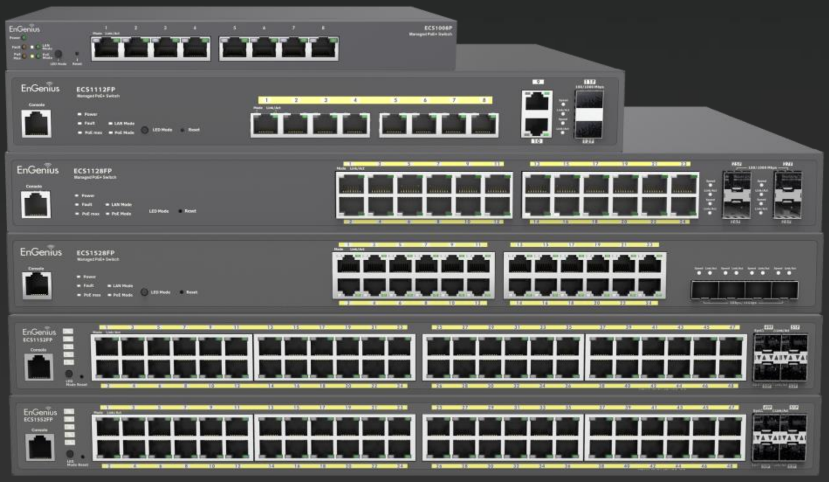
EnGenius®

Business Solutions

Command Line Interface User Manual

Cloud Managed PoE Switch



ECS Switch Series

version 1.0

Table of Contents

Key Conventions

Keyboard Shortcuts

□

- **Up Arrow / Down Arrow** - Displays the previously executed command.
- **Backspace / Ctrl + H** - Removes a single character.
- **TAB** - Completes a command without typing the full word.
- **Left Arrow / Right Arrow** - Traverses the current line.

Others

□

- ? - helps to list the available command
- Q - exits and returns to the switch’s prompt
- History - displays the command history list

CLI Command Modes

The following table format lists the different CLI command modes. Depending on the CLI mode, the prompt will be specific.

Command Mode	Access Method	Prompt
Privileged EXEC	This is the initial mode to start a session.	<*Switch Name*>*#*
Global Configuration	The EXEC mode command ***configure terminal*** is used to enter the Global Configuration mode.	<*Switch Name*> (config)#
Interface Configuration	The Global Configuration mode command ***interface*** ***<interfacetype><interfaceid>*** is used to enter the Interface configuration mode.	<*Switch Name*> (config-if)#
Interface Range Mode	The Global Configuration mode command ***interface range*** ***({ <interfacetype><slot/port-port>} {vlan <vlan-id(1-4094)>-<vlan-id(2-4094)>})*** is used to enter the Interface range mode.	<*Switch Name*> (config-if-range)#
SNTP Configuration	The SNTP Configuration mode command ***sntp*** is used to enter the SNTP configuration mode.	<*Switch Name*> (config-sntp)#
Config-VLAN	The Global configuration mode	<*Switch Name*> (config-vlan)#

	command ***vlan vlan-id*** is used to enter the Config-VLAN mode.	
Line Configuration	The Line Configuration mode command ***line cli*** is used to enter the Line configuration mode.	<*Switch Name*> (config-line)#
IPV4 ACL Extended Access List Configuration	The IPV4 ACL Extended Access List configuration mode command ***ip access-list extended <name>*** is used to enter the IPV4 ACL Extended Access List configuration mode.	<*Switch Name*> (config-ext-nacl)#
IPV6 ACL Extended Access List Configuration	The IPV6 ACL Extended Access List configuration mode command ***ipv6 access-list extended <name>*** is used to enter the IPV6 ACL Extended Access List configuration mode.	<*Switch Name*> (config-ipv6-acl)#
MAC ACL Extended Access List Configuration	The MAC ACL Extended Access List configuration mode command ***mac access-list extended <name>*** is used to enter the MAC ACL Extended Access List configuration mode.	<*Switch Name*> (config-ext-macl)#
Policy Map Configuration Mode	The Policy Map configuration mode command ***class-policy <name>*** is used to enter the Policy Map configuration mode.	<*Switch Name*> (config-qc-ply)#
MSTP Configuration Mode	The MSTP Configuration mode command ***spanning-tree mst configuration*** is used to enter the	<*Switch Name*> (config-mst)#

	MSTP configuration mode.	
DHCP Pool Configuration Mode	The DHCP Pool Configuration command ***ip dhcp pool*** is used to enter the DHCP Pool configuration mode.	<*Switch Name*> (dhcp-config)#

Table 1: CLI command modes overview

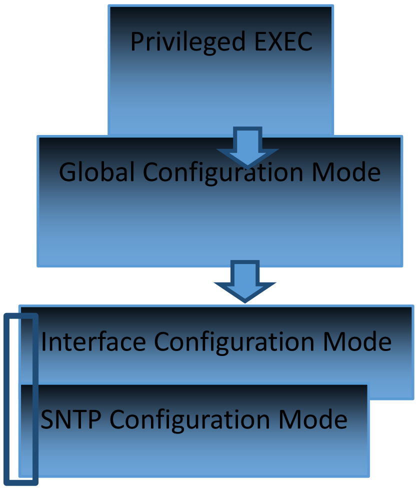


Figure 1: Command Modes Path

System

help

Command Objective	This command displays a brief description for the given command.
Syntax	help [command]
Mode	All Modes

clear screen

Command Objective	This command clears all the contents from the screen.
Syntax	clear screen
Mode	All Modes

end

Command Objective	Exit from Configure mode.
Syntax	end
Mode	All Modes

logout

Command Objective	This command exits from Privileged EXEC/ User EXEC mode to ISS Login Prompt in case of console session. In case of a telnet session, this command terminates the session.
Syntax	logout
Mode	Privileged EXEC Mode

show privilege

Command Objective	Show current privilege level.

Syntax	show privilege
Mode	Privileged EXEC Mode

show cli

Command Objective	This command displays TTY line information such as EXEC timeout.
Syntax	show cli
Mode	Privileged EXEC Mode

exit

Command Objective	This command exits the current mode and reverts to the mode used prior to the current mode.
Syntax	exit
Mode	All Modes

configure terminal

Command Objective	This command enters to Global Configuration Mode which allows the user to execute all the commands that supports global configuration mode.
Syntax	configure terminal
Mode	Privileged EXEC Mode

listuser

Command Objective	This command lists all the default and newly created users, along with their permissible mode.
Syntax	listuser
Mode	Privileged EXEC Mode

show users

Command Objective	This command displays the information about the current user.
Syntax	show users
Mode	Privileged EXEC Mode

lock

Command Objective	This command locks the CLI console. It allows the user/system administrator to lock the console to prevent unauthorized users from gaining access to the CLI command shell. Enter the login password to release the console lock and access the CLI command shell.
Syntax	lock
Mode	Privileged EXEC Mode

show history

Command Objective	This command displays a list of recently executed commands.
Syntax	show history
Mode	Privileged EXEC Mode

username

Command Objective	This command creates a user and sets the enable password for that user with the privilege level. The no form of the command deletes a user and disables the enable password for that user.
Syntax	username <user-name> [password <passwd>] [privilege <1-15>] no username < user-name >
Parameter Description	● <user-name> - Specifies the login username to be created. ● <passwd> - Specifies the password to be entered by the user to login to the system. The size password entered must be a minimum of 8 and maximum of 20 characters containing at least one uppercase, one lowercase, one number and one special character. ● privilege <1-15> - Applies restriction to the user for accessing

	the CLI commands. This value ranges between 1 and 15. For Example, a user ID configured with privilege level as four can access only the commands having privilege ID lesser than or equal to four. >
Mode	Global Configuration Mode

line cli

Command Objective	This command identifies a specific line for configuration and enters the line configuration mode and allows the user to execute all the commands that supports line configuration mode.
Syntax	line cli
Mode	Global Configuration Mode

logging synchronous

Command Objective	This command enables synchronous logging of messages. This command is a complete standardized implementation of the existing command. It operates similar to that of the command

	logging.
Syntax	logging synchronous {severity [{<short (0-7)> | alerts | critical | debugging | emergencies | errors | informational | notification | warnings|all}] | limit <number-of-buffers(size(1-200))}
Mode	Line Configuration Mode

exec-timeout

Command Objective	This command sets a time (in seconds) for EXEC line disconnection. This value ranges between 1 and 10000 seconds. The no form of this command resets the EXEC timeout to its default value.
Syntax	exec-timeout <integer (1-18000)> no exec-timeout
Mode	Line Configuration Mode

set cli pagination

Command Objective	This command sets that whether to use "--MORE--" paging for too long content.
Syntax	set cli pagination {on | off}
Mode	Global Configuration Mode

clear counters

Command Objective	This command clears all the current interface counters from the interface unless the optional arguments type and number are specified to clear only a specific interface type (serial, Ethernet, Token Ring, and so on).
Syntax	clear counters [<interface-type> <interface-id>]
Parameter Description	● <interface-type>- Configures the specified type of interface. ● <interface-id> - Configures the IP interface configuration for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example:

	0/1 represents that the slot number is 0 and port number is 1. >
Mode	Privileged EXEC Mode

interface range

Command Objective	This command selects the range of physical interfaces to be configured.
Syntax	interface range { <interface-type> <slot/port-port> }
Parameter Description	● <interface-type> - Selects the range of the specified interface. ● <slot/port-port> - Selects the range of the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. > >
Mode	Global Configuration Mode

configure

Command Objective	This command enters the configuration mode. Configuration

from memory or network is not supported, when entered into the configuration mode using this command.

Syntax

```
configure
```

Mode

Privileged EXEC Mode

interface

Command Objective

This command allows to configure interface such as VLAN.

Syntax

```
interface {vlan < vlan-id > | port-channel <integer (1-8)> |
<interface-type> <interface-id>}

no interface vlan < vlan-id >
```

Parameter

Description

- vlan <vlan-id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094.

>

>

- port-channel<port-channel-id (1-8)>- Configures the port to be used by the host to configure the router. This value ranges between 1 and 8. The port channel identifier can be created, or a port channel related configuration can done, only if the LA feature

	is enabled in the switch. ● <interface-type>- Configures the specified type of interface. ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. ■ port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. >
Mode	Global Configuration Mode >

set ip-management-vlan

Command Objective	This command configures the ip management vlan.
Syntax	set ip-management-vlan <integer(1-4094)>
Description	● <integer(1-4094)> – Vlan id.
Mode	Global Configuration Mode

shutdown

Command Objective	Set the AdminStatus of Interface down/up.

Syntax	shutdown no shutdown
Description	Set the AdminStatus of Interface down/up.
Mode	Interface Configuration Mode

description

Command Objective	Descriptions about the interface.
Syntax	description <description of this interface> no description
Description	Descriptions about the interface. Or Cancel the descriptions about the interface.

Mode	Interface Configuration Mode

show interface port-security

Command Objective	This command shows the maximum number of learning address and lock mode.
Syntax	show interface port-security [<iftype> <ifnum>]
Parameter Description	● <interface-type> - Displays the IP interface configuration for the specified type of interface. The interface can be: ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. >
Mode	Privileged EXEC Mode

show interface cable-diag

Command Objective	Used to diagnose the copper cable. If there is an error on the cable, it can determine the type of error and the position where the error occurred.

Syntax	show interface cable-diag Gigabitethernet <ifnum>
Parameter Description	● OK- This pair has been connected to partner network device and the link is up. > OPEN–This pair is left open. > SHORT–This pair has been shorted between two lines of its own. > Unknown–The last diagnosis does not obtain the cable' status, please try it again. >
Mode	Privileged EXEC Mode

show interfaces

Command Objective	This command displays the interface status and configuration.
Syntax	show interfaces [{ [<interface-type> <interface-id>] [{ description | storm-control | flowcontrol | capabilities | status | port-security-state | rate-limit }]| {vlan <vlan-id> }
Parameter	● <interface-type> - Displays the interface status and configuration for the specified type of interface. The interface can

Description	be: ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. ■ port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. ● <interface-id> - Displays the interface status and configuration for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1. ● Description **-** Displays the interface description. ● storm-control - Displays the broadcast, multicast, and unicast storm suppression levels for the specified interface ● flowcontrol - Displays the flow control related statistics information for the specified interface. ● capabilities - Displays the interface type, interface speed, duplex operation and flowcontrol status for the specified interface. ● status - Displays the status, duplex details, speed, and negotiation mode of the specified interface. ● port-security-state - Displays the state of the port security option. ● vlan <vlan-id>- VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094. **>**
Mode	Privileged EXEC Mode

show interfaces - counters

Command Objective	This command displays the interface statistics for each port.
Syntax	show interfaces {counters | { <interface-type> <interface-id> counters }}
Parameter Description	● counters- Displays the interface statistics for all the available interfaces. ● <interface-type> - Displays the IP interface configuration for the specified type of interface. The interface can be: ◆ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. ◆ port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. ● <interface-id>- Displays the IP interface configuration for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1.
Mode	Privileged EXEC Mode

clear interfaces - counters

Command Objective	This command clears all the current interface counters from the interface unless the optional arguments type and number are specified to clear only a specific interface type (serial, Ethernet, Token Ring, and so on).
Syntax	clear interfaces [<interface-type> <interface-id>] counters
Parameter Description	● <interface-type>- Configures the specified type of interface. ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. ■ port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. <interface-id>- Displays the IP interface configuration for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1.
Mode	Privileged EXEC Mode

show interface sfp-info

Command Objective	This command displays the SFP module information.
Syntax	show interface sfp-info <interface-type> <interface-id>
Parameter Description	● <interface-type> - Displays the IP interface configuration for the specified type of interface. The interface can be: ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. ■ port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. ● <interface-id> - Displays the IP interface configuration for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1. >
Mode	Privileged EXEC Mode

show interface mtu

Command Objective	This command displays the Maximum Transmission Unit (MTU).

Syntax	show interface mtu [{ Vlan <vlan-id> | port-channel <port-channel-id (1-8)> | <interface-type> <interface-id> }]
Parameter Description	● <interface-type> - Displays the IP interface configuration for the specified type of interface. The interface can be: ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. ■ port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. ● <interface-id> - Displays the IP interface configuration for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1. >
Mode	Privileged EXEC Mode

show ip interface

Command Objective	This command displays IP interface status and configuration.
Syntax	show ip interface [vrf <string(32)>] [{[vlan <short(1-4094)> [switch <string(32)>]] | [<iftype> <ifnum>] | [loopback <short(0-100)>]}]

Parameter Description	● Vrf - Name of the VRF instance. ● Vlan<vlan-id(1-4094)> - Displays the IP interface configuration for the specified VLAN ID. This is a unique value that represents the specific VLAN created. This value ranges between 1 and 4094. ● <interface-type> - Displays the IP interface configuration for the specified type of interface. The interface can be: ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. ● <interface-id> - Displays the IP interface configuration for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1. ● loopback - Loopback ID(0-100) >
Mode	Privileged EXEC Mode

show flow-control

Command Objective	This command displays the flow-control information.
Syntax	show flow-control [interface <interface-type> <interface-id>]

Parameter Description	● <interface-type> - Displays the flow-control information for the specified type of interface. The interface can be: ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. ■ port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. ● <interface-id> - Displays the flow-control information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1. >
Mode	Privileged EXEC Mode

snmp trap link-status

Command Objective	This command enables/disable trap generation on the interface. The interface generated linkUp or linkDown trap. The linkUp trap denotes that the communication link is available and ready for traffic flow. The linkDown trap denotes that the communication link failed and is not ready for traffic flow.
Syntax	snmp trap link-status

	no snmp trap link-status
Mode	Interface Configuration Mode

flowcontrol

Command Objective	This command is used to set the send or receive flow-control value for an interface.
Syntax	flowcontrol { on | off }
Parameter Description	● on - If used with receive allows an interface to operate with the attached device to send flow control packets. If used with send the interface sends flowcontrol packets to a remote device if the device supports it ● off - Turns-off the attached devices (when used with receive) or the local ports (when used with send) ability to send flow-control packets to an interface or to a remote device, respectively. >
Mode	Interface Configuration Mode.

port-security

Command Objective	This command configures the number of learning address on certain interface port.
Syntax	port-security <limit-size(1-256)> no port-security
Parameter Description	● < limit-size(1-256)>-Range is 1 to 256.
Mode	Interface Configuration Mode. This command is applicable in PORT Interface Mode.

mtu

Command Objective	Configures the Maximum Transmission Unit (MTU) for the interface.
Syntax	mtu <frame-size(1522-10240)>

Parameter Description	● <frame-size(1522-10240)>-Range is 1522 to 10240.
Mode	Interface Configuration Mode. This command is applicable in PORT Interface Mode.

system mtu

Command Objective	Configures the Maximum Transmission Unit (MTU) for all interfaces.
Syntax	system mtu <frame-size(1522-10240)> no system mtu <frame-size(1522-10240)>
Parameter Description	● <frame-size(1522-10240)>-Range is 1522 to 10240.
Mode	Global Configuration Mode.

system name

Command Objective	This command sets the system name.
Syntax	system name <systemname>
Mode	Global Configuration Mode

no user-defined system name

Command Objective	This command sets the system name information to the default value.
Syntax	no user-defined system name
Mode	Global Configuration Mode

system contact

Command Objective	This command sets the contact information.

Syntax	system contact <contact info>
Mode	Global Configuration Mode

system location

Command Objective	This command sets the location name.
Syntax	system location <location name>
Mode	Global Configuration Mode

switchport

Command Objective	To put an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration.
Syntax	switchport no switchport

Parameter Description	● <frame-size(1522-10240)>-Range is 1522 to 10240. ● no switchport - To set the interface to the routed-interface status and to erase all Layer 2 configurations.
Mode	Interface Configuration Mode. This command is applicable in PORT Interface Mode.

sntp

Command Objective	This command enters to SNTP configuration mode which allows the user to execute all the commands that supports SNTP configuration mode.
Syntax	sntp
Mode	Global Configuration Mode

set sntp client

Command Objective	This command either enables or disables SNTP client module.
Syntax	set sntp client {enabled | disabled}
Parameter Description	> enabled - Enables SNTP client module and sends a request to the host for time synchronization. > > disabled - Disables SNTP client module and no request is sent to the host for time synchronization. >
Mode	SNTP Configuration Mode

set sntp client port

Command Objective	This command sets the listening port for SNTP client which refers to a port on a server that is waiting for a client connection. The value ranges between 1 and 65535. The no form of this command deletes the listening port for SNTP client and sets the default value.
Syntax	set sntp client port <integer(1-65535)>

	no sntp client port
Mode	SNTP Configuration Mode

set sntp client time-zone

Command Objective	This command sets the system time zone with respect to UTC. The no form of command resets the system time zone to GMT.
Syntax	set sntp client time-zone <UTC-offset value as (+HH:MM /-HH:MM)(+00:00 to +14:00)/ (-00:00 to -12:00)> Eg: +05:30 no sntp client time-zone
Parameter Description	● +/- - Sets the client time zone as after or before UTC. Plus indicates forward time zone and minus indicates backward time zone. ● UTC-offset value as - Sets the UTC offset value in hours - +00:00 to +14:00 - -00:00 to -12:00

>

Mode	SNTP Configuration Mode

set sntp client clock-summer-time

Command Objective	This command enables the DST (Daylight Saving Time). DST is a system of setting clocks ahead so that both sunrise and sunset occur at a later hour. The effect is additional daylight in the evening. Many countries observe DST, although most have their own rules and regulations for when it begins and ends. The dates of DST may change from year to year. The no form of this command disables the Daylight Saving Time.
Syntax	set sntp client clock-summer-time <week-day-month,hh:mm> <week-day-month,hh:mm> Eg: set sntp client clock-summer-time First-Sun-Mar,05:10 Second-Sun-Nov,06:10 no sntp client clock summer-time
Parameter Description	● week-day-month - The list is given below: ■ week - First, Second, Third, Fourth or Last week of month. ■ day - Sunday, Monday, Tuesday, Wednesday, Thursday, Friday,

	or Saturday. ■ month - /January, February, March, April, May, June, July, August, September, October, November, or December. ■ hh:mm - Time in hours and minutes
Mode	SNTP Configuration Mode

set sntp unicast-server

Command Objective	This command configures SNTP unicast-server. The no form of this command deletes the sntp unicast server attributes and sets to default value
Syntax	set sntp unicast-server {ipv4 <ucast_addr> |ipv6 <ip6_addr> | domain-name <string(64)>} [port <integer(1-65535)>] no sntp unicast-server {ipv4 <ucast_addr> | ipv6 <ip6_addr> | domain-name <string(64)>}
Parameter Description	● ipv4 <ucast_addr> - Sets the address type of the unicast-server as Internet Protocol Version 4.

- ipv6 <ip6_addr> - Sets the address type of the unicast server as Internet Protocol Version 6.
- domain-name <string(64)> - Sets the domain name for the unicast server. This value is a string with the maximum size as 64.
- port <integer(1-65535)> - Selects the port identifier numbers in the selected server. This value ranges between 1 and 65535.

Mode	SNTP Configuration Mode

show sntp clock

Command Objective	This command displays the current time.
Syntax	show sntp clock
Mode	User / Privileged EXEC Mode

show sntp status

Command	This command displays SNTP status.

Objective	
Syntax	show sntp status
Mode	User / Privileged EXEC Mode

clock set

Command Objective	This command manages the system clock.
Syntax	clock set hh:mm:ss <day (1-31)> {january|february|march|april|may|june|july|august|september|october|november|december} <year (2000 - 2035)>
Parameter Description	● hh:mm:ss - Sets the current time. The format is hour, minutes, and seconds. ■ <day (1-31)> - Sets the current day. It ranges between 1 and 31. ■ january - Sets the month as January. ■ february - Sets the month as February ■ march - Sets the month as March ■ april - Sets the month as April

- may - Sets the month as May
- june - Sets the month as June
- july - Sets the month as July
- august - Sets the month as August
- september - Sets the month as September
- october - Sets the month as October
- november - Sets the month as November
- december - Sets the month as December
- <year (2000 - 2035)> - Sets the year. It ranges between 2000 and 2035

Mode	Privileged EXEC Mode

show clock

Command Objective	This command displays the system date and time.
Syntax	show clock
Mode	Privileged EXEC Mode

show system information

Command Objective	This command displays system information.
Syntax	show system information
Mode	Privileged EXEC Mode

show system utilization

Command Objective	This command displays the system utilization.
Syntax	show system utilization
Mode	Privileged EXEC Mode

reboot

Command Objective

This command restarts the switch.

