ethertype s-custom-port

Syntax: (config)# vlan ethertype s-custom-port <etype> **Explanation**: Configure ether type used for customer s-ports. **Parameters:**

ethertype s-custom-port <etype>: Specify ether type used for customer s-ports. The valid range is 0x0600 to 0xffff.

Example: Set ether type for customer s-port to 0x88a8.

```
# config t
 (config)# vlan ethertype s-custom-port 0x88a8
```

Negation: (config)# no vlan { { ethertype s-custom-port } | <vlan_list> }

(config)# vlan protocol

Syntax: (config)# vlan protocol { { eth2 { <etype> | arp | ip | ipx | at } } | { snap { <oui> | rfc-1042 | snap-8021h }

<pid> } | { llc <dsap> <ssap> } } group <grp_id>

Explanation: The network devices required to support multiple protocols cannot be easily grouped into a

common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type being used by the inbound packets.

Parameters:

protocol { { eth2 { <etype> | arp | ip | ipx | at } } | { snap { <oui> | rfc-1042 | snap-8021h } <pid> } | { llc <dsap> <ssap> } }: There are three frame types available for selection; these are "Ethernet", "SNAP", and "LLC". The value field will need to be changed accordingly.

eth2 (Ethernet): Ether Type (etype) value. By default, it is set to 0x0800. The range allowed is 0x0600 to 0xffff.

SNAP: This includes OUI (Organizationally Unique Identifier) and PID (Protocol ID) values.

OUI: A value in the format of xx-xx-xx where each pair (xx) in the string is a hexadecimal value in the ranges of 0x00-0xff.

PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type field value for the protocol running on top of SNAP. If the OUI is that of a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of the OUI field is 00-00-00, then value of the PID will be etherType (0x0600-0xffff), and if value of the OUI is other than 00-00-00, then valid value of the PID will be any value from 0x0000 to 0xffff.

LLC (Logical Link Control): This includes DSAP (Destination Service Access Point) and SSAP (Source Service Access Point) values. By default, the value is 0xff. Valid range is 0x00 to 0xff.

group <grp_id>: Indicate the descriptive name for this entry. This field only allows 16 alphabet characters (a-z; A-Z) or integers (0-9).

Example: Set VLAN protocol to eth2 0x88a8.

```
# config t
(config)# vlan protocol eth2 0x88a8 group a12
```

Negation: (config)# no vlan protocol { { eth2 { <etype> | arp | ip | ipx | at } } | { snap { <oui> | rfc-1042 | snap-8021h }

<pid> } | { llc <dsap> <ssap> } } group <grp_id>

Show: # show vlan protocol [eth2 { <etype> | arp | ip | ipx | at }] [snap { <oui> | rfc-1042 | snap-8021h } <pid>] [llc

<dsap> <ssap>]

2.9.45 (config)# web privilege group

Syntax: (config)# web privilege group <group_name> level { [cro <cro>] [crw <crw>] [sro <sro>] [srw <srw>] }*1

Explanation: Assign Aggregation group to crw (configuration/excute read-write) level 15.

Parameters:

group <group_name>: This name identifies the privilege group. Valid words are 'Aggregation' 'DHCP' 'Debug' 'Dhcp_Client' 'Diagnostics' 'EPS' 'ERPS' 'ETH_LINK_OAM' 'EVC' 'IP2"IPMC_Snooping' 'LACP'

'LLDP' 'Loop_Protect' 'MAC_Table' 'MEP' 'MVR' 'Maintenance' 'Mirroring' 'NTP' 'POE' 'PTP' 'Ports"Private_VLANs' 'QoS' 'RPC' 'Security' 'Spanning_Tree' 'System' 'Timer' 'UPnP' 'VCL'

'VLAN_Translation' 'VLANs' 'Voice_VLAN'.

level { [cro <cro: 0-15>] [crw <crw: 0-15>] [sro <sro: 0-15>] [srw <srw: 0-15>] }*1: Every group has an authorization Privilege level for the following sub groups:

cro (configuration read-only): The privilege level is 1 to 15.

crw (configuration/execute read-write): The privilege level is 1 to 15. sro (status/statistics read-only): The privilege level is 1 to 15.

srw (status/statistics read-write): The privilege level is 1 to 15.

User Privilege should be the same or greater than the authorization Privilege level to have access to that group.

Example: Set Voice VLAN to VID 1000.

```
# config t
 (config)#  web privilege group aggregation level crw 15
```

Negation: (config)# no web privilege group <group_name> level

Show: >show web privilege group <group_name> level # show web privilege group <group_name> level