Syntax

```
reboot
```

Mode

Privileged EXEC Mode

reboot-flick

Command Objective

This command restarts the switch but not reset PoE.

Syntax

```
reboot-flick
```

Mode

Privileged EXEC Mode

restore-defaults

Command Objective	This command restores default configuration.
Syntax	restore-defaults
Mode	Privileged EXEC Mode

restore-defaults-without-IP

Command Objective	This command restores default configuration without IP.
Syntax	restore-defaults-without-IP
Mode	Privileged EXEC Mode

show telnet server

Command Objective

This command displays the telnet server status.

Syntax

```
show telnet server
```

Mode

Privileged EXEC Mode

show http server status

Command Objective

This command displays the http server status and HTTP port.

Syntax

```
show http server status
```

Mode

Privileged EXEC Mode

port speed - duplex

Command Objective

This command configures the speed and duplex operation.

Syntax

```
speed { 10 | 100 | 1000 | 10000 } duplex { full | half }

no speed

no duplex
```

Parameter Description

- 10 - Port runs at 10Mbps
- 100 - Port runs at 100Mbps
- 1000 - Port runs at 1000Mbps
- 10000 - Port runs at 10000Mbps
- full - Port is in full-duplex mode, that is data simultaneously communicates in both directions.
- half - Port is in half-duplex mode, that is data can communicate in both directions, but only in one direction at a time.

>

Mode

Interface Configuration

extended speed

Command Objective	This command enables extended speed on the port.
Syntax	extended speed
Mode	Interface Configuration

negotiation

Command Objective	This command enables auto-negotiation on the interface. The no form of the command disables auto-negotiation on the interface. The port in which auto-negotiation is enabled, negotiates with the other end for port properties like speed, duplexity and so one. The normal port uses the port property values configured by the administrator.
Syntax	negotiation

	no negotiation
Mode	Interface Configuration

set switch-name

Command Objective	This command sets the name of the switch.
Syntax	set switch-name <switchname>
Mode	Global Configuration Mode

set system description

Command Objective	This command configures the system description.
Syntax	set system description <switchname>

Mode	Global Configuration Mode

set ip http

Command Objective	This command enables/disables HTTP in the switch.
Syntax	set ip http {enable | disable}
Parameter Description	● enable - Enables HTTP in the switch. ● disable - Disables HTTP in the switch.
Mode	Global Configuration Mode

ip telnet service

Command Objective	This command enables the telnet service in the system.

	The no form of this command disables the telnet service.
Syntax	ip telnet service no ip telnet service
Mode	Global Configuration Mode

firmware upgrade

Command Objective	This command performs firmware upgrade using TFTP from a remote location.
Syntax	firmware upgrade { tftp://ip-address/filename} {flash:normal | flash:fallback} image <1-2>
Mode	Privileged EXEC Mode

save

Command Objective	This command copies variables from the running configuration to the startup configuration file in NVRAM, where the running-config is the current configuration in the router and the startup config is the configuration that is loaded when the switch boots up.
Syntax	save
Mode	Privileged EXEC Mode

copy startup-config

Command Objective	This command copies a file from a source remote site /flash to a destination remote site/flash. The entire copying process takes several minutes and differs from protocol to protocol and from network to network.
Syntax	copy startup-config {flash: filename | tftp://ip-address/filename}
Parameter	● tftp://ip-address/filename - Configures the TFTP details for

Description

taking back up of initial configuration in TFTP server.

- ip-address - The IP address or host name of the server.
- filename - The name of the file in which the initial configuration should be stored. Filenames and directory names are case sensitive

Mode

Privileged EXEC Mode

copy - startup-config

Command Objective

This command copies the configuration or system logs from a remote site to flash.

Syntax

copy { tftp://ip-address/filename startup-config | flash: filename startup-config }

Parameter Description

● tftp://ip-address/filename startup-config - Configures the address from which the file is to be copied and the file name from which configuration is to be copied. This option configures the TFTP server details Filenames and directory names are case sensitive

>

Mode	Privileged EXEC Mode

copy

Command Objective	This command copies a file.
Syntax	copy { tftp://ip-address/filename | flash: filename} { tftp://ip-address/filename | flash: filename | filename}
Parameter Description	● tftp://ip-address/filename | flash: filename - Configures the address from which the file is to be copied and the file name from which configuration is to be copied. This option configures the TFTP server details Filenames and directory names are case sensitive. >
Mode	Privileged EXEC Mode

copy logs

Command Objective	This command writes the system logs to a remote site.
Syntax	copy logs { tftp://ip-address/filename }
Parameter Description	● tftp://ip-address/filename - Configures the address from which the file is to be copied and the file name from which configuration is to be copied. This option configures the TFTP server details Filenames and directory names are case sensitive. >
Mode	Privileged EXEC Mode

show activepartition

Command Objective	This command displays the active image partition.
Syntax	show activepartition
Mode	Privileged EXEC Mode

boot system

Command Objective	This command Set system boot image partition.
Syntax	boot system { image1 | image2 }
Mode	Privileged EXEC Mode

show current running-config

Command Objective	This command displays the currently operating configuration in the system.
Syntax	show current running-config
Mode	Privileged EXEC Mode

show mab debug_log [remove]

Command Objective

This command displays mab debug_log.

Syntax

show mab debug_log [remove]

Parameter Description

- remove - Delete log files.

Mode

Privileged EXEC Mode

show UBIRecoveryCount

Command Objective

This command displays the UBI recovery count.

Syntax

show UBIRecoveryCount

Mode

Privileged EXEC Mode

reset UBIRecoveryCount

Command Objective

This command resets the UBI recovery count.

Syntax

reset UBIRecoveryCount

Mode

Privileged EXEC Mode

ip http port

Command Objective

This command set the HTTP port.

Syntax	ip http port <port-number(1-65535)>
Parameter Description	● <port-number(1-65535)> - HTTP port.
Mode	Global Configuration Mode

ip http session-idle-timeout

Command Objective	This command set the HTTP session timeout (in minutes) for line disconnection.
Syntax	ip http session-idle-timeout <minutes(0-10000)>
Parameter Description	● <minutes(0-10000)> - EXEC timeout value(in minutes).
Mode	Global Configuration Mode

cli exec-timeout

Command Objective	This command sets the default EXEC timeout (in minutes) for line disconnection.
Syntax	cli exec-timeout <minutes (0-10000)>
Parameter Description	● <minutes(0-10000)> - EXEC timeout value(in minutes).
Mode	Global Configuration Mode

no shutdown switch-instance-shared-port

Command Objective	This command starts Switch Instance Shared Port Feature(SISP) in the switch. Once SISP is started, interfaces can be mapped to more than one switch instance through appropriate SISP configurations.
Syntax	no shutdown switch-instance-shared-port

Mode

Global Configuration Mode

ping

Command Objective

This command sends echo messages. The Packet Internet Groper (Ping) module is built based on the ICMP echo request and ICMP echo response messages. The network administrator uses this ping on a remote device to verify its presence. Ping involves sending ICMP echo messages repeated and measuring the time between transmission and reception of message. The output displays the time taken for each packet to be transmitted, number of packets transmitted, number of packets received and packet loss percentage.

Syntax

ping [ip] {IpAddress | hostname } [{repeat|count} packet_count (1-10)] [size packet_size (8-5120)] [timeout time_out (1-100)]

Parameter Description

- ip - Configures the IP address of the node to be pinged.
- ipAddress - Configures the source IP address of the node to be pinged.
- hostname - Configures the name of the host.
- repeat - Configures number of ping messages.

	● count - Configures the number of times the given node address is to be pinged. ● size packet_size (8-5120) - Configures the size of the data portion of the PING PDU. This value ranges between 8 and 5120. ● timeout time_out (1-100) - Configures the time in seconds after which the entity waiting for the ping response times out. The value ranges between 1 and 100. >
Mode	Privileged EXEC Mode

traceroute

Command Objective	This command traces route to the destination.
Syntax	traceroute {<ip-address>| hostname | ipv6 <prefix>} [max-ttl <value (2-255)>]
Parameter Description	● <ip-address> - Configures the destination IP address to which a route has to be traced. ● <hostname> - Configures the destination IP hostname to which a route has to be traced. ● ipv6 <prefix> - Configures the destination IPv6 address to which a route has to be traced. ● [max-ttl <short (2-255)>] - Configures the maximum value of

	the TTL field to be filled up in the IP packets used for the trace route. >
Mode	Privileged EXEC Mode

show device temperature

Command Objective	This command displays current device temperature.
Syntax	show device temperature
Mode	Privileged EXEC Mode

free

Command Objective	This command gets a detailed report on the system's memory usage. The free command provides information about the total amount of the physical and swap memory, as well as the free and used memory.

Syntax	free
Mode	Privileged EXEC Mode

mpstat

Command Objective	This command is used to report processor related statistics. It accurately displays the statistics of the CPU usage of the system. It displays information about CPU utilization and performance.
Syntax	mpstat
Mode	Privileged EXEC Mode

clock time source

Command Objective	This command configures the time source of primary clock. The no form of this command resets time source of the primary clock to default time source.

Syntax	clock time source { ntp | internal-oscillator } no clock time source [{ ntp | internal-oscillator }]
Parameter Description	● ntp - Primary time source of the system is ntp. ● internal-oscillator - Primary time source of the system is internal-oscillator. >
Mode	Global Configuration Mode

clock utc-offset

Command Objective	This command sets the system time zone with respect to UTC. The no form of command resets the system time zone to GMT.
Syntax	clock utc-offset <offset> Eg: +05:30 no clock utc-offset
Parameter	● +/- - Sets the client time zone as after or before UTC. Plus indicates forward time zone and minus indicates backward time

Description	zone. ● <offset> - Sets the UTC offset value in hours. Current utc-offset value as (+HH:MM /-HH:MM)(+00:00 to +14:00)/ (-00:00 to -12:00). Eg: +05:30 >
Mode	Global Configuration Mode

clock set time

Command Objective	This command configures the time of primary clock.
Syntax	clock set time <time-nanoseconds>
Mode	Global Configuration Mode

show clock properties

Command Objective	This command displays primary system PTP clock properties.

Syntax	show clock properties
Mode	Privileged EXEC Mode

EEE

eee

Command Objective	This command enables Energy Efficient Ethernet on the specified port. The no form of the command disables Energy Efficient Ethernet on the specified port.
Syntax	eee no eee
Mode	Interface Configuration Mode

show eee

Command Objective	This command displays the Energy Efficient Ethernet information of each port.
Syntax	show eee
Mode	Privileged EXEC Mode

SSL

show ip http secure server status

Command Objective	This command displays SSL status and configuration information. Information such as HTTP secure server status, http secure server ciphersuite are displayed.
Syntax	show ip http secure server status
Mode	Privileged EXEC Mode

show ip http session-idle-timeout

Command Objective	This command displays web session timeout value.
Syntax	show ip http session-idle-timeout
Mode	Privileged EXEC Mode

ip http secure server

Command Objective	This command enables the server status to establish the secure layer in the network The no form of the command disables the server status.
Syntax	ip http secure server no ip http secure server
Mode	Global Configuration Mode

SSH

show ssh-configurations

Command Objective	This command displays the SSH server listening IP address and port information.
Syntax	show ssh-configurations
Mode	Privileged EXEC Mode

ip ssh server

Command Objective	This command enables the ssh system The no form of the command disables the ssh system.
Syntax	ip ssh server no ip ssh server
Mode	Global Configuration Mode

POE

set poe global power threshold

Command Objective	This command modifies Power Over Ethernet module global power budget in the switch.
Syntax	set poe global power threshold <value>
Mode	Global Configuration Mode

power inline

Command Objective	This command enables/disables Power Over Ethernet on the specified port to provide power over a copper Ethernet cable to an endpoint or powered device.
Syntax	power inline { enable | disable }
Mode	Interface Configuration Mode

power inline limit

Command Objective	This command limits Power Over Ethernet on the specified port to provide power over a copper Ethernet cable to an endpoint or powered device.
Syntax	power inline limit { auto | <value> }
Parameter Description	● auto - automatically and allocates power to the PoE port after device detection if enough power is available. ● <value> - The maximum wattage feature limits the power allocated on the port. >
Mode	Interface Configuration Mode

power inline priority

Command Objective	This command sets the priority of the Power Over Ethernet on the specified port.
Syntax	power inline priority { critical | high | medium | low }

Parameter Description	● critical - Sets the Power Over Ethernet port priority to critical ● high - Sets the Power Over Ethernet port priority to high ● medium - Sets the Power Over Ethernet port priority to medium ● low - Sets the Power Over Ethernet port priority to low >
Mode	Interface Configuration Mode

show power detail

Command Objective	This command displays the Power Over Ethernet power supply status information such as PoE Global admin state, PSE operational status and Maximum power supply.
Syntax	show power detail
Mode	Privileged EXEC Mode

show power inline

Command Objective	This command displays the Power Over Ethernet power

	supply status information of each pse.
Syntax	show power inline [{<interface-type> <interface-id>}]
Parameter Description	● <interface-type> - Displays the information about the specified type of interface. The interface can be: ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. ● <interface-id> - Displays the information about the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1. >
Mode	Privileged EXEC Mode

PD Lifeguard

set pdlg

Command Objective	This command enables/disables PD Lifeguard module in the switch.
Syntax	set pdlg {enable | disable}
Mode	Global Configuration Mode

set pdlg port

Command Objective	This command enables/disables PD Lifeguard module on the specified port.
Syntax	set pdlg port <integer(1-48)> {enable | disable}
Mode	Global Configuration Mode

set pdlg port - mode

Command Objective	This command selects PD Lifeguard mode on the specified port.
Syntax	set pdlg port <integer(1-48)> mode { auto | force-ping }
Parameter Description	● auto - PD reachability is judged by LLDP packet (priority) or ping IP test. ● force-ping - PD reachability is judged via ping IP test. >
Mode	Global Configuration Mode

set pdlg port - ping ip

Command Objective	This command sets PD Lifeguard ping IP Address on the specified port.
Syntax	set pdlg port <integer(1-48)> ping ip <ucast_addr>
Mode	Global Configuration Mode

set pdlg port - ping interval

Command Objective	This command sets PD Lifeguard ping IP Interval on the specified port.
Syntax	set pdlg port <integer(1-48)> ping interval <integer(1-3600)>
Mode	Global Configuration Mode

set pdlg port - ping max-try

Command Objective	This command sets PD Lifeguard ping IP max count on the specified port.
Syntax	set pdlg port <integer(1-48)> ping max-try <integer(1-255)>
Mode	Global Configuration Mode

set pdlg port - reboot interval

Command Objective	This command sets PD Lifeguard reboot interval between disabling and enabling the specified port.

Syntax	set pdlg port <integer(1-48)> reboot interval <integer(1-600)>
Mode	Global Configuration Mode

set pdlg port - reboot max-try

Command Objective	This command sets PD Lifeguard reboot PD max retry count on the specified port.
Syntax	set pdlg port <integer(1-48)> reboot max-try <integer(0-20)>
Mode	Global Configuration Mode

set pdlg port - reboot refresh

Command Objective	This command resets PD Lifeguard reboot retry count on the specified port.
Syntax	set pdlg port <integer(1-48)> reboot refresh

Mode	Global Configuration Mode

set pdlg port - reboot

Command Objective	This command sets PD Lifeguard reboot allowed or denied on the specified port.
Syntax	set pdlg port <integer(1-48)> reboot {allow | deny}
Parameter Description	● allow – allow reboot (reboot + system log). ● deny – deny reboot (system log only).
Mode	Global Configuration Mode

set pdlg reboot port

Command Objective	This command restarts the specified PoE port.
Syntax	set pdlg reboot port <integer(1-48)>

Mode	Global Configuration Mode

set pdlg port - pd-boot-time

Command Objective	This command sets PD Lifeguard PD boot up time.
Syntax	set pdlg port <integer(1-48)> pd-boot-time <integer(50-1200)>
Parameter Description	● pd-boot-time <integer(50-1200)> – The duration waiting for LLDP signal when first switches to auto mode. The reboot max retry value can be set from 50 to 1200. (0 means unlimited)
Mode	Global Configuration Mode

show pdlg port

Command Objective	This command shows PD Lifeguard per port status.
Syntax	show pdlg port <integer(1-48)>
Mode	Privileged EXEC Mode

show pdlg detail

Command Objective	This command shows PD Lifeguard status in detail.
Syntax	show pdlg detail
Mode	Privileged EXEC Mode

Link Aggregation

no shutdown port-channel

Command Objective	This command starts and enables LA feature in the switch and allocates required memory to the LA module. The LA feature is made available in the switch only if the LA is enabled in the switch. LA feature allows to aggregate individual point-to-point links into a port channel group, so that the capacity and availability of the communications channel between devices are increased using the existing interface technology.
Syntax	no shutdown port-channel
Mode	Global Configuration Mode.

lacp system-priority

Command Objective	This command configures the LACP priority associated with actor's system ID. The switch with the lowest LACP decides the standby and active links in the LA.

Syntax	lacp system-priority <short(0-65535)> no lacp system-priority
Mode	Global Configuration Mode.

port-channel load-balance

Command Objective	This command configures the load balancing policy for all port channels created in the switch
Syntax	port-channel load-balance {src-mac | dest-mac | arc-dest-mac | src-ip | dest-ip | src-dest-ip | dest-l4-port | src-l4-port}
Parameter Description	● src-mac - Distributes the load based on the source MAC address. The bits of the source MAC address in the packet are used to select the port in which the traffic should flow. Packets from different hosts use different ports in the channel, but packets from the same host use the same port. ● dest-mac - Distributes the load based on the destination host MAC address. The bits of the destination MAC address in the packet are used to select the port in which the traffic should flow. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the

	channel ● src-dest-mac - Distributes the load based on the source and destination MAC address. The bits of the source and destination MAC address in the packet are used to select the port in which the traffic should flow. ● src-ip - Distributes the load based on the source IP address. The bits of the source IP address in the packet are used to select the port in which the traffic should flow. ● dest-ip - Distributes the load based on the destination IP address. The bits of the destination IP address in the packet are used to select the port in which the traffic should flow. ● src-dest-ip - Distributes the load based on the source and destination IP address. The bits of the source and destination IP address in the packet are used to select the port in which the traffic should flow. ● dest-l4-port - Distributes the load based on the destination Layer 4 port. The bits of the destination Layer 4 port in the packet are used to select the port in which the traffic should flow. ● src-l4-port - Distributes the load based on the source Layer 4 port. The bits of the source Layer 4 port in the packet are used to select the port in which the traffic should flow.
Mode	Global Configuration Mode.

channel-group

Command Objective

This command adds the port as a member of the specified port channel that is already created in the switch.

The no form of the command deletes the aggregation of the port from all port channels.

Syntax

```
channel-group <channel-group-number(1-8)> Mode { on | active | passive }

no channel-group
```

Parameter Description

- <channel-group-number(1-8)> - Adds the port as a member of the specified port channel. This is a unique value that represents the specific port-channel created. This value ranges from 1 to 8.
- Mode - Configures the LACP activity for the port:

- active - Starts LACP negotiation un-conditionally.

- passive - Starts LACP negotiation only when LACP packet is received from peer.

- on - Forces the interface to channel without LACP. This is equivalent to manual aggregation.

Mode

Interface Configuration Mode (Physical Interface Mode)

This command is applicable in PORT Interface Mode.

lacp timeout

Command Objective	This command configures the LACP timeout period within which LACPDUs should be received on a port to avoid timing out of the aggregated link. The no form of the command sets the LACP timeout period to its default value.
Syntax	lacp timeout {long | short } no lacp timeout
Parameter Description	● long - Configures the LACP timeout period as 90 seconds. The LACP PDU is sent every 30 seconds. ● short - Configures the LACP timeout period as 3 seconds. The LACP PDU is sent every second.
Mode	Interface Configuration Mode (Physical Interface Mode) This command is applicable in VLAN Interface Mode.

show etherchannel

Command Objective

This command displays Etherchannel information for all port-channel groups created in the switch. This information contains admin and oper status of port-channel module, and status of protocol operate Mode for each group.

Syntax

show etherchannel [[channel-group-number] { detail | load-balance | port | port-channel | summary | protocol}]

Parameter Description

- channel-group-number - Displays Etherchannel information for the specified port-channel group. This is a unique value that represents the specific port-channel created. This value ranges from 1 to 8.

- detail - Displays detailed Etherchannel information. The information contains admin and oper status of port channel module, LACP system priority, status of protocol operate Mode for each group, port details for each group and port channel details. The port details contain port state, group to which the port belongs, port Mode, aggregation state, port-channel ID, pseudo port-channel ID, admin key, oper key, port number, port state, and LACP port-priority, wait-time, port identifier, activity, and timeout. The port channel details contain port channel ID, number of member ports, ID of hot standby port, port state, status of protocol operate Mode, aggregator MAC and default port ID.

- load-balance - Displays the load balancing policy applied for each port-channel group.

- port - Displays the status of protocol operate Mode and port

	details for each group. The port details contain port state, group to which the port belongs, port Mode, aggregation state, port-channel ID, pseudo port-channel ID, admin key, oper key, port number, port state, and LACP port-priority, wait-time, port identifier, activity, and timeout. ● port-channel - Displays the admin and oper status of port channel module, and port channel details. The port channel details contain port channel ID, number of member ports, ID of hot standby port, port state, status of protocol operate Mode, aggregator MAC and default port ID. ● summary - Displays the admin and oper status of port channel module, number of channel groups used, number of aggregators, group IDs, and port channel ID, status of protocol operate Mode and member ports for each group. ● protocol - Displays the status of protocol operate Mode for each port-channel group.
Mode	Privileged EXEC Mode

Mirror

monitor session - destination

Command Objective

This command configures a destination port for a mirroring session.

The no form of the command removes the destination port configuration of the mirroring session.

Syntax

monitor session <session-id (1-3)> destination { interface <interface-type> <interface-id>} [allow-ingress]

no monitor session <session-id (1-3)> destination { interface<interface-type> <interface-id> }[allow-ingress]

Parameter Description

- session-id - Specifies the index of the mirroring session. This value ranges between 1 and 3.
- interface - Specifies the destination port for the mirroring session.
  - <interface-type> - Interface type. This can be: GigabitEthernet or Port Channel.
  - <interface-id> – Interface identifier. This is a combination of slot number and port number.
- allow-ingress- Allow Packets Ingress to Destination Port.

Mode	Global Configuration Mode

monitor session - source

Command Objective	This command configures a source port / remote VLAN for a mirroring session. The no form of the command removes the source port / remote VLAN configuration of the mirroring session.

Syntax	monitor session <session-id (1-3)> { source { interface <interface-type> <interface-id> [{ rx | tx | both }] }}}
	no monitor session <session-id (1-3)> { source{interface <interface-type> <interface-id> [{rx|tx|both}]}}

Parameter Description	● session-id - Configures the session number that is used to identify a session. ● interface - Configures the source interface whose traffic to be mirrored. The details to be provided are: ■ <interface-type> - Sets the type of interface. The interface can be:

◆ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.

■ <interface-id> - Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash.

- rx - Mirrors received traffic
- tx - Mirrors transmitted traffic
- both - Specifies the traffic direction to monitor. If the traffic direction is not specified, both transmitted and received traffic is mirrored.

Mode	Global Configuration Mode

no monitor session

Command Objective	This command is used to remove the mirroring configuration.
Syntax	no monitor session { session-id (1-3)}
Parameter Description	● session-id - Specifies the index of the mirroring session.

Mode	Global Configuration Mode

show monitor

Command Objective	This command displays the mirroring information present in the system.
Syntax	show monitor { session <session-id (1-3)> | all } [detail]
Parameter Description	● <session-id (1-3)> - Displays the mirroring information for the specified index of the mirroring session. ● all - Displays the mirroring information of all the sessions. ● detail - Displays the detailed information regarding the session.
Mode	Global Configuration Mode

STP

spanning-tree

Command Objective	This command enables the spanning tree operation in the switch for the selected spanning tree Mode. Spanning tree operation provides path redundancy while preventing undesirable loops in the network that are created by multiple active paths between stations. It logically breaks such loops and prevents looping traffic from clogging the network. The no form of this command disables the spanning tree operation in the switch. The spanning tree operation is automatically enabled in the switch once the spanning tree Mode is changed.
✏	The spanning tree operation can be enabled in the switch only if the spanning tree functionality is not shut down in the switch. The type of spanning tree Mode should be set if the functionality is already shutdown.
Syntax	spanning-tree no spanning-tree
Mode	Global Configuration Mode

spanning-tree mode

Command Objective	This command sets the type of spanning tree to be executed, enables spanning tree operation, and starts spanning tree functionality in the switch. The current selected type of spanning tree is enabled, and the existing spanning tree type is disabled in the switch.
Syntax	spanning-tree mode {mst|rst}
Parameter Description	● mst - Configures the switch to execute MSTP for preventing undesirable loops. MSTP configures spanning tree on per VLAN basis or multiple VLANs per spanning tree. The Mode cannot be set as mst if the base bridge Mode is configured as transparent bridging. ● rst - Configures the switch to execute RSTP for preventing undesirable loops. RSTP provides rapid recovery of connectivity following the failure of a bridge/bridge port or a LAN >
Mode	Global Configuration Mode

spanning-tree transmit hold-count

Command Objective	This command sets the transmit hold-count value for the switch. The transmit hold count value is a counter that is used to limit the maximum transmission rate of the switch and to avoid flooding. This value specifies the maximum number of packets that can be sent in a given hello time interval. This value ranges between 1 and 10. The no form of this command sets the transmit hold-count to its default value. The transmit hold-count is changed to its default value even if the spanning tree Mode is changed.
✏	The transmit hold-count value can be configured in the switch, only if the spanning tree functionality is not shut down in the switch. The type of spanning tree Mode should be set if the functionality is already shutdown.
Syntax	spanning-tree transmit hold-count <value (1-10)> no spanning-tree transmit hold-count
Parameter Description	● hold-count - This value specifies the maximum number of packets that can be sent in a given hello time interval. This value ranges between 1 and 10. >
Mode	Global Configuration Mode

spanning-tree forward-time

Command Objective

This command configures the forward timer of the spanning tree and the no form of the command sets the forward timer to the default value. The forward timer controls the speed at which a port changes its spanning tree state from Blocking state to Forwarding state. The timer value ranges between 4 and 30 seconds.

✏

The values configured for the spanning tree forward timers should satisfy the following conditions:

2* (forward-time - 1) >= max-age, and max-age >= 2 * (hello-time +1)

This command is a standardized implementation of the existing command, spanning-tree timers. It operates similar to the existing command.

Syntax

```
spanning-tree forward-time <seconds(4-30)>
```

```
no spanning-tree forward-time
```

Mode

Global Configuration Mode

spanning-tree max-age

Command Objective	This command configures the max-age timer of the spanning tree. The max-age timer denotes the time (in seconds) after which the spanning tree protocol information learnt from the network on any port will be discarded. The timer value ranges between 6 and 40 seconds. The no form of the command sets the max-age timer to the default value.
✏	The values configured for the spanning tree forward timers should satisfy the following conditions: 2* (forward-time - 1) >= max-age, and max-age >= 2 * (hello-time +1) This command is a standardized implementation of the existing command, spanning-tree timers. It operates similar to the existing command.
Syntax	spanning-tree max-age <seconds(6-40)> no spanning-tree max-age
Mode	Global Configuration Mode

spanning-tree hello-time

Command Objective	This command configures the spanning tree hello time. The no form of this command resets the hello time to its default value. The hello time represents the time interval (in seconds) between two successive configuration BPDUs generated by the switch on the port. This value is either 1 or 2 seconds. This value is applied to all active MSTIs.
Syntax	spanning-tree hello-time<value(1-2)> no spanning-tree hello-time
Mode	Global Configuration Mode

spanning-tree mst forward-time

Command Objective	This command configures the forward timer of the spanning tree and the no form of the command sets the forward timer to the default value. The forward timer controls the speed at which a port changes its spanning tree state from Blocking state to Forwarding state. The timer value ranges between 4 and 30 seconds.

✏	The values configured for the spanning tree forward timers should satisfy the following conditions: 2* (forward-time - 1) >= max-age, and max-age >= 2 * (hello-time +1) This command is a standardized implementation of the existing command, spanning-tree timers. It operates similar to the existing command. The STP forward timers can be configured in the switch, only if the spanning tree functionality is not shut down in the switch. The type of spanning tree Mode should be set if the functionality is already shutdown.
Syntax	spanning-tree mst forward-time <seconds(4-30)> no spanning-tree mst forward-time
Mode	Global Configuration Mode

spanning-tree mst max-age

Command Objective	This command configures the max-age timer of the spanning tree. The max-age timer denotes the time (in

	seconds) after which the spanning tree protocol information learnt from the network on any port will be discarded. The timer value ranges between 6 and 40 seconds. The no form of the command sets the max-age timer to the default value.
✏	The values configured for the spanning tree forward timers should satisfy the following conditions: 2* (forward-time - 1) >= max-age, and max-age >= 2 * (hello-time +1) This command is a standardized implementation of the existing command, spanning-tree timers. It operates similar to the existing command. The STP forward timers can be configured in the switch, only if the spanning tree functionality is not shut down in the switch. The type of spanning tree Mode should be set if the functionality is already shutdown.
Syntax	spanning-tree mst max-age <seconds(6-40)> no spanning-tree mst max-age
Mode	Global Configuration Mode

spanning-tree mst hello-time

Command Objective	This command configures the spanning tree hello time. The no form of this command resets the hello time to its default value. The hello time represents the time interval (in seconds) between two successive configuration BPDUs generated by the switch on the port. This value is either 1 or 2 seconds. This value is applied to all active MSTIs.
✏	This command can be executed successfully, only if the spanning tree functionality is not shut down in the switch. The type of spanning tree Mode should be set as mst.
Syntax	spanning-tree mst hello-time<value(1-2)> no spanning-tree mst hello-time
Mode	Global Configuration Mode / PORT Interface Mode

clear spanning-tree counters

Command Objective

This command deletes all bridge and port level spanning tree statistics information.

For RSTP, the information contains number of:

- Transitions to forwarding state
- RSTP BPDU count received / transmitted
- Config BPDU count received / transmitted
- TCN BPDU count received / transmitted
- Invalid BPDU count transmitted
- Port protocol migration count

For MSTP, the information contains number of:

- Port forward transitions
- Port received BPDUs
- Port transmitted BPDUs
- Port invalid BPDUs received
- Port protocol migration count
- BPDUs sent / received for each MSTI

✏

The statistics information can be deleted, only if the spanning tree functionality is not shut down in the switch. The type of spanning tree Mode should be set if the functionality is already shutdown.

Syntax

```
clear spanning-tree [mst <instance-id>] counters[interface <interface-type> <interface-id>]
```

Parameter Description	● mst <instance-id>] - Clears the statistical counters specific to the MSTP instance already created in the switch. This value ranges between 1 and 64. This option is applicable, only if the spanning tree Mode is set as mst. ● interface - Clears all port-level spanning-tree statistics information for the given port. ■ <interface-type> - Clears all port-level spanning-tree statistics information for the specified type of interface. The interface can be: ◆ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. ◆ port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. ■ <interface-id> - Clears all port-level spanning-tree statistics information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface type port-channel. For Example: 1 represents port-channel ID. >
Mode	Global Configuration Mode

spanning-tree priority

Command Objective	This command configures the priority value that is assigned to the switch. The no form of this command resets the priority to its default value. The priority value is changed to its default value even if the spanning tree Mode is changed. In RSTP, this value is used during the election of root. In MSTP, this value is used during the election of CIST root, CIST regional root and IST root.
✏	The priority value can be configured in the switch, only if the spanning tree functionality is not shut down in the switch. The type of spanning tree Mode should be set if the functionality is already shutdown.
Syntax	spanning-tree [mst <instance-id>] priority <value(0-61440)> no spanning-tree [mst <instance-id(1-64)>] priority
Parameter **Description**	● mst <instance-id> - Configures the ID of MSTP instance already created in the switch. This value ranges between 1 and 64. The special value 4094 can be used only in the switch that supports PBB-TE. This special value represents PTETID that identifies VID used by ESPs. This option is applicable, only if the spanning tree Mode is set as mst. ● priority <value(0-61440)> - Configures the priority value for the switch and for the MSTI, in RSTP and MSTP, respectively. This value ranges between 0 and 61440. The value should be set in

	steps of 4096, that is, you can set the value as 0, 4096, 8192, 12288 and so on. >
Mode	Global Configuration Mode

spanning-tree mst max-instance

Command Objective	This command configures the maximum number of active MSTIs that can be created. This value ranges between 1 and 64. The no form of this command resets maximum MSTP instance value to its default value.
✏	This command can be executed successfully, only if the spanning tree functionality is started and enabled in the switch. The type of spanning tree Mode should be set as mst.
Syntax	spanning-tree mst max-instance <short(1-64)> no spanning-tree mst max-instance
Mode	Global Configuration Mode

spanning-tree mst root

Command Objective	This command enables BPDU (Bridge Protocol Data Unit) transmission and reception on the interface. This command is a standardized implementation of the existing command, spanning-tree priority. It operates similar to the existing command. The no form of the command disables BPDU transmission and reception on the interface.
✏	This command executes only if • instance is created • spanning tree Mode is set as mst.
Syntax	spanning-tree mst {instance-id <instance-id(1-64)>} root {primary | secondary} no spanning-tree mst {instance-id <instance-id(1-64)>} root
Parameter Description	● instance-id <instance-id(1-64)> - Configures the ID of MSTP instance already created in the switch. This value ranges between 1 and 64. This option is applicable, only if the spanning tree Mode

	is set as mst. ● primary - Sets high enough priority (low value) for the switch so that the switch can be made as the bridge root of the spanning-tree instance. The priority value is set as 24576. ● secondary - Sets the switch as a secondary root if the primary root fails. The priority value is set as 28672. >
Mode	Global Configuration Mode

spanning-tree mst configuration

Command Objective	This command enters into MSTP configuration Mode, where instance specific and MST region configuration can be done.
✏	This command can be executed successfully, only if the spanning tree functionality is started and enabled in the switch. The type of spanning tree Mode should be set as mst.
Syntax	spanning-tree mst configuration
Mode	Global Configuration Mode

name

Command Objective	This command configures the name for the MST region. The name is unique and used to identify the specific MST region. Each MST region contains multiple spanning tree instances and runs special instance of spanning tree known as IST to disseminate STP topology information for other STP instances. The no form of this command resets the name to its default value.
Syntax	name <string(optional max Length)> no name
Mode	MSTP Configuration Mode

revision

Command Objective	This command configures the revision number for the MST region. This value ranges between 0 and 65535. The no form of this command resets the revision number to

	its default value.
Syntax	revision <value(0-65535)> no revision
Mode	MSTP Configuration Mode

instance

Command Objective	This command creates an MST instance and maps it to VLANs. The no form of this command deletes the instance / unmaps specific VLANs from the MST instance.
Syntax	instance <instance-id(1-64 | 4094)> vlan <vlan-range> no instance <instance-id (1-64 | 4094)> [vlan <vlan-range>]
Mode	MSTP configuration Mode

spanning-tree auto-edge

Command Objective	This command enables automatic detection of Edge port parameter of an interface. The no form of this command disables automatic detection of Edge port parameter of an interface. The automatic detection of Edge port parameter is disabled, even if the spanning tree Mode is changed. Once automatic detection is enabled, the Edge port parameter is automatically detected and set. The port is set as edge port, if no BPDU is received on the port. The port is set as non-edge port, if any BPDU is received.
✏	The automatic detection of Edge port parameter can be configured in the switch, only if the spanning tree functionality is not shut down in the switch. The type of spanning tree Mode should be set if the functionality is already shutdown.
Syntax	spanning-tree auto-edge no spanning-tree auto-edge
Mode	Interface Configuration Mode

This command is applicable in PORT/PORT-CHANNEL Interface Mode.

spanning-tree - Properties of an interface

Command Objective

This command configures the port related spanning tree information for all kinds of STPs. This can be applied for any port, in RSTP/MSTP Mode. This command creates port in STP when Automatic Port Create feature is disabled.

The no form of this command resets the port related spanning tree information to its default value. The port related spanning tree information is changed to its default value even if the spanning tree Mode is changed. This command also deletes port in STP when Automatic Port Create feature is disabled.

✏

In STP module, whenever a port is mapped to any context, the corresponding port is created irrespective of whether STP is intended to be enabled on that interface. This leads To STP scaling issues and this problem is solved by having control at STP module on the port entry creation at STP module itself.

Syntax

```
spanning-tree [{cost <value(0-200000000)>|disable|link-type{point-to-point|shared}|port-priority <value(0-240)>}]
```

no spanning-tree [{cost |disable|link-type|port-priority}]

Parameter Description

● cost <value(0-200000000)> - Configures the port’s path cost value that contributes to the path cost of paths containing this particular port. The paths’ path cost is used during calculation of shortest path to reach the root. The path cost represents the distance between the root port and designated port. This value ranges between 1 and 200000000. The configured path cost is used, even if the dynamic path cost calculation feature or LAGG speed feature is enabled.

● disable - Disables the spanning tree operation on the port. The port does not take part in the execution of spanning tree operation for preventing undesirable loops in the network.

■ link-type - Configures the link status of the LAN segment attached to the port. The options available are:

◆ point-to-point – The port is treated as if it is connected to a point-to-point link.

◆ shared - The port is treated as if it is using a shared media connection.

● port-priority – 128

>

Mode

Interface Configuration Mode

This command is applicable in PORT/PORT-CHANNEL Interface Mode.

spanning-tree mst- Properties of an interface for MSTP

Command Objective	This command configures the port related spanning tree information for a specified MSTI in a port. The no form of this command resets the spanning tree information of a port to its default value.
✏	This command can be executed successfully, only if the spanning tree functionality is not shut down in the switch. The type of spanning tree Mode should be set as mst.

Syntax	spanning-tree mst <instance-id(1-64)> { cost <value(1-200000000)>| port-priority <value(0-240)> | disable }
	no spanning-tree mst <instance-id(1-64)>{cost|port-priority | disable}

Parameter Description	● <instance-id(1-64)> - Configures the ID of MSTP instance already created in the switch. This value ranges between 1 to 64. ● cost<value(1-200000000)> - Configures the port's path cost value that contributes to the path cost of paths containing this particular port. The paths' path cost is used during calculation of shortest path to reach the root. The path cost represents the distance between the root port and designated port. This value ranges between 1 and 200000000. The configured path cost is used, even if the dynamic path cost calculation feature or LAGG speed feature is enabled. ● port-priority<value(0-240)> - Configures the priority value

	assigned to the port. This value is used during port role selection process. This value ranges between 0 and 240. This value should be set in steps of 16, that is, you can set the value as 0, 16, 32, 48, and so on. The MSTP puts the interface with lowest number in forwarding state and blocks all other interfaces, if all interfaces have the same priority value. ● disable - Disables the spanning tree operation on the port. The port does not take part in the execution of spanning tree operation for preventing undesirable loops in the network. >
Mode	Interface Configuration Mode This command is applicable in PORT/PORT-CHANNEL Interface Mode.

show spanning-tree - Summary, Blockedports, Pathcost

Command Objective	This command displays spanning tree related information available in the switch for the current STP enabled in the switch. The information contains priority, address and timer details for root and bridge, status of dynamic path cost calculation feature, status of spanning tree function, STP compatibility version used, configured spanning tree Mode, bridge and port level spanning tree statistics information, and details of ports enabled in the switch. The port details contain port ID, port role, port state, port cost, port priority and link type.

✏	This command can be executed successfully, only if the spanning tree functionality is not shut down in the switch. The type of spanning tree Mode should be set if the functionality is already shutdown.
Syntax	show spanning-tree [{ summary | blockedports | pathcost method }] [switch <context_name>]
Parameter Description	● summary - Displays the currently used STP, applied path cost method and port details such as port ID, port role, port state and port status. ● blockedports - Displays the list of ports in blocked state and the total number of blocked ports. ● pathcost method - Displays the port path cost method configured for the switch. ● switch <context_name> - Displays the STP related information in the switch, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature. >
Mode	Privileged EXEC Mode

show spanning-tree detail

Command Objective

This command displays detailed spanning tree related information of the switch and all ports enabled in the switch.

The information contains status of spanning tree operation, current selected spanning Mode, current spanning tree compatibility version, bridge and root priority, bridge and root addresses, port path cost, port priority, port timers, bridge, and port level spanning tree statistics information, transmit hold-count value, link-type, and status of L2GP, loop guard, BPDU receive, BPDU transmit, restricted TCN, restricted role and port fast features.

✏

This command can be executed successfully, only if the spanning tree functionality is not shut down in the switch. The type of spanning tree Mode should be set if the functionality is already shutdown.

Syntax

```
show spanning-tree detail [ switch <context_name>]
```

Parameter

Description

- switch <context_name> - Displays detailed spanning tree related information, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.

>

Mode

Privileged EXEC Mode

show spanning-tree active

Command Objective

This command displays spanning tree related information available in the switch for the current STP enabled in the switch.

The information contains priority, address and timer details for root and bridge, status of dynamic path cost calculation feature, status of spanning tree function, STP compatibility version used, configured spanning tree Mode, bridge and port level spanning tree statistics information, and details of ports enabled in the switch. The port details contain port ID, port role, port state, port cost, port priority and link type.

✏

This command can be executed successfully, only if the spanning tree functionality is not shut down in the switch. The type of spanning tree Mode should be set if the functionality is already shutdown.

Syntax

show spanning-tree active [detail] [switch <context_name>]

Parameter Description

- detail - Displays detailed spanning tree related information of the switch and all ports enabled in the switch. The information contains status of spanning tree operation, current selected spanning Mode, current spanning tree compatibility version,

	bridge and root priority, bridge and root addresses, port path cost, port priority, port timers, bridge, and port level spanning tree statistics information, transmit hold-count value, link-type, and status of L2GP, loop guard, BPDU receive, BPDU transmit, restricted TCN, restricted role and port fast features. ● switch <context_name> - Displays spanning tree related information available in the switch, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature. >
Mode	Privileged EXEC Mode

show spanning-tree interface

Command Objective	This command displays the port related spanning tree information for the specified interface. The information contains port ID, port role, port state, port cost, port priority and link type.
✏	This command can be executed successfully, only if the spanning tree functionality is not shut down in the switch. The type of spanning tree Mode should be set if the functionality is already shutdown.

Syntax

show spanning-tree interface <interface-type> <interface-id> [{ cost | priority | portfast | rootcost | restricted-role | restricted-tcn | state | stats | detail }]

Parameter Description

- <interface-type> - Displays the port related spanning tree information for the specified type of interface. The interface can be:
  - gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
  - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
- <interface-id> - Displays the information about the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface type port-channel. For Example: 1 represents port-channel ID.
- cost - Displays the cost of the port or instances assigned to that port.
- priority - Displays the priority of the port or instances assigned to that port.
- rootcost - Displays the root cost of the port or instances assigned to that port. The root cost defines the path cost to reach the root bridge.
- restricted-role - Displays the status of the restricted role feature for the port. This option cannot be executed in the PVRST

	Mode. ● restricted-tcn - Displays the status of the restricted TCN feature for the port. This option cannot be executed in the PVRST Mode. ● state - Displays the state of the port. ● stats - Displays the port level spanning tree statistics information. ● detail - Displays detailed spanning tree related information for the port. The information contains current selected spanning Mode, bridge and root priority, bridge and root addresses, port path cost, port priority, port timers, bridge and port level spanning tree statistics information, link-type, and status of L2GP, loop guard, BPDU receive, BPDU transmit, restricted TCN, restricted role and port fast features. >
Mode	Privileged EXEC Mode

show spanning-tree root

Command Objective	This command displays the spanning tree root information. The information contains root ID, root path cost, maximum age time, forward delay time and root port, for the RSTP. The information also contains the instance ID for MSTP.

✏	This command can be executed successfully, only if the spanning tree functionality is not shut down in the switch. The type of spanning tree Mode should be set if the functionality is already shutdown.
Syntax	show spanning-tree root [{ address | cost | forward-time | id | max-age | port | priority | detail }] [switch <context_name>]
Parameter **Description**	● address - Displays the MAC address of the root bridge. ● cost - Displays the cost of the root bridge. ● forward-time - Displays the forward delay time of the root bridge. ● id - Displays the ID of the root bridge. ● max-age - Displays the maximum age time of the root bridge. ● port - Displays the ID of the root port. ● priority - Displays the priority of the root bridge. ● detail - Displays the root priority, root address, root cost, root port, forward delay time and maximum age time. ● switch <context_name> - Displays spanning tree root information, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature. >
Mode	Privileged EXEC Mode

show spanning-tree bridge

Command Objective	This command displays the spanning tree bridge information. The information contains bridge ID, hello time, maximum age time, forward delay time and protocol enabled, for the RSTP. The information also contains the instance ID for MSTP.
✏	This command can be executed successfully, only if the spanning tree functionality is not shut down in the switch. The type of spanning tree Mode should be set if the functionality is already shutdown.
Syntax	show spanning-tree bridge [{ address | forward-time | hello-time | id | max-age | protocol | priority | detail }] [switch <context_name>]
Parameter Description	● address - Displays the MAC address of the bridge. ● forward-time - Displays the forward delay time of the bridge. ● hello-time - Displays the hello time of the bridge. ● id - Displays the ID of the bridge. ● max-age - Displays the maximum age time of the bridge. ● protocol - Displays the protocol currently enabled in the

	bridge. ● priority - Displays the priority of the bridge. ● detail - Displays the priority, address, maximum age time and forward delay time for the bridge. ● switch - Displays spanning tree bridge information, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature. >
Mode	Privileged EXEC Mode

show spanning-tree mst - CIST or specified mst Instance

Command Objective	This command displays multiple spanning tree information for all MSTIs in the switch. The information contains MSTI ID, VLAN IDs mapped to the instance, bridge address and priority, root address and priority, IST root address, priority and path cost, forward delay, maximum age, maximum hop count, and port details of interfaces enabled in the switch. The port details contain interface ID, port role, port state, port cost, port priority and port link type.
✏	This command can be executed successfully, only if the spanning tree functionality is not shut down in the switch.

	The type of spanning tree Mode should be set as mst.
Syntax	show spanning-tree mst [<instance-id(1-64 | 4094)>] [detail] [switch <context_name>]
Parameter Description	● <instance-id(1-64)> - Displays the multiple spanning tree information for the specified MSTI. This value ranges between 1 to 64. ● detail - Displays the detailed multiple spanning tree information for the MSTI. This information contains MSTI ID, VLAN IDs mapped to the instance, bridge address and priority, root address and priority, IST root address, priority and path cost, forward delay, maximum age, maximum hop count, and BPDUs sent and received in the port. ● switch<context_name> - Displays multiple spanning tree bridge information, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature. >
Mode	Privileged EXEC Mode

show spanning-tree mst configuration

Command Objective	This command displays multiple spanning tree instance related information. This information contains the MST

	region name, MST region revision, and a list containing MSTI IDs and VLAN IDs mapped to the corresponding MSTI.
✏	This command can be executed successfully, only if the spanning tree functionality is not shut down in the switch. The type of spanning tree Mode should be set as mst.
Syntax	show spanning-tree mst configuration [switch <context_name>]
Parameter Description	● switch <context_name> - Displays multiple spanning tree instance related information, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature. >
Mode	Privileged EXEC Mode

show spanning-tree mst - Port Specific Configuration

Command Objective	This command displays multiple spanning tree port specific information for the specified port. This information contains interface ID, edge port status, port link type, port hello time, BPDUs sent and received on the port, and instance related details. The instance details contain MSTI ID, MSTI role, MSTI status, MSTI cost and MSTI priority.

✏ This command can be executed successfully, only if the spanning tree functionality is not shut down in the switch. The type of spanning tree Mode should be set as mst.

Syntax

show spanning-tree mst [<instance-id(1-64)>] interface <interface-type> <interface-id> [{ stats | hello-time | detail }]

Parameter Description

- <instance-id(1-64)> - Displays the multiple spanning tree port specific information for the specified MSTI. This value ranges between 1 to 64.

- <interface-type> - Displays the port related spanning tree information for the specified type of interface. The interface can be:

  ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.

  ■ port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.

- <interface-id> - Displays the information about the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface type port-channel. For Example: 1 represents port-channel ID.

- stats - Displays the number of BPDUs sent and received for the MSTIs assigned to the specified interface.

	● hello-time - Displays the hello time of the MSTIs assigned to the specified interface. ● detail - Displays detailed multiple spanning tree port specific information for the specified interface. The information contains port priority, port cost, root address, priority and cost, IST address, priority and cost, bridge address, priority and cost, forward delay, maximum age, maximum hop count, and BPDUs sent and received. >
Mode	Privileged EXEC Mode

show customer spanning-tree

Command Objective	This command displays the detailed customer spanning tree information.
Syntax	show customer spanning-tree [cep interface <interface-type><interface-number>] [{ detail [active] | active [detail] }]
Parameter Description	● <interface-type> - Displays the port related spanning tree information for the specified type of interface. The interface can be: ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.

	■ port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. ● detail - - Displays in detail about the port and bridge. This includes designated Bridge details, designated port details, timer values, root bridge and so on. ● active - Displays the Bridge and details of the active (active ports are those ports that are participating in the spanning-tree) ports >
Mode	Privileged EXEC Mode

show spanning-tree - layer2-gateway-port

Command Objective	This command displays spanning tree layer two gateway port specific configuration.
Syntax	show spanning-tree [interface <interface-type> <interface-id>] layer2-gateway-port [switch <context_name>]
Parameter Description	● <interface-type> - Displays the port related spanning tree information for the specified type of interface. The interface can be: ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. ■ port-channel – Logical interface that represents an

	aggregator which contains several ports aggregated together. >
Mode	Privileged EXEC Mode

LBD

lbd

Command Objective	This command enables/disables Loopback Detection.
Syntax	lbd { enable | disable }
Mode	Global Configuration Mode

show lbd state

Command Objective	This command displays the Loopback Detection information.
Syntax	show lbd state
Mode	Privileged EXEC Mode

show lbd port state

Command Objective	This command displays the Loopback Detection information of each port.
Syntax	show lbd port state
Mode	Privileged EXEC Mode

MAC Address Table

mac-address-table static unicast

Command Objective

This command configures a static unicast MAC address in the forwarding database.

The no form of the command deletes a configured static Unicast MAC address from the forwarding database.

Syntax

mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id > interface <interface-type> <iface_list>

no mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id >

Parameter Description

- <aa:aa:aa:aa:aa:aa> - Configures the static unicast destination MAC address. The received packets having the specified MAC address are processed.
- vlan <vlan-id> - Configures the static unicast destination MAC address for the specified VLAN. This value ranges between 1 and 4094.
  - <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
- interface - Configures the member ports interface type and ID. The details to be provided are:
  - <interface-type> - Configures the member ports for the specified type of interface. The interface can be:

◆ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.

■ <0/a-b, 0/c, ...> - Configures the member ports for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. Port-channel ID is provided, for interface type port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1, 0/3 or 1, 3.

>

Mode	Global Configuration Mode

mac-address-table aging-time

Command Objective	This command configures the timeout period (in seconds) for aging out dynamically learned forwarding information entry and static entry in the MAC address table. That is, the entry is deleted once the aging timer expires. High value for the aging time helps to record dynamic entries for a longer time if traffic is not frequent. This reduces the possibility of flooding. The no form of the command resets the maximum age of an entry in the MAC address table to its default value.
Syntax	mac-address-table aging-time <10-630 seconds>

	no mac-address-table aging-time
Mode	Global Configuration Mode

show mac-address-table

Command Objective	This command displays all static / dynamic unicast and multicast MAC entries created in the MAC address table. These entries contain VLAN ID, unicast / multicast MAC address, unicast backbone MAC address of peer backbone edge bridge, member ports, the type of entry (that is static, learnt and so on), and total number of entries displayed.
Syntax	show mac-address-table [vlan <string(9)>] [address <mac_addr>] [{interface <interface-type> <ifnum> | switch <string(32)>}]
Parameter Description	● vlan <vlan-range>- Displays all static / dynamic unicast and multicast MAC entries created in the MAC address table for the specified VLANs alone. This value denotes the VLAN ID range for which the entries need to be displayed. This value is a string with the maximum size as 9. For example, the value is provided as 4000-4010 to display the entries for VLAN IDs from 4000 to 4010. ● address <aa:aa:aa:aa:aa:aa> - Displays all static / dynamic unicast and multicast MAC entries created in the MAC address

	table for the specified unicast / multicast MAC address. ● <interface-type> - Sets the type of interface. ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. ● switch <context_name> - Displays the VLAN global information that is applicable to all VLANs, for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
Mode	● Privileged EXEC Mode

show mac-address-table count

Command Objective	This command displays the total number of static / dynamic unicast and multicast MAC address entries created in the FDB table. The count is displayed for all active VLANs, VLANs (that are not active) for which the port details are configured, and VLANs for which the MAC address table entries are created.
Syntax	show mac-address-table count [vlan <vlan_id>] [switch <string(32)>]
Parameter Description	● vlan <vlan-id>- Displays the total number of static / dynamic unicast and multicast MAC address entries created for the

	specified VLAN ID. This value ranges between 1 and 65535. ● switch <context_name> - Displays the VLAN global information that is applicable to all VLANs, for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
Mode	Privileged EXEC Mode

show mac-address-table static multicast/unicast

Command Objective	This command displays the static multicast/unicast MAC address entries created in the FDB table. These entries contain VLAN ID to which multicast/unicast MAC address entry is assigned, multicast/unicast MAC address, member ports, receiver ports, forbidden ports, the status of entry (that is permanent, static, and so on), and total number of entries displayed.
Syntax	show mac-address-table static multicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-id> | switch <context_name>}]

```
show mac-address-table static unicast [vlan <vlan-range>]
[address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type>
<interface-id> | switch <context_name>}]
```

Parameter Description

- vlan <vlan-range>- Displays all static / dynamic unicast and multicast MAC entries created in the MAC address table for the specified VLANs alone. This value denotes the VLAN ID range for which the entries need to be displayed. This value is a string with the maximum size as 9. For example, the value is provided as 4000-4010 to display the entries for VLAN IDs from 4000 to 4010.

- address <aa:aa:aa:aa:aa:aa> - Displays all static / dynamic unicast and multicast MAC entries created in the MAC address table for the specified unicast / multicast MAC address.

- <interface-type> - Displays all static multicast MAC address entries for the specified interface.

  - ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.

- switch <context_name> - Displays the VLAN global information that is applicable to all VLANs, for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

>

Mode Privileged EXEC Mode

show mac-address-table dynamic unicast

Command Objective	This command displays all dynamically learnt unicast entries from the MAC address table. These entries contain VLAN ID for which unicast MAC address entry is learnt, unicast MAC address, ports through which the entry is learnt, the status of entry (that is permanent, static, and so on), the unicast backbone MAC address of peer backbone edge bridge, and total number of entries displayed.
Syntax	show mac-address-table dynamic unicast [vlan <string(9)>] [address <ucast_mac>] [{interface <interface-type> <ifnum> | switch <string(32)>}]
Parameter Description	● vlan <vlan-range>- Displays all static / dynamic unicast and multicast MAC entries created in the MAC address table for the specified VLANs alone. This value denotes the VLAN ID range for which the entries need to be displayed. This value is a string with the maximum size as 9. For example, the value is provided as 4000-4010 to display the entries for VLAN IDs from 4000 to 4010. ● address <aa:aa:aa:aa:aa:aa> - Displays all static / dynamic unicast and multicast MAC entries created in the MAC address table for the specified unicast / multicast MAC address. ● <interface-type> - Displays all static multicast MAC address entries for the specified interface. ■ gigabitethernet – A version of LAN standard architecture that

	supports data transfer up to 1 Gigabit per second. ● switch <context_name> - Displays the VLAN global information that is applicable to all VLANs, for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature. >
Mode	Privileged EXEC Mode

show mac-address-table aging-time

Command Objective	This command displays the ageing time configured for the MAC address table. This time denotes the interval (in seconds) after which the dynamically learned forwarding information entry and static entry in the MAC address table are deleted.
Syntax	show mac-address-table aging-time [switch <string(32)>]
Parameter Description	● switch <context_name> - Displays ageing time of the MAC address table, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature. >

Mode

Privileged EXEC Mode

show dot1d mac-address-table

Command Objective

This command displays all static / dynamic unicast and multicast MAC address entries created in the FDB table, when the VLAN base bridge mode is transparent bridging.

These entries contain unicast / multicast MAC address, member ports, and the type of entry (that is static, learnt and so on).

Syntax

```
show dot1d mac-address-table [address <aa:aa:aa:aa:aa:aa>]
[{interface <interface-type> <interface-id> | switch
<context_name>}]
```

Parameter Description

- address <aa:aa:aa:aa:aa:aa> - Displays all static / dynamic unicast and multicast MAC entries created in the MAC address table for the specified unicast / multicast MAC address.

>

- <interface-type> - Displays the interface status and configuration for the specified type of interface. The interface can be:

■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.

■ port-channel – Logical interface that represents an

	aggregator which contains several ports aggregated together. > ● switch <context_name>- Displays the VLAN entry related information or total number of existing VLANs, for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
Mode	Privileged EXEC Mode >

show dot1d mac-address-table static multicast

Command Objective	This command displays all static multicast MAC address entries created in the FDB table, when the VLAN base bridge mode is transparent bridging. These entries contain multicast MAC address, member ports, receiver ports, the status of entry (that is permanent, static, and so on), and total number of entries displayed.
Syntax	show dot1d mac-address-table static multicast [address <aa:aa:aa:aa:aa:aa>] [interface <interface-type> <interface-id>]

Parameter Description

- address <aa:aa:aa:aa:aa:aa> - Displays all static / dynamic unicast and multicast MAC entries created in the MAC address table for the specified unicast / multicast MAC address.

>

- <interface-type> - Displays the interface status and configuration for the specified type of interface. The interface can be:

■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.

■ port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.

>

- switch <context_name>- Displays the VLAN entry related information or total number of existing VLANs, for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode Privileged EXEC Mode

>

show dot1d mac-address-table static unicast

Command Objective

This command displays all static unicast MAC address entries created in the FDB table, when the VLAN base bridge mode is transparent bridging.

These entries contain unicast MAC address, member ports, receiver ports, the status of entry (that is permanent, static, and so on), and total number of entries displayed.

Syntax

```
show dot1d mac-address-table static unicast [address <aa:aa:aa:aa:aa:aa>] [interface <interface-type> <interface-id>]
```

Parameter Description

- address <aa:aa:aa:aa:aa:aa> - Displays all static / dynamic unicast and multicast MAC entries created in the MAC address table for the specified unicast / multicast MAC address.

>

- <interface-type> - Displays the interface status and configuration for the specified type of interface. The interface can be:

  - ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.

  - ■ port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.

>

- switch <context_name>- Displays the VLAN entry related information or total number of existing VLANs, for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode	Privileged EXEC Mode >

LLDP

set lldp

Command Objective	This command transmits or receives LLDP frames from the server to the LLDP module.
Syntax	set lldp {enable | disable}
Parameter Description	● enable - Transmits/receives the LLDP packets between LLDP module and the server. ● disable - Does not transmit/receive the LLDP packets between LLDP module and the server. >
Mode	Global Configuration Mode

set lldp version

Command Objective	This command enables the lldp version to be used on the system.
Syntax	set lldp version {v1 | v2}
Parameter	● v1 - Enables LLDP 2005 version 1 on the port

Description	> ● v2 - Enables LLDP 2009 version 2 on the port >
Mode	Global Configuration Mode

lldp transmit-interval

Command Objective	This command sets the transmission interval in which the server sends the LLDP frames to the LLDP module. The value ranges between 5 and 32768 seconds. The no form of the command sets the transmission interval to the default value.
Syntax	lldp transmit-interval <seconds(5-32768)> no lldp transmit-interval
Mode	Global Configuration Mode

lldp holdtime-multiplier

Command Objective	This command sets the holdtime-multiplier value, which is the amount of time, the server should hold the LLDP. The value ranges between 2 and 10 seconds. The no form of the command sets the multiplier to the default value.
✏	TLV (Time to Live) A value that tells the receiving agent, how long the information contained in the TLV Value field is valid. TTL = message transmission interval * hold time multiplier. For Example, if the value of LLDP transmission interval is 30, and the value of the LLDP hold multiplier is 4, then the value 120 is encoded in the TTL field in the LLDP header.
Syntax	lldp holdtime-multiplier <value(2-10)> no lldp holdtime-multiplier
Mode	Global Configuration Mode

lldp reinitialization-delay

Command Objective	This command sets the reinitialization delay time which is the minimum time an LLDP port will wait before reinitializing LLDP transmission. The value ranges between 1 and 10 seconds. The no form of the command sets the reinitialization delay time to the default value.
Syntax	lldp reinitialization-delay <seconds(1-10)> no lldp reinitialization-delay
Mode	Global Configuration Mode

lldp tx-delay

Command Objective	This command sets the transmit delay which is the minimum amount of delay between successive LLDP frame transmissions. The value ranges between 1 and 8192 seconds. The no form of the command sets the transmit delay to the default value.
✏	TxDelay should be less than or equal to (0.25 * Message Tx Interval)

Syntax	lldp tx-delay <seconds(1-8192)> no lldp tx-delay
Mode	Global Configuration Mode

show lldp

Command Objective	This command displays LLDP global configuration details to initialize on an interface.
Syntax	show lldp
Mode	Privileged EXEC Mode

show lldp interface

Command Objective	This command displays the information about interfaces where LLDP is enabled.

Syntax	show lldp interface [<interface-type> <interface-id>] [mac-address <mac_addr>]
Parameter Description	● <interface-type> - Displays the information about the specified type of interface. The interface can be: ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. ● <interface-id> - Displays the information about the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface type port-channel. For Example: 1 represents port-channel ID. ● mac-address <mac_addr> - Displays information about neighbors for the specified destination MAC address of the LLDP agent. >
Mode	Privileged EXEC Mode

show lldp neighbors

Command Objective	This command displays information about neighbors on an interface or all interfaces.

Syntax

show lldp neighbors [chassis-id <string(255)> port-id <string(255)>] [<interface-type> <interface-id> [mac-address<mac_addr>]][detail]

Parameter Description

- chassis-id <string(255)> - Configures the chassis identifier string. This value is a string value with a maximum size of 255.

- port-id <string(255)> - Configures the port number that represents the concerned aggregation port This value is a string value with a maximum size of 255.

- <interface-type> - Displays information about neighbors for the specified type of interface. The interface can be:

■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.

- <interface-id> - Displays information about neighbors for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface type port-channel. For Example: 1 represents port-channel ID.

- mac-address <mac_addr> - Displays information about neighbors for the specified destination MAC address of the LLDP agent.

- detail - Displays the information obtained from all the received TLVs .

>

Mode

Privileged EXEC Mode

show lldp local

Command Objective This command displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces.

Syntax show lldp local {[<interface-type> <interface-id> [mac-address <mac_addr>]] | [mgmt-addr]}

Parameter Description

- <interface-type> - Displays the current switch information for the specified type of interface. The interface can be:

■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.

- <interface-id> - Displays the current switch information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface type port-channel. For Example: 1 represents port-channel ID.

- mac-address <mac_addr> - Displays information about neighbors for the specified destination MAC address of the LLDP agent.

- mgmt-addr - All the management addresses configured in the system and Tx enabled ports.

>

Mode Privileged EXEC Mode

show lldp peers

Command Objective This command displays information about neighbors learnt on an interface or all interfaces.

Syntax show lldp peers [chassis-id <string(255)> port-id <string(255)>] <interface-type> <interface-id>[[mac-address <mac_addr>] [detail]]

Parameter Description

- <interface-type> - Displays the current switch information for the specified type of interface. The interface can be:

■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.

- <interface-id> - Displays the current switch information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface type port-channel. For Example: 1 represents port-channel ID.

- mac-address <mac_addr> - Displays information about neighbors for the specified destination MAC address of the LLDP

	agent. >
Mode	Privileged EXEC Mode

IGMP

ip igmp querier-timeout

Command Objective	This command sets the IGMP snooping router port purge time-out interval. Snooping learns the available router ports and initiates router port purge time-out timer for each learnt router port. The routers send control messages to the ports. If the router ports receive such control messages, the timer is restarted. If no message is received by the router ports before the timer expires, the router port entry is purged. The purge time-out value ranges between 60 and 600 seconds. This command is a standardized implementation of the existing command; ip igmp snooping mrouter-time-out. It operates similar to the existing command.
Syntax	ip igmp querier-timeout <(60 - 600) seconds>
Mode	Global Configuration Mode

ip igmp snooping vlan - immediate leave

Command Objective	This command enables fast leave processing and IGMP snooping for a specific VLAN. It enables IGMP snooping only for the specific VLAN, when IGMP snooping is globally disabled. When the fast leave feature is enabled, port information is removed from a multicast group entry immediately after fast leave message is received. The ID of the VLAN ranges between 1 and 4094. The no form of the command disables fast leave processing for a specific VLAN. This command is a standardized implementation of the existing command; ip igmp snooping fast-leave. It operates similar to the existing command.
✏	Fast leave configurations done in a VLAN when IGMP snooping is disabled in a VLAN, will be applied only when IGMP snooping is enabled in the VLAN.
Syntax	ip igmp snooping vlan <vlanid(1-4094)> immediate-leave no ip igmp snooping vlan <vlanid(1-4094)> immediate-leave
Mode	Global Configuration Mode

ip igmp snooping mrouter

Command Objective	This command enables IGMP snooping and configures a list of multicast router ports for a specific VLAN, when IGMP snooping is globally enabled. This will enable IGMP snooping only for the specific VLAN, if IGMP snooping is globally disabled. Any IGMP message received on a switch is forwarded only on the router-ports and not on the host ports. In this manner, the IGMP snooping functionality avoids flooding of IGMP query messages from the host to the entire network. The no form of the command deletes the statically configured router ports for a VLAN .
✏	The list of multicast router ports configured while IGMP snooping is disabled in the VLAN is applied only when the IGMP snooping is enabled in the VLAN.
Syntax	ip igmp snooping vlan <integer (1-4094)> mrouter <ifXtype> <iface_list> no ip igmp snooping vlan <integer (1-4094)> mrouter <ifXtype> <iface_list>
Parameter Description	● <interface-type> - Clears all port-level spanning-tree statistics information for the specified type of interface. The interface can be: ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. ■ port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.

	>
Mode	Config-VLAN Mode

shutdown snooping

Command Objective	This command shuts down snooping in the switch. When the user does not require the IGMP snooping module to be running, it can be shut down. When shut down, all resources acquired by the Snooping Module are released to the system. For the IGS feature to be functional on the switch, the 'system-control' status must be set as 'start' and the 'state' must be 'enabled'. The no form of the command starts and enables snooping in the switch.
✎	Snooping cannot be started in the switch if the base bridge mode is configured as transparent bridging.
Syntax	shutdown snooping no shutdown snooping
Mode	Global Configuration Mode

snooping multicast-forwarding-mode

Command Objective	This command specifies the snooping multicast forwarding mode (IP based or MAC based).
Syntax	snooping multicast-forwarding-mode {ip | mac}
Parameter Description	● ip - Configures the multicast forwarding mode as IP Address based. The PIM queries the IGS module to obtain the Portlist. ● mac - Configures the multicast forwarding mode as MAC Address based. The PIM queries the VLAN to obtain the Portlist. >
Mode	Global Configuration Mode

ip igmp snooping

Command Objective	This command enables IGMP snooping in the switch/ a specific VLAN. When snooping is enabled in a switch or interface, it learns the hosts intention to listen to a specific multicast address. When the switch receives any packet from the specified multicast address, it forwards the

	packet to the host listening for that address. Broadcasting is avoided to save bandwidth. When IGMP snooping is enabled globally, it is enabled in all the existing VLAN interfaces. The no form of the command disables IGMP snooping in the switch/a specific VLAN. When IGMP snooping is disabled globally, it is disabled in all the existing VLAN interfaces.
Syntax	Global Configuration Mode ip igmp snooping [vlan < vlan–id >] no ip igmp snooping [vlan < vlan–id >] Config-VLAN Mode ip igmp snooping no ip igmp snooping
Parameter Description	● <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094. >
Mode	Global Configuration Mode / Config-VLAN Mode

ip igmp snooping report-suppression interval

Command Objective

This command sets the IGMP snooping report-suppression time interval. The switch forwards IGMPv2 report message to the multicast group. A timer is started immediately after forwarding the report message and runs for set period of time. During this interval, the switch does not forward another IGMPv2 report message addressed to the same multicast group to the router ports.

The no form of the command sets the IGMP snooping report-suppression interval time to the default value.

The ip igmp snooping report-suppression-interval is used only when the proxy and proxy-reporting are disabled.

Syntax

```
ip igmp snooping report-suppression-interval <(1 – 25) seconds>
```

```
no ip igmp snooping report-suppression-interval
```

Mode

Global Configuration Mode

ip igmp snooping group-query-interval

Command Objective

This command sets the time interval after which the switch sends a group specific query to find out if there are any interested receivers in the group when it receives a leave message. If it does not receive a response from the group, the port is removed from the group membership information in the forwarding database. This value ranges between 2 and 5.

The no form of the commands sets the group specific query interval time to default value.

Syntax

```
ip igmp snooping group-query-interval <2-5) seconds>

no ip igmp snooping group-query-interval
```

Mode

Global Configuration Mode

ip igmp snooping version

Command Objective

This command configures the operating version of the IGMP snooping switch for a specific VLAN. The version can be set manually to execute condition specific commands.

Syntax	ip igmp snooping version { v1 |v2 | v3}
Parameter Description	● v1 - **Configures the version as IGMP snooping Version 1.** ● v2 - **Configures the version IGMP snooping Version 2.** ● v3 - **Configures the version IGMP snooping Version 3.** >
Mode	Config-VLAN Mode

ip igmp snooping fast-leave

Command Objective	This command enables fast leave processing and IGMP snooping for a specific VLAN. It enables IGMP snooping only for the specific VLAN, when IGMP snooping is globally disabled. When the fast leave feature is enabled, port information is removed from a multicast group entry immediately after fast leave message is received. The no form of the command disables fast leave processing for a specific VLAN.
✎	Fast leave configurations done in a VLAN when IGMP snooping is disabled in a VLAN, will be applied only when IGMP snooping is enabled in the VLAN.
Syntax	ip igmp snooping fast-leave

	no ip igmp snooping fast-leave
Mode	Config-VLAN Mode

ip igmp snooping querier

Command Objective	This commands configures the IGMP snooping switch as a querier for a specific VLAN. When configured as a querier, the switch sends IGMP query messages. The query messages will be suppressed if there are any routers in the network. The no form of the command configures the IGMP snooping switch as non-querier for a specific VLAN.
Syntax	ip igmp snooping querier no ip igmp snooping querier
Mode	Config-VLAN Mode

ip igmp snooping query-interval

Command Objective	This command sets the time period with which the general queries are sent by the IGMP snooping switch when configured as querier on a VLAN. The value range is between 60 to 600 seconds. The no form of the command sets the IGMP querier interval to default value.
✎	The switch must be configured as a querier for this configuration to be imposed.
Syntax	ip igmp snooping query-interval <(60 - 600) seconds> no ip igmp snooping query-interval
Mode	Config-VLAN Mode

ip igmp snooping startup-query-interval

Command Objective	This command sets the time interval between the general query messages sent by the IGMP snooping switch, during startup of the querier election process. This time interval ranges between 15 and 150 seconds and should be less than or equal to query interval/ 4. The no form of the command sets the IGMP startup query interval to the default value.

✎

The switch should be configured as querier for the startup query interval command to produce results.

The startup query interval should be less than or equal to ¼ of the query interval.

Syntax

ip igmp snooping startup-query-interval <(15 - 150) seconds>

no ip igmp snooping startup-query-interval

Mode

Config-VLAN Mode

ip igmp snooping startup-query-count

Command Objective

This command sets the maximum number of general query messages sent out on switch startup, when the switch is configured as a querier. This value ranges between two and five. Startup query messages are sent to announce the presence of the switch along with its identity. The startup query count is manually configured to change the existing count. This value ranges between 2 and 5.The no form of the command sets the number of general query messages sent out on switch startup, when the switch is configured as a querier to default value.

✎

The switch should be configured as a querier for startup query count configuration to be effective.

Syntax

ip igmp snooping startup-query-count <2 - 5>

	no ip igmp snooping startup-query-count
Mode	Config-VLAN Mode

no ip igmp snooping other-querier-present-interval

Command Objective	This command sets the other querier present interval to default value.
Syntax	no ip igmp snooping other-querier-present-interval
Mode	Config-VLAN Mode

ip igmp snooping max-response-code

Command Objective	This command sets the maximum response code inserted in general queries sent to host. The unit of the response code is tenth of second. This value ranges between 0 and 255. The no form of the command sets the query response code to default value.
Syntax	ip igmp snooping max-response-code <(0 - 255)>

no ip igmp snooping max-response-code

Mode

Config-VLAN Mode

ip igmp snooping mrouter

Command Objective

This command enables IGMP snooping and configures a list of multicast router ports for a specific VLAN, when IGMP snooping is globally enabled. This will enable IGMP snooping only for the specific VLAN, if IGMP snooping is globally disabled.

Any IGMP message received on a switch is forwarded only on the router-ports and not on the host ports. In this manner, the IGMP snooping functionality avoids flooding of IGMP query messages from the host to the entire network.

The no form of the command deletes the statically configured router ports for a VLAN .

✏

The list of multicast router ports configured while IGMP snooping is disabled in the VLAN is applied only when the IGMP snooping is enabled in the VLAN.

Syntax

ip igmp snooping mrouter <interface-type> <0/a-b, 0/c, ...>

no ip igmp snooping mrouter <interface-type> <0/a-b, 0/c, ...>

Parameter Description	● <interface-type> - Clears all port-level spanning-tree statistics information for the specified type of interface. The interface can be: ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. ■ port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. >
Mode	Config-VLAN Mode

ip igmp snooping mrouter-port

Command Objective	This command configures the router port purge time-out interval for a VLAN.
Syntax	ip igmp snooping mrouter-port <interface-type> <0/a-b, 0/c, ...> time-out <short(60-600)> no ip igmp snooping mrouter-port <interface-type> <0/a-b, 0/c, ...> time-out
Parameter Description	● <interface-type> - Configures the specified type of interface. The interface can be: ■ gigabitethernet - A version of LAN standard architecture that

	supports data transfer up to 1 Gigabit per second. ● <0/a-b, 0/c, ...> - Sets the list of multicast router ports for the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash. Port-channel ID is provided, for interface type port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1, 0/3. ● <short(60-600)> - Time-out value.
Mode	Config-VLAN Mode

ip igmp snooping mrouter-port

Command Objective	This command configures the operating version of the router port for a VLAN.
Syntax	ip igmp snooping mrouter-port <interface-type> <0/a-b, 0/c, ...> version {v1 | v2 | v3} no ip igmp snooping mrouter-port <interface-type> <0/a-b, 0/c, ...> version
Parameter Description	● <interface-type> - Configures the specified type of interface. The interface can be: ■ gigabitethernet - A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. ● <0/a-b, 0/c, ...> - Sets the list of multicast router ports for the list of

	interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash. Port-channel ID is provided, for interface type port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1, 0/3. ● v1 - IGMP snooping Version 1. ● v2 - IGMP snooping Version 2. ● v3 - IGMP snooping Version 3. >
Mode	Config-VLAN Mode

ip igmp snooping blocked-router

Command Objective	This command configures a static router-port as blocked router port. The no form of the command resets the blocked router ports to normal router port.
✎	The ports to be configured as blocked router ports, must not be configured as static router ports.
Syntax	ip igmp snooping blocked-router <interface-type> <0/a-b, 0/c, ...>
Parameter	● <interface-type> - Clears all port-level spanning-tree statistics information for the specified type of interface. The interface can be:

Description	■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. ■ port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. ● <0/a-b, 0/c, ...> - Sets the list of multicast router ports for the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash. Port-channel ID is provided, for interface type port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1, 0/3. >
Mode	Config-VLAN Mode

ip igmp snooping static-group

Command Objective	This command adds static multicast fwd entry in the IGMP Snooping switch.
Syntax	ip igmp snooping static-group <mcast_addr> ports <ifXtype><iface_list> no ip igmp snooping static group <mcast-addr>
Parameter Description	● <mcast_addr> - Mcast Address(ip address). ● <ifXtype> - Clears all port-level spanning-tree statistics information for the specified type of interface. The interface can

be:

  - ■ gigabitethernet - A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.

- ■ port-channel - Logical interface that represents an aggregator which contains several ports aggregated together.

- ● <iface_list> - Sets the list of multicast router ports for the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash. Port-channel ID is provided, for interface type port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1, 0/3.

>

Mode Config-VLAN Mode

show ip igmp snooping mrouter

Command Objective

This command displays the router ports for all VLANs or a specific VLAN for a given switch or for all the switches (if no switch is specified). The interface details and the corresponding port number along with its type (static/dynamic are displayed.

Syntax show ip igmp snooping mrouter [Vlan <vlan-id >] [detail] [switch <switch_name>]

Parameter

- ● < vlan-id (1-4094)> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and

Description	4094 ● detail - Displays detailed information about the router ports ● switch <switch_name> - Displays the router ports for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature. >
Mode	Privileged EXEC Mode

show ip igmp snooping blocked-router

Command Objective	This command displays the blocked router ports for all VLANs or a specific VLAN for a given switch or for all the switches (if no switch is specified).
Syntax	show ip igmp snooping blocked-router [Vlan <vlan-id >] [switch <switch_name>]
Parameter Description	● < vlan-id (1-4094)> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094 ● switch <switch_name> - Displays the blocked router ports for specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

	>
Mode	Privileged EXEC Mode

show ip igmp snooping globals

Command Objective	This command displays IGMP snooping information for all VLANs or a specific VLAN for a given switch or for all switches (if switch is not specified).
Syntax	show ip igmp snooping globals [switch <switch_name>]
Parameter Description	● switch <switch_name> - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature. >
Mode	Privileged EXEC Mode

show ip igmp snooping

Command Objective	This command displays IGMP snooping information for all VLANs or a specific VLAN for a given context or for all the context (if no switch is

	specified).
Syntax	show ip igmp snooping [Vlan <vlan-id >] [switch <switch_name>]
Parameter Description	● < vlan-id (1-4094)> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094 ● switch <switch_name> - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature. >
Mode	Privileged EXEC Mode

show ip igmp snooping groups

Command Objective	This command displays IGMP group information for all VLANs or a specific VLAN or specific VLAN and group address for a given switch or for all switch (if no switch is specified) .
Syntax	show ip igmp snooping groups [Vlan <vlan-id > [Group <Address>]] [switch <switch_name>]
Parameter Description	● < vlan-id (1-4094)> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094

- Group <Address> - Displays the Group Address of the VLAN ID

- switch <switch_name> - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

>

Mode

Privileged EXEC Mode

show ip igmp snooping port-cfg

Command Objective

This command displays IGS port configuration information for all Inner VLANs or a specific Inner VlanId or a given switch.

Syntax

```
show ip igmp snooping port-cfg [{interface <interface-type>
<interface-id> [InnerVlanId vlan-id(1-4094)] | switch
<switch_name>}]
```

Parameter Description

- interface - Interface type and identifier.
  - <interface-type> - Clears all port-level spanning-tree statistics information for the specified type of interface. The interface can be:
    - gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
    - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
- <interface-id> - Displays the IP interface configuration for the specified interface identifier. This is a unique value that represents the

	specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1. ● vlan-id(1-4094) - Vlan index. ● <switch_name> - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature. >
Mode	Privileged EXEC Mode

show ip igmp snooping forwarding-database

Command Objective	show ip igmp snooping forwarding-database
Syntax	show ip igmp snooping forwarding-database [Vlan <vlan-id>] switch <switch_name>]
Parameter Description	● < vlan-id (1-4094)> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094 ● Group <Address> - Displays the Group Address of the VLAN ID ● switch <switch_name> - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to

	multiple instance feature. >
Mode	Privileged EXEC Mode

show ip igmp snooping statistics

Command Objective	This command displays IGMP snooping statistics for all VLANs or a specific VLAN for a given switch or for all switch (if no switch is specified).
Syntax	show ip igmp snooping statistics [Vlan <vlan-id >] [switch <switch_name>]
Parameter Description	● < vlan-id (1-4094)> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094 ● switch <switch_name> - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature. >
Mode	Privileged EXEC Mode

show ip igmp snooping multicast-vlan

Command Objective	This command displays multicast VLAN statistics in a switch and displays various profiles mapped to the multicast VLANs.
Syntax	show ip igmp snooping multicast-vlan [switch <switch_name>]
Parameter Description	● switch <switch_name> - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature. >
Mode	Privileged EXEC Mode

MLD

ipv6 mld snooping

Command Objective	This command enables MLD snooping in the switch or a specific VLAN. Memory resources required by the MLDS module are allocated and the module starts running. It initializes semaphore creation, timer task RBTree, hash table, RBT Tree nodes MLD snooping is enabled and disabled globally in all the existing VLAN interfaces. The no form of this command disables MLD snooping in the switch or a specific VLAN.
✎	The MLDS can be enabled for a VLAN, only if the MLDS is started in the switch and the VLAN is activated.
Syntax	ipv6 mld snooping no ipv6 mld snooping
Mode	Global Configuration Mode/ Config-VLAN Mode

ipv6 mld snooping report-suppression-interval

Command Objective	This command sets the MLD snooping report-suppression interval for which MLDv1 report messages do not get forwarded onto the router ports

	for the same group. This value ranges are between 1 and 25. This timer is used when both proxy and proxy-reporting are disabled. This timer is started as soon as a report message for that group is forwarded out. Within this interval if another report for the same group arrives, it will not be forwarded. The no form of this command sets the MLD snooping report-suppression interval to its default value.
Syntax	ipv6 mld snooping report-suppression-interval <(1-25) seconds> no ipv6 mld snooping report-suppression-interval
Mode	Global Configuration Mode

ipv6 mld snooping group-query-interval

Command Objective	This command sets the time interval after which the switch sends a group specific query on a port. The value ranges between 2 and 5. The no form of this command sets the MLDS query interval to default value.
Syntax	ipv6 mld snooping group-query-interval <(2 - 5) seconds> no ipv6 mld snooping group-query-interval

Mode	Global Configuration Mode

ipv6 mld snooping version

Command Objective	This command configures the operating version of the MLD snooping switch for a specific VLAN.
✎	The configuration can be done only for the VLANs that are activated in the switch.
Syntax	ipv6 mld snooping version {v1 | v2}
Parameter Description	● v1 - Configures the version as MLDv1. MLDS report is accessed only with group address. It is provided with leave request option. ● v2 - Configures the version as MLDv2. MLDS report is accessed with source and group address. >
Mode	Config-VLAN Mode

ipv6 mld snooping fast-leave

Command Objective	This command enables fast leave processing for a specific VLAN. When fast leave is disabled, on reception of a leave message the switch checks if there are any interested receivers for the group by sending a group specific query before removing the port from the forwarding table. If fast leave is enabled, the switch does not send a group specific query and immediately removes the port from the forwarding table. The no form of the command disables fast leave processing for a specific VLAN.
✎	The configuration can be done only for the VLANs that are activated in the switch.
Syntax	ipv6 mld snooping fast-leave no ipv6 mld snooping fast-leave
Mode	Config-VLAN Mode

pv6 mld snooping querier

Command Objective	This command configures the MLD snooping switch as a querier for a specific VLAN. The switch starts sending general queries at regular time intervals. When the router port gets operationally down and there are no router ports in the switch, the switch continues the querier functionality. The no form of this command configures the MLD snooping switch as

	non-querier for a specific VLAN.
✎	The configuration can be done only for the VLANs that are activated in the switch.
Syntax	ipv6 mld snooping querier no ipv6 mld snooping querier
Mode	Config-VLAN Mode

ipv6 mld snooping query-interval

Command Objective	This command sets the time period for which the switch waits after sending a group specific query to determine if the hosts are still interested in a specific multicast group.. The value ranges between 60 and 600. In proxy reporting mode, general queries are sent on all downstream interfaces with this interval, only if the switch is the Querier. The no form of this command sets the MLDS query interval to default value.
✎	The configuration can be done only for the VLANs that are activated in the switch.
Syntax	ipv6 mld snooping query-interval <(60 - 600) seconds>

	no ipv6 mld snooping query-interval
Mode	Config-VLAN Mode

ipv6 mld snooping mrouter

Command Objective	This command configures statically the router ports for a VLAN. The no form of this command deletes the statically configured router ports for a VLAN. By default, the router port list is set to none.
✎	The configuration can be done only for the VLANs that are activated in the switch. The specified interface can be set as router ports for the VLAN, only if the interfaces are configured as member ports for that VLAN.
Syntax	ipv6 mld snooping mrouter <interface-type> <0/a-b, 0/c, ...> no ipv6 mld snooping mrouter <interface-type> <0/a-b, 0/c, ...>
Parameter Description	● <interface-type> - Clears all port-level spanning-tree statistics information for the specified type of interface. The interface can be: ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. ■ port-channel – Logical interface that represents an aggregator

	which contains several ports aggregated together. ● <0/a-b, 0/c, ...> - Sets the list of multicast router ports for the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash. Port-channel ID is provided, for interface type port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1, 0/3 or 1, 3. >
Mode	Config-VLAN Mode

ipv6 mld snooping blocked-router

Command Objective	This command configures a static router-port as blocked router port. The no form of the command resets the blocked router ports to normal router port.
✎	The ports to be configured as blocked router ports, must not be configured as static router ports.
Syntax	ipv6 mld snooping blocked-router <interface-type> <0/a-b, 0/c, ...> no ipv6 mld snooping blocked-router <interface-type> <0/a-b, 0/c, ...>

Parameter Description	● <interface-type> - Clears all port-level spanning-tree statistics information for the specified type of interface. The interface can be: ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. ■ port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. > ● <0/a-b, 0/c, ...> - Sets the list of multicast router ports for the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash. Port-channel ID is provided, for interface type port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1, 0/3 or 1, 3. >
Mode	Config-VLAN Mode

show ipv6 mld snooping mrouter

Command Objective	This command displays the router ports for all the VLANs or a specific VLAN. Interface, ports (type of ports) and switch details are displayed.
Syntax	show ipv6 mld snooping mrouter [Vlan <vlan-id >] [detail] [switch <switch_name>]
Parameter	● < vlan-id (1-4094)> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and

Description	4094 ● detail - Displays detailed information about the router ports ● switch <switch_name> - Displays the router ports for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature. >
Mode	Privileged EXEC Mode

show ipv6 mld snooping globals

Command Objective	This command displays the global MLD snooping information for all VLANs or a specific VLAN. Information such as MLD Snooping globally enabled, MLD Snooping operationally enabled, Transmit Query on Topology Change and so on.
Syntax	show ipv6 mld snooping globals [switch <switch_name>]
Parameter Description	● switch <switch_name> - Displays the router ports for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature. >
Mode	Privileged EXEC Mode

show ipv6 mld snooping

Command Objective	This command displays MLD snooping information for all VLANs or a specific VLAN. Information such as MLD Snooping enabled, MLD configured version is v2 and so on.
Syntax	show ipv6 mld snooping [Vlan <vlan-id >] [switch <switch_name>]
Parameter Description	● < vlan-id (1-4094)> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094 ● switch <switch_name> - Displays the router ports for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature. >
Mode	Privileged EXEC Mode

show ipv6 mld snooping groups

Command Objective	This command displays the MLDS group information for all VLANs or a specific VLAN or a specific VLAN and group address. Information displayed in the output are Snooping Group information, Vlan id, Group

	address, Filter mode and so on.
Syntax	show ipv6 mld snooping groups [Vlan <vlan-id > [Group <Address>]] [switch <string (32)>]
Parameter Description	● < vlan-id (1-4094)> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094 ● Group <Address> - Displays the Group Address of the VLAN ID ● switch <switch_name> - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature. >
Mode	Privileged EXEC Mode

show ipv6 mld snooping forwarding-database

Command Objective	This command displays multicast forwarding entries for all VLANs or a specific VLAN. The information displayed are VLAN, Source address, Group address and Ports.
Syntax	show ipv6 mld snooping forwarding-database [Vlan <vlan-id >] [switch <switch_name>]

Parameter **Description**	● < vlan-id (1-4094)> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094 ● switch <switch_name> - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature. >
Mode	Privileged EXEC Mode

show ipv6 mld snooping statistics

Command Objective	This command displays MLD snooping statistics for all VLANs or a specific VLAN. The information displayed are Snooping Statistics for Vlan 1, General queries received, Group specific queries received, Group and source specific queries received and so on.
Syntax	show ipv6 mld snooping statistics [Vlan <vlan-id >] [switch <string (32)>]
Parameter **Description**	● < vlan-id (1-4094)> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094 ● switch <switch_name> - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to

	multiple instance feature. >
Mode	Privileged EXEC Mode

Multicast Filtering

multicast-filtering

Command Objective	This command enable/disable multicast-filtering in the switch.
Syntax	multicast-filtering {enable | disable}
Parameter Description	● enable - Enables multicast-filtering. ● disable - Disables multicast-filtering. >
Mode	Global Configuration Mode

show multicast-filtering status

Command Objective	This command displays the multicast filtering status.
Syntax	show multicast-filtering status

Mode

Privileged EXEC Mode

Jumbo Frame

jumbo-frame

Command Objective

This command configures the maximum transmission unit frame size for all the frames transmitted and received on all the interfaces in a switch. The size of the jumbo frame size can be increased using this command. The value ranges between 1522 and 10240. This value defines the largest PDU that can be passed by the interface without any need for fragmentation. This value is shown to the higher interface sub-layer and should not include size of the encapsulation or header added by the interface. For Fast ethernet the value should not be greater than 1522.

Syntax

```
jumbo-frame <frame-size(1522-10240)>
```

Parameter Description

- <frame-size(1522-10240)> - jumbo frame size.

>

Mode

Global Configuration Mode

show jumbo-frame

Command Objective

This command displays the maximum transmission unit frame size for all the frames transmitted and received on all the interfaces in a switch.

Syntax

```
show jumbo-frame
```

Mode

Privileged EXEC Mode

SNMP

snmp trap link-status

Command Objective	This command enables/disable trap generation on the interface. The interface generated linkUp or linkDown trap. The linkUp trap denotes that the communication link is available and ready for traffic flow. The linkDown trap denotes that the communication link failed and is not ready for traffic flow.
Syntax	snmp trap link-status no snmp trap link-status
Mode	Interface Configuration Mode

enable snmpagent

Command Objective	This command enables SNMP agent which provides an interface between a SNMP manager and a switch. The agent processes SNMP packets received from the manager, frames the appropriate response packets, and sends them to the manager.
Syntax	enable snmpagent

Mode	Global Configuration Mode

disable snmpagent

Command Objective	This command disables SNMP agent.
Syntax	disable snmpagent
Mode	Global Configuration Mode

snmp community

Command Objective	This command enables SNMP agent which provides an interface between a SNMP manager and a switch. The agent processes SNMP packets received from the manager, frames the appropriate response packets, and sends them to the manager. The no form of the command disables the snmp agent.
Syntax	snmp community name <CommunityName> security <SecurityName> [context <name>] [{volatile | nonvolatile}] [transporttag <TransportTagIdentifier | none>]

	no snmp community name < CommunityName >
Parameter Description	● name<CommunityName> - Creates a community name which stores the community string. ● security<SecurityName> - Stores the security model of the corresponding Snmp community name. string specified by the corresponding instance of snmp community name ● context - Configures the name of the SNMP context. ● volatile | nonvolatile - Sets the required storage type for the entry. ⍰ volatile – Sets the storage type as temporary. Erases the configuration setting on restarting the system. ⍰ nonvolatile – Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system. > ● <TransportTagIdentifier> - Specifies a set of transport endpoints from which a command responder application can accept management request. >
Mode	Global Configuration Mode

snmp group

Command Objective

This command configures SNMP group details.

The no form of the command removes the SNMP group details.

Syntax

snmp group <GroupName> user <UserName> security-model {v1 | v2c | v3 } [{volatile | nonvolatile}]

no snmp group <GroupName> user <UserName> security-model {v1 | v2c | v3 }

Parameter Description

- <GroupName> - Creates a name for an SNMP group
- user<UserName> - Sets a user for the configured group.
- security-model - Sets the security model for SNMP

■ v1 - Sets the SNMP version as Version 1.

■ v2c - Sets the SNMP version as Version 2.

■ v3 - Sets the SNMP version as Version 3.

● volatile | nonvolatile - Sets the required storage type for the

> group entry.

>

 volatile – Sets the storage type as temporary. Erases the configuration setting on restarting the system.

>

	nonvolatile - Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system. >
Mode	Global Configuration Mode

snmp access

Command Objective	This command configures the SNMP group access details. To configure an SNMP access along with the group, a group must have already been created using the snmp group command. The no form of the command removes the SNMP group access details.
Syntax	snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}} [read <ReadView | none>] [write <WriteView | none> [notify <NotifyView | none>] [{volatile | nonvolatile}] [context <string(32)>] no snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}}
Parameter Description	● <GroupName> - Sets the name of the group for which access is to be provided. ● v1 | v2c | v3- Sets the SNMP version.

■ v1 – Sets the SNMP version as Version 1.

■ v2c – Sets the SNMP version as Version 2.

■ v3 – Sets the SNMP version as Version 3. It is the most secure model as it allows packet encryption with the priv key word.

◆ auth - Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication.

◆ noauth - Sets no-authentication.

◆ priv - Sets both authentication and privacy.

● read - Mentions the MIB view of the SNMP context to which read access is authorized by this entry.

● write - Mentions the MIB view of the SNMP context to which write access is authorized by this entry.

● notify - Mentions the MIB view of the SNMP context to which notification access is authorized by this entry.

● volatile | nonvolatile - Sets the required storage type for

> the group entry.

>

 volatile – Sets the storage type as temporary. Erases the configuration setting on restarting the system.

 nonvolatile - Sets the storage type as permanent. Saves the configuration to the system. The saved configuration is viewed on restarting the system.

● context<string(32)> - Configures the name of the SNMP context. The maximum length of the string is 32.

Mode	Global Configuration Mode

snmp engineid

Command Objective	This command configures the engine ID that is utilized as a unique identifier of a SNMPv3 engine. This engine ID is used to identify a source SNMPv3 entity and a destination SNMPv3 entity to coordinate the exchange of messages between the source and the destination. The no form of the command resets the engine ID to the default value.
Syntax	snmp engineid <EngineIdentifier> no snmp engineid
Mode	Global Configuration Mode

snmp view

Command Objective	This command configures the SNMP view.

The no form of the command removes the SNMP view.

Syntax

```
snmp view <ViewName> <OIDTree> [mask <OIDMask>] {included | excluded} [{volatile | nonvolatile}]

no snmp view <ViewName> <OIDTree>
```

Parameter Description

- <ViewName> - Specifies the view name for which the view details are to be configured. This is a string value with maximum size as 32.
- <OIDTree> - Specifies the sub tree value for the particular view.
- mask <OIDMask> - Specifies a mask value for the particular view.
- included - Allows access to the subtree
- excluded - Denies access to the subtree
- volatile - Sets the storage type as temporary. Erases the configuration setting on restarting the system.
- nonvolatile - Sets the storage type as permanent. Saves the configuration to the system. The saved configuration can be viewed on restarting the system.

Mode

Global Configuration Mode

snmp targetaddr

Command Objective

This command configures the SNMP target address.

The no form of the command removes the configured SNMP target address.

Syntax

```
snmp targetaddr <TargetAddressName> param <ParamName>
{<IPAddress> | <IP6Address>} [timeout <Seconds(1-1500)]
[retries <RetryCount(1-3)] [taglist <TagIdentifier(1-20)>]
[{volatile | nonvolatile}] [port <integer (1-65535)>]

no snmp targetaddr <TargetAddressName>
```

Parameter Description

- <TargetAddressName> - Configures a unique identifier of the Target.
- param<ParamName> - Configures the parameters when generating messages to be sent to transport address.
- IPAddress - Configures an IP target address to which the generated SNMP notifications are sent.
- IP6Address - Configures a IP6 target address to which the generated SNMP notifications are sent.
- timeout<Seconds(1-1500)> - Sets the time in which the SNMP agent waits for a response from the SNMP Manager before retransmitting the Inform Request Message. The value ranges between 1 and 1500 seconds.
- retries<RetryCount(1-3)> - Sets the maximum number of times the agent can retransmit the Inform Request Message. This

	value ranges between 1 and 3. ● taglist<TagIdentifier | none> - Sets the tag identifier that selects the target address for the SNMP. ● volatile - Sets the storage type as temporary. Erases the configuration setting on restarting the system. ● nonvolatile - Sets the storage type as permanent. Saves the configuration to the system. The saved configuration can be viewed on restarting the system. ● port <integer (1-65535)> - Configures a port number through which the generated SNMP notifications are sent to the target address. The value ranges between 1 and 65535. >
Mode	Global Configuration Mode

snmp targetparams

Command Objective	This command configures the SNMP target parameters. The no form of the command removes the SNMP target parameters.
Syntax	snmp targetparams <ParamName> user <UserName> security-model {v1 | v2c | v3 {auth | noauth | priv}} message-processing {v1 | v2c | v3} [{volatile | nonvolatile}] no snmp targetparams <ParamName>

Parameter Description

- <ParamName> - Sets a unique identifier of the parameter.

- User <UserName> - Sets a user for which the target parameter is to be done.

- security-model - Sets the security model

■ v1 – Sets the SNMP version as Version 1.

■ v2c – Sets the SNMP version as Version 2.

■ v3 – Sets the SNMP version as Version 3. It is the most secure model as it allows packet encryption with the priv key word

◆ auth - Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication

◆ noauth - Sets no-authentication

◆ priv - Specifies both authentication and privacy

- message-processing - Sets the message processing model

■ v1 – Sets the SNMP version as Version 1.

■ v2c – Sets the SNMP version as Version 2.

■ v3 – Sets the SNMP version as Version 3. It is the most secure model as it allows packet encryption with the priv key word.

- volatile - Sets the storage type as temporary. Erases the configuration setting on restarting the system.

- nonvolatile - Sets the storage type as permanent. Saves the configuration to the system. The saved configuration can be viewed on restarting the system.

>

Mode	Global Configuration Mode

snmp user

Command Objective	This command configures the SNMP user details. The no form of the command removes the SNMP user details.
Syntax	snmp user <UserName> [auth {md5 | sha} <passwd> [priv {{{DES | AES_CFB128} <passwd> } | None}]] [{volatile | nonvolatile}] no snmp user <UserName>
Parameter Description	● <UserName> - Configures a username which is the User- > based Security Model dependent security ID. ● auth - Sets an authentication Algorithm . Options are: ■ md5 - Sets the Message Digest 5 based authentication. ■ sha - Sets the Security Hash Algorithm based authentication. ● <Passwd> - Sets the authentication password that will be used for the configured authentication algorithm. ● priv - Sets the DES encryption and also the password to be used for the encryption key. Options are: DES – Configures the data encryption standard algorithm related configuration. AES_CFB128 – Configures Advanced Encryption Standard

(AES) algorithm for encryption.

- <Passwd> - Sets the authentication password that will be used for the configured authentication algorithm.
- None - Sets no encryption configurations.

- volatile - Sets the storage type as temporary. Erases the configuration setting on restarting the system.
- nonvolatile - Sets the storage type as permanent. Saves the configuration to the system. The saved configuration can be viewed on restarting the system.

Mode	Global Configuration Mode

snmp notify

Command Objective	This command configures the SNMP notification details. The no form of this command removes the SNMP notification details.
Syntax	snmp notify <NotifyName> tag <TagName> type {Trap | Inform} [{volatile | nonvolatile}] no snmp notify <NotifyName>
Parameter	● <NotifyName> - Configures a unique identifier associated

Description

with the entry.

- tag<TagName> - Sets a notification tag, which selects the entries in the Target Address Table.
- type - Sets the notification type. The list contains:
    - ■ Trap – Allows routers to send traps to SNMP managers. Trap is a one-way message from a network element such as a router, switch, or server to the network management system.
    - ■ Inform – Allows routers / switches to send inform requests to SNMP managers.
- volatile - Sets the storage type as temporary. Erases the configuration setting on restarting the system.
- nonvolatile - Sets the storage type as permanent. Saves the configuration to the system. The saved configuration can be viewed on restarting the system.

Mode Global Configuration Mode

snmp-server enable traps snmp authentication

Command Objective

This command enables generation of authentication traps from the snmp agent (for all snmpv1, snmpv2 and snmpv3)

	The no form of the command disables generation of authentication traps.
Syntax	snmp-server enable traps snmp authentication no snmp-server enable traps snmp authentication
Mode	Global Configuration Mode

snmp-server trap udp-port

Command Objective	This command configures the udp port over which agent sends the trap. The no form of the command configures the snmp agent to set trap on default udp port.
Syntax	snmp-server trap udp-port <port> no snmp-server trap udp-port
Mode	Global Configuration Mode

snmp-server trap proxy-udp-port

Command Objective	This command configures the udp port over which agent sends the trap to the proxy entity. The no form of the command configures the snmp agent to set trap on default udp port.
Syntax	snmp-server trap proxy-udp-port <port> no snmp-server trap proxy-udp-port
Mode	Global Configuration Mode

snmp agent port

Command Objective	This command configures the agent port on which agent listens. The port number value ranges between 1 and 65535.
Syntax	snmp agent port <port>
Mode	Global Configuration Mode

snmp tcp enable

Command Objective

This command enables sending snmp messages over tcp.

The no form of the command disables sending snmp messages over tcp.

Syntax

```
snmp tcp enable

no snmp tcp enable
```

Mode

Global Configuration Mode

snmp trap tcp enable

Command Objective

This command enables sending snmp trap messages over tcp.

The no form of the command disables sending snmp trap messages over tcp.

Syntax

```
snmp trap tcp enable
```

	no snmp trap tcp enable
Mode	Global Configuration Mode

snmp-server tcp-port

Command Objective	This command configures the tcp port over which agent sends the snmp message. This value ranges between 1 and 65535. The no form of the command configures the snmp agent to send snmp message on default tcp port.
Syntax	snmp-server tcp-port <port> no snmp-server tcp-port
Mode	Global Configuration Mode

snmp-server trap tcp-port

Command Objective	This command configures the tcp port over which agent sends the

	trap. This value ranges between 1 and 65535. The no form of the command configures the snmp agent to set trap on default tcp port.
Syntax	snmp-server trap tcp-port <port> no snmp-server trap tcp-port
Mode	Global Configuration Mode

snmp-server enable traps

Command Objective	This command enables generation of a particular trap. The no form of the command disables generation of a particular trap.

Syntax	snmp-server enable traps {[firewall-limit] [linkup] [linkdown] [sip-states] [sip-cfg-change] [coldstart] [poe-power] [dhcp-pool-limit] [dsx1-line] [auth-trap]}
	no snmp-server enable traps {[firewall-limit] [linkup] [linkdown] [sip-states] [sip-cfg-change] [coldstart] [poe-power] [dhcp-pool-limit] [dsx1-line] [auth-trap]}

Parameter Description	● firewall-limit - Generates a trap for all the firewall attack summary ● linkup - Generates a trap whenever there is a linkup ● linkdown - Generates a trap whenever there is a linkdown ● sip-states - Generates a trap for all the SIP states . ● sip-cfg-change - Generates a trap for all the SIP configuration ● coldstart - Generates a trap for all the Coldstart ● poe-power - Generates a trap whenever there is Power on Ethernet ● dhcp-pool-limit - Generates a trap for all the DHCP server pool limit trap ● dsx1-line - Generates a trap for all the DSX1 line trap ● auth-trap – Generates a trap for authentication failure trap >
Mode	Global Configuration Mode

snmpwalk mib

Command Objective	This command displays all the mib objects of the given table.

Syntax	snmpwalk mib {name | oid} <value> [count <integer(1-100)>] [short]
Parameter Description	● name <value> - Gets the next mib object name for the given mib object name. This is a string value with maximum size as 32. ● oid <value> - Gets the next mib object identifier for the given mib object identifier. ● count <integer(1-100)> - Sets the number of entries to be displayed in the mib object. This value ranges between 1 and 100. ● short - Displays the value of the mib object.
Mode	Global Configuration Mode

show snmp

Command Objective	This command displays the status information of SNMP communications.
Syntax	show snmp
Mode	Privileged EXEC Mode

show snmp community

Command Objective	This command displays the configured SNMP community details.
Syntax	show snmp community
Mode	Privileged EXEC Mode

show snmp group

Command Objective	This command displays the configured SNMP groups.
Syntax	show snmp group
Mode	Privileged EXEC Mode

show snmp group access

Command Objective	This command displays the configured SNMP group access

	details.
Syntax	show snmp group access
Mode	Privileged EXEC Mode

show snmp engineid

Command Objective	This command displays the Engine Identifier.
Syntax	show snmp engineid
Mode	Privileged EXEC Mode

show snmp viewtree

Command Objective	This command displays the configured SNMP Tree views.
Syntax	show snmp viewtree

Mode	Privileged EXEC Mode

show snmp targetaddr

Command Objective	This command displays the configured SNMP target Addresses.
Syntax	show snmp targetaddr
Mode	Privileged EXEC Mode

show snmp targetparam

Command Objective	This command displays the configured SNMP Target Address Params.
Syntax	show snmp targetparam
Mode	Privileged EXEC Mode

show snmp user

Command Objective	This command displays the configured SNMP users.
Syntax	show snmp user
Mode	Privileged EXEC Mode

show snmp notif

Command Objective	This command displays the configured SNMP Notification types.
Syntax	show snmp notif
Mode	Privileged EXEC Mode

show snmp inform statistics

Command Objective	This command displays the inform message statistics.
Syntax	show snmp inform statistics
Mode	Privileged EXEC Mode

show snmp-server traps

Command Objective	This command displays the set of traps that are currently enabled.
Syntax	show snmp-server traps
Mode	Privileged EXEC Mode

show snmp-server proxy-udp-port

Command Objective	This command displays the proxy udp port.

Syntax	show snmp-server proxy-udp-port
Mode	Privileged EXEC Mode

show snmp tcp

Command Objective	This command displays the configuration for snmp over tcp.
Syntax	show snmp tcp
Mode	Privileged EXEC Mode

show mib name

Command Objective	This command displays the name of the corresponding mib object identifier.
Syntax	show mib name <Object OID. eg 1.3.6.1.6>

Mode	Privileged EXEC Mode

DNS

ip name-server

Command Objective	This command configures default name server IP.
Syntax	ip name-server {ipv4 <ucast_addr> | ipv6 <ip6_addr>}
Parameter Description	● ipv4 <ucast_addr> - Sets the IP address for the domain name server in IPv4 address format. ● ipv6 <ip6_addr> - Sets the IP address for the domain name server in IPv6 address format. >
Mode	Global Configuration Mode

domain name-server

Command Objective	This command configures the IP address for the domain name server. The no form of the command disables the IP address configured for the domain name server.
Syntax	domain name-server ipv4 <ucast_addr>

	no domain name-server ipv4 <ucast_addr>
Parameter Description	● ipv4 <ucast_addr> - Sets the IP address for the domain name server in IPv4 address format. >
Mode	Global Configuration Mode

show ip dns name-server

Command Objective	This command displays the DNS name servers information.
Syntax	show ip dns name-server
Mode	Privilege EXEC Mode

IP

ip address

Command Objective	This command sets the IP address for an interface.
Syntax	ip address <ucast_addr> <ip_mask> no ip address <ucast_addr>
Parameter Description	● ucast_addr - Sets the IP address for an interface. If the network in which the switch is implemented contains a server such as DHCP server, dynamically allocating IP address, the configured IP address should not be within the range of the addresses that will be allocated by the server to the other switches. This precaution avoids creation of IP address conflicts between the switches. > ● ip_mask - Sets the subnet mask for the configured IP address. The configured subnet mask should be in the same subnet of the network in which the switch is placed. >
Mode	Interface Configuration Mode This command is applicable in VLAN Interface Mode / OOB Interface Mode.

ip address dhcp

Command Objective	This command sets the DHCP IP address for an interface.
Syntax	ip address dhcp no ip address
Parameter Description	● dhcp – Get IP by using DHCP protocol. >
Mode	Interface Configuration Mode This command is applicable in VLAN Interface Mode / OOB Interface Mode.

show ip source binding dhcp snooping

Command Objective	This command displays the dynamic IP binding updates through DHCP snooping.
Syntax	show ip source binding dhcp-snooping [interface

	<interface-type> <interface-id>] [vlan <vlan-id (1-4094)>] [switch <switch_name>]
Parameter Description	● <interface-type> - Clears all port-level spanning-tree statistics information for the specified type of interface. The interface can be: ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. >
Mode	Privileged EXEC Mode

ip dhcp snooping

Command Objective	This command globally enables the layer 2 DHCP snooping in the switch or enables the snooping in the specific VLAN. The DHCP snooping module will start the protocol operation when the snooping is enabled globally.
Syntax	ip dhcp snooping [vlan < vlan-id (1-4094)>] no ip dhcp snooping [vlan < vlan-id (1-4094)>]

Mode	Global Configuration mode

ip dhcp snooping verify mac-address

Command Objective	This command globally enables DHCP MAC verification in the switch.
Syntax	ip dhcp snooping verify mac-address no ip dhcp snooping verify mac-address
Mode	Global Configuration mode

ip dhcp snooping

Command Objective	This command enables layer 2 DHCP snooping in the VLAN.
Syntax	ip dhcp snooping no ip dhcp snooping

Mode	Config-VLAN mode

ip dhcp snooping trust

Command Objective	This command configures the port as a trusted port.
Syntax	ip dhcp snooping trust no ip dhcp snooping trust
Mode	Interface Configuration Mode This command is applicable in PORT/ PORT-CHANNEL Interface Mode

show ip dhcp snooping globals

Command Objective	This command displays the global configuration of DHCP snooping. The global status of layer 2 DHCP snooping and MAC verification are displayed.

Syntax	show ip dhcp snooping globals [switch <string (32)>]
Mode	Privileged EXEC Mode

show ip dhcp snooping

Command Objective	This command displays the DHCP snooping configuration and statistics of all VLANs in which the DHCP snooping feature is enabled.
Syntax	show ip dhcp snooping [vlan <vlan-id (1-4094)>] [switch <context name>]
Mode	Privileged EXEC Mode

show ip route

Command Objective	This command displays the IP routing table.
Syntax	show ip route [{ <ip_addr> [<ip_mask>] | connected | static | summary | details}]

Parameter Description	● <ip-address>- Displays the IP routing table for the specified destination IP Address. > ● <mask>- Displays the IP routing table for the specified prefix mask address. > ● connected- Displays the Directly Connected Network Routes. ● static- Displays the Static Routes in the table. ● summary- Displays the Summary of all routes. ● details-Displays the details of all routes. >
Mode	Privileged EXEC Mode

show ip arp

Command Objective	This command displays IP ARP table.
Syntax	show ip arp [{ Vlan <vlan_vfi_id> | <ucast_addr> | <ucast_mac> | summary | information | statistics }]
Parameter Description	● Vlan <vlan_vfi_id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094.

	> ● <ucast_addr> - Displays the IP Address of ARP Entry. ● <ucast_mac> - Displays the MAC Address of ARP Entry. ● summary - Displays IP ARP Table summary. ● information- Displays the ARP Configuration information regarding maximum retries and ARP cache timeout. ● statistics – Displays the ARP packet statistics. >
Mode	Privileged EXEC Mode

ip route

Command Objective	This command adds a static route. The Route defines the IP address or interface through which the destination can be reached. The no form of this command deletes a static route.
Syntax	ip route <ip_addr> <ip_mask> <ucast_addr> [<short (1-254)>] no ip route <ip_addr> <ip_mask>

Parameter Description	● <ip-address>- Configures the IP Address of ARP Entry. > ● <mask> - Configures the subnet mask for the IP address. This is a 32-bit number which is used to divide the IP address into network address and host address. > ● <next-hop> - Defines the IP address or IP alias of the next hop that can be used to reach that network. >
Mode	Global Configuration Mode

arp timeout

Command Objective	This command sets the ARP (Address Resolution Protocol) cache timeout. The arp timeout defines the time period an arp entry remains in the cache. When a new timeout value is assigned, it only affects the new arp entries. All the older entries retain their old timeout values. The timeout values can be assigned to dynamic arp entries only. All static arp entries remain unaltered by the timeout value. This value ranges between 30 and 86400 seconds. The no form of this command sets the ARP cache timeout to its default value.

Syntax	arp timeout <integer (30-86400)> no arp timeout
Mode	Global Configuration Mode

arp

Command Objective	This command adds a static entry in the ARP cache.

Syntax	arp <ucast_addr> <ucast_mac> { Vlan <vlan_vfi_id> }
	no arp {<ucast_addr>}

Parameter Description	● <ucast_addr>- Configures the IP Address of ARP Entry. > ● <ucast_mac> - The MAC address corresponding to the IP address above. > ● <vlan_vfi_id>- VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094. >

Mode	Global Configuration Mode

ip arp max-retries

Command Objective	This command sets the maximum number of ARP request retries. The maximum number of ARP requests that the switch generates before deleting an un-resolved ARP entry is defined. The no form of this command sets the maximum number of ARP request retries to its default value.
Syntax	ip arp max-retries <short (2-10)> no ip arp max-retries
Parameter Description	● <short (2-10)> - Configures the maximum number of ARP request entries. The value ranges between 2 and 10. >
Mode	Global Configuration Mode

DHCP Server

show dhcp server

Command Objective	This command displays the DHCP servers' IP addresses. These addresses denotes the PCs or switches that can act as a DHCP server.
Syntax	show dhcp server
Mode	Privileged EXEC Mode

show dhcp-relay

Command Objective	This command displays DHCP relay agent configuration.
Syntax	show dhcp-relay
Mode	Privileged EXEC Mode

service dhcp-relay

Command Objective	This command enables the DHCP relay agent in the switch. DHCP relay agent relays DHCP messages between DHCP client and DHCP server located in different subnets. The no form of the command disables the DHCP relay agent.
Syntax	service dhcp-relay no service dhcp-relay
Mode	Global Configuration Mode

ip dhcp server

Command Objective	This command adds the configured IP address to the IP address list created for the DHCP server. The switches or systems having these IP addresses represent the DHCP servers to which the DHCP relay agent can forward the packets that are received from DHCP clients. The DHCP relay agent broadcasts the received packets to entire network except the network from which the packets are received, if the DHCP server list is empty (that is IP address is configured as 0.0.0.0).

	The no form of the command deletes the mentioned IP address from the IP address list.
Syntax	ip dhcp server <ip address> no ip dhcp server <ip address>
Mode	Global Configuration Mode

ip dhcp client fast-access

Command Objective	This command enables DHCP fast access Mode. If fast access mode is enabled, time to wait between discovery messages ie. discovery timeout and time to wait after four unsuccessful discovery will be user configurable and the default value for discovery timeout is 5 seconds and for the null state timeout is 1 second.
Syntax	ip dhcp client fast-access
Mode	Privileged EXEC Mode

IPv6

ipv6 address - prefix and prefix length

Command Objective

This command configures IPv6 address on the interface.

Syntax

ipv6 address { <prefix> "/" <prefix Len> | <string> } [{unicast| link-local }]

no ipv6 address <prefix> <prefix Len> [unicast]

Parameter Description

- <prefix>-Configures the IPv6 prefix for the interface.

>

- <prefix Len> - Configures the number of high-order bits in the IPv6 address. These bits are common among all hosts within a network. This value ranges between 0 and 128.

>

- unicast- Configures the address type of the prefix as Unicast.

- link-local - Configures the address type of the prefix as Link-local.

>

Mode

Interface Configuration Mode

This command is applicable in VLAN Interface Mode.

ipv6 address dhcp

Command Objective	This command enables the DHCPv6 client functionality over the interface and requests for configuration information from the client. The no form of the command disables the DHCPv6 client functionality over the interface.
Syntax	ipv6 address dhcp no ipv6 address dhcp
Mode	Interface Configuration Mode

ipv6 unicast-routing

Command Objective	This command enables unicast routing which is used for one to one communication across the ipv6 internet. An IPv6 unicast address is an identifier for a single interface, on a single node. A packet that is sent to a unicast address is delivered to the interface

	identified by that address. The no form of the command disables unicast routing.
Syntax	ipv6 unicast-routing no ipv6 unicast-routing
Mode	Global Configuration Mode / Interface Configuration Mode

ipv6 route

Command Objective	This command adds a static route. The Route defines the IPv6 address or interface through which the destination can be reached. The no form of this command deletes a static route.
Syntax	ipv6 route <prefix> <prefix len> ([<NextHop>] {vlan <vlan-id>})

	no ipv6 route <prefix> <prefix len> [vlan <vlan-id>]
Mode	Global Configuration Mode

ipv6 neighbor

Command Objective	This command configures a static entry in the IPv6 neighbor cache table. The no form of the command removes the static entry from the IPv6 neighbor cache table.

Syntax	ipv6 neighbor <prefix> {vlan <vlan-id> <MAC ADDRESS (xx:xx:xx:xx:xx:xx)>}
	no ipv6 neighbor <prefix> {vlan <vlan-id> <MAC ADDRESS xx:xx:xx:xx:xx:xx>}

Mode	Global Configuration Mode

clear ipv6 neighbors

Command Objective	This command removes all the entries in the IPv6 neighbor table.
Syntax	clear ipv6 neighbors
Mode	Global Configuration Mode

clear ipv6 traffic

Command Objective	This command removes all the entries in the IPv6 traffic table.
Syntax	clear ipv6 traffic
Mode	Global Configuration Mode

clear ipv6 route

Command Objective	This command removes all the entries in IPv6 route table

Syntax	clear ipv6 route
Mode	Global Configuration Mode

ipv6 enable

Command Objective	This command enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address. The no form of the command disables IPv6 processing on the interface.
Syntax	ipv6 enable no ipv6 enable
Mode	Interface Configuration Mode

ipv6 address - prefix and prefix length

Command Objective	This command configures IPv6 address on the interface. The no form of the command disables IPv6 address on the interface.
Syntax	ipv6 address <prefix> <prefix Len> [unicast] no ipv6 address <prefix> <prefix Len> [unicast]
Parameter Description	● <prefix> - Configures the IPv6 prefix for the interface. > ● <prefix Len> - Configures the number of high-order bits in the IPv6 address. These bits are common among all hosts within a network. This value ranges between 0 and 128. > ● unicast- Configures the address type of the prefix as Unicast. >
Mode	Interface Configuration Mode

ipv6 address - link local

Command Objective	This command configures the IPv6 link-local address on the interface. The link-local address is an IP address that is intended only for communications within the segment of a local network (a link) or a point-to-point connection.
Syntax	ipv6 address <prefix> link-local
Parameter Description	● <prefix> - Configures the IPv6 prefix for the interface. >
Mode	Interface Configuration Mode

show ipv6 interface

Command Objective	This command displays the IPv6 interfaces.
Syntax	show ipv6 interface [{vlan <vlan-id> [prefix]}]
Parameter Description	● <vlan –id>- VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094. >

Mode	Privileged EXEC Mode

show ipv6 route

Command Objective	This command displays the IPv6 Routes.
Syntax	show ipv6 route
Mode	Privileged EXEC Mode

show ipv6 route - summary

Command Objective	This command displays the summary of IPv6 Routes.
Syntax	show ipv6 route summary
Mode	Privileged EXEC Mode

show ipv6 neighbors

Command Objective	This command displays the IPv6 Neighbor Cache Entries.
Syntax	show ipv6 neighbors
Mode	Privileged EXEC Mode

ping ipv6

Command Objective	This command sends IPv6 echo messages along with the total number of packets to the destination.
Syntax	ping ipv6 <prefix%interface> [repeat <count>] [size <value>] [source {vlan <vlan-id> <source_prefix>}] [timeout <value (1-100)>]
Parameter Description	● <prefix%interface>- Configures the IPv6 Destination Prefix. ● repeat<count>- Configures the number of ping messages. The range varies between 0 and 10. ● size<value> - Configures the size of the data portion of the Ping packet in the message. ● source - Configures the Source Interface of the ping message.

	● vlan <vlan-id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094. ● <source_prefix>- Configures source prefix of the ping message. ● timeout <value (1-100)>- Configures the time in seconds after which this entity times out waiting for a particular ping response. The value ranges between 1 to 100. >
Mode	Privileged EXEC Mode

VLAN

vlan

Command Objective	This command creates a VLAN ID and enters into the config-VLAN mode in which VLAN specific configurations are done. This command directly enters into the config-VLAN mode for the specified VLAN ID, if the VLAN is already created.
Syntax	vlan <vlan-id> no vlan <vlan-id>
Parameter Description	● <vlan –id>- This is a unique value that represents the specific VLAN. This value ranges between 1 and 4094.
Mode	Global Configuration Mode/ Switch Configuration Mode

ports

Command Objective	This command statically configures a VLAN entry with the required member ports, untagged ports and/or forbidden ports, and activates the VLAN. The VLAN can also be activated using the vlan active command.
Syntax	ports [add] <interface-type> <0/a-b,0/c,...> [<interface-type>

	<0/a-b,0/c,...>] [untagged ([<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>][all])] [forbidden ([<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>])] ports [add] forbidden ([<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>]) no ports [<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>] [all] [untagged ([<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>] [all])] [forbidden ([<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>] [all])]
Parameter Description	● add - Appends the new configured ports to the existing member port list of the vlan. ● <interface-type> <0/a-b,0/c,...>- Configures the ports that should be set as a member of the VLAN. ● port-channel<a,b,c,d> - Sets the list of port channel interfaces or a specific port channel identifier. Use comma as a separator without space while configuring list of interfaces. Example: 1,3. ● all- Deletes all configured member ports for the VLAN and sets the member ports as none. This option is available only in the no form of the command. ● untagged<interface-type> <0/a-b,0/c,...>- Configures the

	ports that should be used for the VLAN to transmit egress packets as untagged packets. ● forbidden<interface-type> <0/a-b,0/c,...>- Configures the ports that should never receive packets from the VLAN. ● name<vlan-name>- Configures the unique name of the VLAN. This name is used to identify the VLAN and is an administratively assigned string with the maximum size as 32. >
Mode	Config-VLAN Mode >

ports name

Command Objective	This command configures Vlan name.
Syntax	ports name [<vlan-name>]
Mode	Config-VLAN Mode

gvrp advertisement

Command Objective	This command sets Enables or Disables gvrp advertisement on

	this vlan.
Syntax	gvrp advertisement {enable | disable}
Mode	Config-VLAN Mode

switchport pvid

Command Objective	This command configures the PVID on the specified port. The PVID represents the VLAN ID that is to be assigned to untagged frames or priority-tagged or C-VLAN frames received on the port. The PVID is used for port based VLAN type membership classification. This value ranges between 1 and 65535.
Syntax	switchport pvid <vlan-id/vfi_id> no switchport pvid
Parameter Description	● pvid<vlan-id(1-4094)>- Configures the PVID for the provider edge port for the specified VLAN ID. This is a unique value that represents the specific VLAN. This value ranges between 1 and 4094. >

Mode	Interface Configuration mode (Physical / Port channel)

switchport acceptable-frame-type

Command Objective	This command configures the type of VLAN dependent BPDU frames such as GMRP BPDU, that the port should accept during the VLAN membership configuration. The no form of the command resets the acceptable frame type for the port to its default value. This configuration does not affect VLAN independent BPDU frames such as GVRP BPDU and STP BPDU. It affects only the VLAN dependent BPDU frames.
Syntax	switchport acceptable-frame-type {all | tagged | untaggedAndPrioritytagged }
Parameter Description	● all- Configures the acceptable frame type as all. All tagged, untagged and priority tagged frames received on the port are accepted and subjected to ingress filtering. ● tagged- Configures the acceptable frame type as tagged. ● untaggedAndPrioritytagged- Configures the acceptable frame

type as untagged and priority tagged. Only the untagged or priority tagged frames received on the port are accepted and subjected to ingress filtering. The tagged frames received on the port are rejected.

Mode	Interface Configuration mode (Physical / Port channel)

switchport ingress-filter

Command Objective	This command enables ingress filtering feature on the port. The ingress filtering is applied for the incoming frames received on the port. Only the incoming frames of the VLANs that have this port in its member list are accepted. This configuration does not affect VLAN independent BPDU frames such as GVRP BPDU and STP BPDU. It affects only the VLAN dependent BPDU frames GMRP BPDU. The no form of the command disables ingress filtering feature on the port. All incoming frames received on the port are accepted.
Syntax	switchport ingress-filter no switchport ingress-filter

Mode	Interface Configuration mode (Physical / Port channel)

show forward-all

Command Objective	This command displays all entries in the VLAN forward all table. These entries contain forward all details of all active VLANs in the switch. The details have VLAN ID and information regarding forward all ports, forward all static ports, and forward all forbidden ports assigned to the VLAN.
Syntax	show forward-all [switch <context_name>]
Mode	Privileged EXEC Mode

show vlan

Command Objective	This command displays VLAN entry related information of all active VLANs and VLANs (that are not active) for which the port details are configured. The information contains the member ports, untagged ports,

	forbidden ports, VLAN name and the status of that VLAN entry.
Syntax	show vlan [brief | id <vlan-range> | summary] [switch <context_name>]
Parameter Description	● brief - Displays the VLAN entry related information of all active VLANs and VLANs (that are not active) for which the port details are configured. > ● id <vlan-range>- Displays the VLAN entry related information for specified VLANs alone. This value denotes the VLAN ID range for which the information needs to be displayed. This value is a string whose maximum size is 9. For example, the value is provided as 4000-4010 to display the information for VLANs IDs from 4000 to 4010. The information is displayed only for the active VLANs and VLANs (that are not active) for which the port details are configured. > ● summary- Displays only the total number of VLANs existing in the switch. This includes only the active VLANs and VLANs (that are not active) for which the port details are configured. The VLAN entry related information is not displayed. > ● switch <context_name>- Displays the VLAN entry related information or total number of existing VLANs, for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode	Privileged EXEC Mode >

show vlan device info

Command Objective	This command displays the VLAN global information that is applicable to all VLANs created in the switch / all contexts. The information contains VLAN status, VLAN oper status, GVRP status, GMRP status, GVRP oper status, GMRP oper status, MAC-VLAN status, subnet-VLAN status, protocol-VLAN status, bridge mode of the switch, VLAN base bridge mode, VLAN traffic class status, VLAN learning mode, VLAN version number, maximum VLAN ID supported, maximum number of VLANs supported and VLAN unicast MAC learning limit.
Syntax	show vlan device info
Mode	Privileged EXEC Mode

show vlan static

Command Objective	This command displays static VLAN global status for the specified VLAN range.
Syntax	show vlan static [id <vlan-range>]
Parameter Description	- vlan <vlan-range>- Displays the unicast / broadcast statistics details for specified VLANs alone. This value denotes the VLAN ID range for which the details need to be displayed. This value is a string whose maximum size is 9. For example, the value is provided as 4000-4010 to display the details for VLAN IDs from 4000 to 4010. The details are displayed only for the VLANs that are activated and VLANs (that are not active) for which the port details are configured.
Mode	Privileged EXEC Mode

show vlan device capabilities

Command Objective	This command displays only the list of VLAN features such as traffic class feature, supported in the switch / all contexts.
Syntax	show vlan device capabilities

Mode Privileged EXEC Mode

show vlan port config

Command Objective This command displays the VLAN related port specific information for all interfaces available in the switch / all contexts. The information contains PVID, acceptable frame type, port mode, filtering utility criteria, default priority value and status of ingress filtering feature, GVRP module, GMRP module, restricted VLAN registration feature, restricted group registration feature, MAC-based VLAN membership, subnet based VLAN membership, protocol-VLAN based membership and port protected feature.

Syntax

```
show vlan port config [{port < interface-type > <ifnum> | switch <string(32)>}]
```

Parameter Description

● <interface-type> - Displays the VLAN related port specific information for the specified interface.

■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.

● switch <context_name> - Displays the VLAN global information that is applicable to all VLANs, for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode	Privileged EXEC Mode

show vlan statistics

Command Objective	This command displays the unicast / broadcast statistics details of all active VLANs and VLANs (that are not active) for which the port details are configured. The statistics details include VLAN ID, number of unicast packets received in the VLAN, number of multicast / broadcast packets received in the VLAN, number of unknown unicast packets flooded in the VLAN, number of known unicast packets forwarded in the VLAN, and number of known broadcast packets forwarded in the VLAN.
Syntax	show vlan statistics [vlan <vlan-range>] [switch <string(32)>]
Parameter Description	● vlan <vlan-range>- Displays the unicast / broadcast statistics details for specified VLANs alone. This value denotes the VLAN ID range for which the details need to be displayed. This value is a string whose maximum size is 9. For example, the value is provided as 4000-4010 to display the details for VLAN IDs from 4000 to 4010. The details are displayed only for the VLANs that are activated and VLANs (that are not active) for which the port

details are configured.

- switch <context_name> - Displays the VLAN global information that is applicable to all VLANs, for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.

Mode	Privileged EXEC Mode

Voice-VLAN

voice vlan state

Command Objective	This command Enables / Disables voice vlan in the switch.
Syntax	voice vlan state [{oui-enabled | disabled | auto}]
Parameter Description	● oui-enable – Enable voice vlan with OUI. ● disabled – Disable voice vlan. ● auto – Enable voice vlan with LLDP-MED. >
Mode	Global Configuration Mode

voice vlan id

Command Objective	This command specifies the voice VLAN.
Syntax	voice vlan id <integer(1-4094)>
Parameter Description	● <integer(1-4094)> – Vlan id.

Mode	Global Configuration Mode

voice vlan aging-time

Command Objective	This command specifies the voice VLAN aging timeout interval in minutes.
Syntax	voice vlan aging-time <integer(30-65535)>
Parameter Description	● <integer(30-65535)> – Timeout in minutes.
Mode	Global Configuration Mode

voice vlan cos

Command Objective	This command specifies the OUI Voice VLAN Class of Service (CoS).
Syntax	voice vlan cos <integer(0-7)> [remark]

Parameter Description	● <integer(0-7)> – cos. ● [remark] – Specifies that the L2 user priority is remarked with the CoS value. >
Mode	Global Configuration Mode

voice vlan vpt

Command Objective	This command specifies the LLDP-MED vlan priority tag.
Syntax	voice vlan vpt <integer(0-7)>
Parameter Description	● <integer(0-7)> – vpt.
Mode	Global Configuration Mode

voice vlan dscp

Command Objective	This command specifies the LLDP-MED dscp.

Syntax	voice vlan dscp <integer(0-63)>
Parameter Description	● <integer(0-63)> – dscp.
Mode	Global Configuration Mode

voice vlan oui-table

Command Objective	This command specifies the voice vlan OUI table.
Syntax	voice vlan oui-table {add <aa:aa:aa> [text] | remove <aa:aa:aa> }
Parameter Description	● add <aa:aa:aa> – Add voice device mac address prefix to OUI table. ● [text] - Voice device prefix description. ● remove <aa:aa:aa> - Remove voice device mac address prefix from OUI table. >
Mode	Global Configuration Mode

voice vlan enable

Command Objective	This command specifies the OUI voice vlan enable/disable on interfaces.
Syntax	voice vlan enable no voice vlan enable
Mode	Interface Configuration Mode

voice vlan cos mode

Command Objective	This command specifies the OUI voice vlan cos mode on interfaces.
Syntax	voice vlan cos mode {src | all }
Parameter Description	● src –QoS attributes are applied to packets with OUIs in the source MAC address. ● all - QoS attributes are applied to packets that are classified to the Voice VLAN.

>

Mode	Interface Configuration Mode

show voice vlan

Command Objective	Show voice vlan state.
Syntax	show voice vlan [oui-table]
Parameter **Description**	● [oui-table] –Specifies OUI table.
Mode	Privilege EXEC Mode

GVRP

set gvrp

Command Objective

This command enables/disables GVRP in the switch.

Syntax

```
set gvrp {enable | disable}
```

Parameter Description

- enable - Enables GVRP in the switch.
- disable - Disables GVRP in the switch.

Mode

Global Configuration Mode

set port gvrp

Command Objective

This command enables/disables GVRP on the port.

Syntax

```
set port gvrp <interface-type> <interface-id> { enable | disable }
```

Parameter Description

- <interface-type> - Configures the specified type of interface. The interface can be:

  ⍰ gigabitethernet - A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.

  ⍰ port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.

- <interface-id> – Displays the IP interface configuration for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1.

  - enable - Enables GVRP on the interface.
  - disable - Disables GVRP on the interface.

Mode

Global Configuration Mode

set garp timer

Command Objective

This command sets GARP timers on the port.

Syntax

```
set garp timer {join | leave | leaveall} <integer>
```

Parameter Description

- join - Interval (in milliseconds) between opportunities to transmit GARP PDUs.
- leave - Time period (in milliseconds) until which the registrar state machine waits in the leave state before entering the empty state.
- leaveall - Frequency (in milliseconds) at which the leaveall state machine generates a leaveall message in a GARP PDU.
- <integer> - Time value(in milliseconds).

Mode

Interface Configuration Mode

vlan restricted

Command Objective

This command enables/disables restricted VLAN registration on the port.

Syntax

```
vlan restricted {enable | disable}
```

Parameter Description

- enable - Enables the restricted VLAN registration.
- disable - Disables the restricted VLAN registration.

Mode

Interface Configuration Mode

show garp timer

Command Objective

This command displays GARP timer information on the interfaces.

Syntax

show garp timer [{ port <interface-type> <interface-id> | switch <context_name>}]

Parameter Description

- <interface-type> - Configures the specified type of interface. The interface can be:

   gigabitethernet - A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.

   port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.

- <interface-id> – Displays the IP interface configuration for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1.

- switch<context_name> - Context name.

Mode

Privileged EXEC Mode

show gvrp statistics

Command Objective

This command displays GVRP statistics on the interfaces.

Syntax

show gvrp statistics [{ port <interface-type> <interface-id> }]

Parameter Description

- <interface-type> - Configures the specified type of interface. The interface can be:
  - gigabitethernet - A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.
  - port-channel - Logical interface that represents an aggregator which contains several ports aggregated together.
- <interface-id> – Displays the IP interface configuration for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1.

Mode

Privileged EXEC Mode

PNAC

dot1x system-auth-control

Command Objective	This command enables dot1x in the switch. The dot1x is an authentication mechanism. It acts as mediator between the authentication server and the supplicant (client). If the client accesses the protected resources, it contacts the authenticator with EAPOL frames.
Syntax	dot1x system-auth-control no dot1x system-auth-control
Mode	Global Configuration Mode

shutdown dot1x

Command Objective	This command shuts down dot1x feature. By shutting down the dot1x feature, the supplicant-authenticator-authentication server architecture is dissolved. The data transport and authentication are directly governed by the authentication server/server. When shutdown, all resources acquired by dot1x module are released to the system.

Syntax	shutdown dot1x no shutdown dot1x
Mode	Global Configuration Mode

dot1x clear statistics

Command Objective	This command clears dot1x counters for all the ports on the switch.
Syntax	dot1x clear statistics {interface <iftype> <ifnum> | all}
Parameter Description	● interface - Displays all static multicast MAC address entries for the specified interface. ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. >
Mode	Global Configuration Mode

dot1x guest-vlan

Command Objective	This command configures Dot1x Guest VLAN ID.
Syntax	dot1x guest-vlan <short (1-4094)> no dot1x guest-vlan
Parameter Description	● <vlan –id>- This is a unique value that represents the specific VLAN. This value ranges between 1 and 4094. >
Mode	Global Configuration Mode

dot1x default

Command Objective	This command configures dot1x with default values for this port. The previous configurations on this port are reset to the default values. These details are not displayed but are the basic settings for a port.
Syntax	dot1x default
Mode	Interface Configuration Mode

dot1x max-req

Command Objective	This command sets the maximum number of EAP (Extensible Authentication Protocol) retries to the client by the authenticator before restarting authentication process. The count value ranges between 1 and 10.
Syntax	dot1x max-req <count(1-10)> no dot1x max-req
Mode	Interface Configuration Mode

dot1x max-start

Command Objective	This command sets the maximum number of EAPOL retries to the authenticator. The value range is 1 to 65535.
Syntax	dot1x max-start <count(1-65535)> no dot1x max-start

Mode	Interface Configuration Mode

dot1x reauthentication

Command Objective	This command enables periodic re-authentication from authenticator to client. The periodic re-authentication is requested to ensure if the same supplicant is accessing the protected resources. The amount of time between periodic re-authentication attempts can be configured manually.
Syntax	dot1x reauthentication no dot1x reauthentication
Mode	Interface Configuration Mode

dot1x timeout

Command Objective	This command sets the dot1x timers. The timer module manages timers, creates memory pool for timers, creates timer list, and starts and stops timer. It provides handlers to respective expired timers.

Syntax	dot1x timeout {quiet-period <short(0-65535)> | {reauth-period | server-timeout | supp-timeout | tx-period | start-period | held-period | auth-period} <short(1-65535)>}
	no dot1x timeout {quiet-period | reauth-period | server-timeout | supp-timeout | tx-period | start-period | held-period | auth-period}

Parameter Description	● quiet-period <value (0-65535)>- Configures the quiet-period. Number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. ● reauth-period- Configures the reauth-period. Number of seconds between re-authentication attempts. ● server-timeout- Configures the number of seconds that the switch waits for the retransmission of packets to the authentication server. ● supp-timeout- Configures the number of seconds that the switch waits for the retransmission of packets to the client. ● tx-period- Configures the number of seconds that the switch waits for a response to an EAP-request/identity frame, from the client before retransmitting the request. ● start-period- Configures the number of seconds that the supplicant waits between successive retries to the authenticator. ● held-period - Configures the number of seconds that the supplicant waits before trying to acquire the authenticator. ● auth-period <value(1-65535)>- Configures the number of

	seconds that the supplicant waits before timing-out the authenticator >
Mode	Interface Configuration Mode

dot1x port-control

Command Objective	This command configures the authenticator port control parameter. The dot1x exercises port based authentication to increase the security of the network. The different Modes employed to the ports offer varied access levels. The 802.1x protocol is supported on both Layer 2 static-access ports and Layer 3 routed ports.
Syntax	dot1x port-control {auto|force-authorized|force-unauthorized} no dot1x port-control
Parameter Description	● auto- Configures the 802.1x authentication process in this port. Causes the port to begin the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. The switch can uniquely identify each

	client attempting to access the network by the client's MAC address. > ● force-authorized- Configures the port to allow all the traffic through this port. Disables 802.1X authentication and causes the port to transit to the authorized state without requiring authentication exchange. The port transmits and receives normal traffic without 802.1X-based authentication of the client. ● force-unauthorized- Configures the port to block all the traffic through this port. Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface. >
Mode	Interface Configuration Mode

dot1x mab

Command Objective	This command
Syntax	dot1x mab {mab_mode | hybrid_mode | disable}

Parameter Description	● mab_mode- MAC Authentication Bypass Only. > ● hybrid_mode- Username/Password and MAC Authentication Bypass. > ● disable- Username/Password authentication. >
Mode	Interface Configuration Mode

dot1x guest-vlan enable

Command Objective	This command enables/disables guest-vlan feature.
Syntax	dot1x guest-vlan enable no dot1x guest-vlan enable
Mode	Interface Configuration Mode

show dot1x

Command Objective	This command displays dot1x information. The configured information can be viewed by running this show command. When there is any change in the configuration to ensure that the port is configured as desired, the show command is used.
Syntax	show dot1x [{ interface <interface-type> <interface-id> | statistics interface <interface-type> <interface-id> | supplicant-statistics interface <interface-type> <interface-id>|local-database | mac-info [address <aa.aa.aa.aa.aa.aa>] | mac-statistics [address <aa.aa.aa.aa.aa.aa>] | all }]
Parameter **Description**	● interface <interface-type> <interface-id>- Displays dot1x parameters for the switch or the specified interface. > ● statistics interface <interface-type> <interface-id> - Displays dot1x authenticator port statistics parameters for the switch or the specified interface. > ● supplicant-statistics interface<interface-type> <interface-id> - Displays dot1x supplicant statistics parameters for the switch or the specified interface. ● local-database- Displays dot1x authentication server database with username and password. ● mac-info [address <aa.aa.aa.aa.aa.aa>] - Displays dot1x information for all MAC session or the specified MAC address. ● mac-statistics [address <aa.aa.aa.aa.aa.aa>] - Displays dot1x

	MAC statistic for all MAC session or the specified MAC address. ● all - Displays dot1x status for all interfaces. >
Mode	Privileged EXEC Mode

show dot1x guest-vlan

Command Objective	Displays dot1x Guest Vlan information.
Syntax	show dot1x guest-vlan
Mode	Privileged EXEC Mode

show dot1x dynamic-vlan

Command Objective	This command displays dot1x dynamic VLAN assignment information.
Syntax	show dot1x dynamic-vlan

Mode	Privileged EXEC Mode

show dot1x authenticated host

Command Objective	This command displays dot1x authenticated host status.
Syntax	show dot1x authenticated host
Mode	Privileged EXEC Mode

dot1x re-authenticate

Command Objective	This command initiates re-authentication of all dot1x-enabled ports or the specified dot1x-enabled port. This initializes the state machines and sets up the environment for fresh authentication. Re-authentication is manually configured if periodic re-authentication is not enabled. Re-authentication is requested by the authentication server to the supplicant to furnish the identity without waiting for the configured number of seconds (re-authperiod). If no interface is specified, re-authentication is initiated on all dot1x ports.

Syntax	dot1x re-authenticate [interface <interface-type><interface-id>]
Parameter **Description**	● <interface type>- Configures the specified type of interface. ● <interface id>- Configures the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1. >
Mode	Privileged EXEC Mode

dot1x radius-vlan-assignment

Command Objective	This command enabled radius vlan assignment function on port.
Syntax	dot1x radius-vlan-assignment enable no dot1x radius-vlan-assignment
Mode	Interface Configuration Mode

Port Isolation

port-isolation

Command Objective

This command set the status of the traffic to be allowed in these configured egress ports when the ingress is this interface.

Syntax

port-isolation {enable|disable}

Parameter Description

- enabled - Enables the Port Isolation rule in this ingress interface.
- disabled - Disables the Port Isolation rule in this ingress interface.

Mode

Interface Configuration

show port-isolation status

Command Objective

This command displays the Port Isolation table.

Syntax

show port-isolation status

Mode

Privileged EXEC Mode

Radius Server

radius-server host

Command Objective

This command configures the RADIUS client with the parameters (host, timeout, key, retransmit).

Syntax

```
radius-server host {ipv4-address |ipv6-address | host-name}
[auth-port <integer(1-65535)>] [acct-port <integer(1-65535)>]
[timeout <1-120>] [retransmit <1-254>] [key <secret-key-string>]
[primary]
```

```
no radius-server host {ipv4-address |ipv6-address | host-name}
[primary]
```

Parameter Description

- ipv4-address- Configures the IPv4 address of the RADIUS server host.
- ipv6-address- Configures the IPv6 address of the RADIUS server host.
- host-name - Configures the DNS (Domain Name System) name of the RADIUS server host. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.
- auth-port <integer(1-65535)>- Configures a specific UDP (User Datagram Protocol) destination port on this RADIUS server to be used solely for the authentication requests. The value of the auth port ranges between 1 and 65535.

- acct-port <integer(1-65535)>- Configures a specific UDP destination port on this RADIUS to be solely used for accounting requests. The value of the auth port ranges between 1 and 65535.

- timeout <1-120> - Configures the time period in seconds for which a client waits for a response from the server before re-transmitting the request. The value of the time out in ranges between 1 to 120 in seconds.

- retransmit <1-254> - Configures the maximum number of attempts the client undertakes to contact the server. The value number of retransmit attempts ranges between 1 and 254.

- key <secret-key-string> - Configures the Per-server encryption key which specifies the authentication and encryption key for all RADIUS communications between the authenticator and the RADIUS server. The value of the maximum length of the secret key string is 46.

- primary - Sets the RADIUS server as the primary server. Only one server can be configured as the primary server, any existing primary server will be replaced, when the command is executed with this option.

>

Mode	Global Configuration Mode

show radius server

Command Objective	This command displays RADIUS server Host information which contains, Index, Server address, Shared secret, Radius Server status, Response Time, Maximum Retransmission, Authentication Port and Accounting Port.
Syntax	show radius server [{<ucast_addr> | <ip6_addr> | <string>}]
Parameter **Description**	● <ucast_addr>- Displays the related information of the specified unicast address of the RADIUS server host. > ● <ip6_addr>- Displays the related information of the specified IPv6 address of the RADIUS server host. > > ● <string>- Displays the name of the RADIUS server host. This maximum value of the string is of size 32. >
Mode	Privileged EXEC Mode

show radius statistics

Command Objective	This command displays RADIUS Server Statistics for the data transfer between server and the client from the time of initiation.

Syntax	show radius statistics
Mode	Privileged EXEC Mode

Dos

security-suite

Command Objective	This command enables/disables DoS prevention.
Syntax	security-suite no security-suite
Mode	Global Configuration Mode

security-suite enable

Command Objective	This command enables/disables DoS prevention.
Syntax	security-suite enable no security-suite enable
Mode	Interface Configuration Mode

show security-suite

Command Objective	Displays Dos information.
Syntax	show security-suite
Mode	Privileged EXEC Mode

RMON

set rmon

Command Objective	This command is used to enable or disable the RMON feature.
Syntax	set rmon {enable | disable}
Parameter Description	● enable - Enables the RMON feature in the system. On enabling, the RMON starts monitoring the networks both local and remote and provides network fault diagnosis > ● disable - Disables the RMON feature in the system. On disabling, the RMON's network monitoring is called off. > >
Mode	Global Configuration Mode

rmon alarm

Command Objective	This command sets an alarm on a MIB object. The Alarm group periodically takes statistical samples from variables in the probe and compares them to thresholds that have been configured.

Syntax	rmon alarm <short (1-65535)> stats <short (1-65535)> {etherStatsDropEvents | etherStatsOctets | etherStatsPkts | etherStatsBroadcastPkts | etherStatsMulticastPkts | etherStatsCRCAlignErrors | etherStatsUndersizePkts | etherStatsOversizePkts | etherStatsFragments | etherStatsJabbers | etherStatsCollisions | etherStatsPkts64Octets | etherStatsPkts65to127Octets | etherStatsPkts128to255Octets | etherStatsPkts256to511Octets | etherStatsPkts512to1023Octets | etherStatsPkts1024to1518Octets } <short (1-65535)> { absolute | delta } rising-threshold <integer (0-2147483647)> [<integer (1-65535)>] falling-threshold <integer (0-2147483647)> [<integer (1-65535)>] [owner <string (127)>] no rmon alarm <number (1-65535)>
Parameter Description	● <alarm-number>/ <number (1-65535)>- Displays the value of the statistic during the last sampling period. This value remains available until the current sampling period is completed. For example, if the sample type is deltaValue, this value will be the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value will be the sampled value at the end of the period. This value is compared with the rising and falling thresholds. The value ranges between 1 and 65535. > ● <mib-object-id (255)>- Identifies the mib object. > ● <sample-interval-time (1-65535)>- Identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a

particular level for a MIB object in the device. This value ranges between 1 and 65535 seconds.

>

- absolute- Compares the value of the selected variable with the thresholds at the end of the sampling interval.

- delta- Subtracts the value of the selected variable at the last sample from the current value, and the difference is compared with the thresholds at the end of the sampling interval.

- rising-threshold <value (0-2147483647)>- Configures the rising threshold value. If the startup alarm is set as Rising alarm or RisingOrFalling alarm and if the configured threshold value is reached, then an alarm is raised. When the current sampled value is greater than or equal to the configured Rising threshold, and the value at the last sampling interval is less than this configured threshold, a single event will be generated. The value ranges between 0 and 2147483647.

- <rising-event-number (1-65535)>- Raises the index of the event, when the Rising threshold is reached. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. This value ranges between 1 and 65535.

- falling-threshold <value (0-2147483647)> - Configures the falling threshold value. If the startup alarm is set as Falling alarm or RisingOrFalling alarm and if the configured threshold value is reached, then an alarm is raised. When the current sampled value is

	lesser than or equal to the configured Falling threshold, and the value at the last sampling interval is greater than this threshold, a single event will be generated. This value ranges between 0 and 2147483647. > > ● <falling-event-number (1-65535)>- Raises the index of the event when the Falling threshold is reached. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. This value ranges between 1 and 65535. ● owner<ownername (127)>- Sets the entity that are configured this entry. >
Mode	Global Configuration Mode

rmon event

Command Objective	This command adds an event to the RMON event table. The added event is associated with an RMON event number.
Syntax	rmon event <number (1-65535)> [description <event-description (127)>] [log] [owner <ownername (127)>] [trap <community (127)>]

	no rmon event <number (1-65535)>
Parameter Description	● <number (1-65535)>- Sets the number of events to be added in the event table. This value ranges between 1 and 65535. > ● description<event-description (127)>- Provides a description for the event. This value is a string with a maximum length of 127. ● log- Creates an entry in the log table for each event. > ● owner<ownername (127)>- Displays the entity that are configured this entry. This value is a string with a maximum value of 127. ● trap<community (127)>- Generates a trap, The SNMP community string is to be passed for the specified trap. This value is a string with a maximum value of 127. >
Mode	Global Configuration Mode

rmon collection stats

Command Objective	This command enables RMON statistic collection on the interface/

	VLAN. The no form of the command disables RMON statistic collection on the interface/ VLAN.
Syntax	rmon collection stats <index (1-65535)> [owner <ownername (127)>] no rmon collection stats <index (1-65535)>
Parameter Description	● <index (1-65535)>- Identifies an entry in the statistics table.. This value ranges between 1 and 65535. > ● owner <ownername (127)>- Configures the name of the owner of the RMON group of statistics. >
Mode	Interface Configuration Mode / Config VLAN Mode

rmon collection history

Command Objective	This command enables history collection of interface/ VLAN statistics in the buckets for the specified time interval. The no form of the command disables the history collection on the

	interface/VLAN.
Syntax	rmon collection history <index (1-65535)> [buckets <bucket-number (1-65535)>] [interval <seconds (1-3600)>] [owner <ownername (127)>] no rmon collection history <index (1-65535)>
Parameter Description	● <index (1-65535)>- Identifies an entry in the history control table. Each such entry defines a set of samples at a particular interval for an interface on the device. This value ranges between 1 and 65535. > ● buckets<bucket-number (1-65535)> - Configures the number of buckets desired for the RMON collection history group of statistics. This is the requested number of discrete time intervals over which data is to be saved in the part of the media-specific table associated with this History Control Entry. The polling cycle is the bucket interval where the interface statistics details are stored. This value ranges between 1 and 65535. > ● interval<seconds (1-3600)>- Configures the time interval over which the data is sampled for each bucket. The value ranges between 1 and 3600. ● owner<ownername (127)>- Configures the name of the owner of the RMON group of statistics.

>

Mode	Interface Configuration Mode / Config VLAN Mode

show rmon

Command Objective	This command displays the RMON statistics, alarms, events, and history configured on the interface.
Syntax	show rmon [statistics [<stats-index (1-65535)>]] [alarms] [events] [history [history-index (1-65535)] [overview]]
Parameter Description	● statistics- Displays a collection of statistics for a particular Ethernet Interface. The probe for each monitored interface on this device measures the statistics. ● alarms- Displays the value of the statistic during the last sampling period. This value remains available until the current sampling period is completed. ● events- Generates events whenever an associated condition takes place in the device. The Conditions may be alarms. Alarms are generated when a sampled statistical variable value exceeds the defined threshold value. Alarm module calls events module. ● history- Displays the history of the configured RMON. ● overview- Displays only the overview of rmon history entries.

>

Mode	Privileged EXEC Mode

Log

show logging-file

Command Objective	This command displays the priority and file name of all the three files configured in the syslog file table.
Syntax	show logging-file
Mode	Privileged EXEC Mode

show logging-server

Command Objective	This command displays the information about the syslog logging server table.
Syntax	show logging-server
Mode	Privileged EXEC Mode

show logging

Command Objective	This command displays all the logging status and configuration information.
Syntax	show logging
Mode	Privileged EXEC Mode

logging

Command Objective	This command enables syslog server and configures the syslog related parameters The logging process controls the distribution of logging messages to the various destinations.

Syntax	logging { [facility {local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7}] | [severity { alerts | critical | debugging | emergencies | errors | informational | notification | warnings }]}
	logging {buffered [<short (1-200)>]}

Parameter Description	● facility - The facility that is indicated in the message. Can be one of the following values: local0, local1, local2, local3, local4,

local5, local 6, local7.

>

- severity - Message severity level. Messages with severity level equal to or high than the specified value are printed asynchronously. This can be configured using numerical value or using the available option. The options are:
  - 0 | emergencies - System is unusable
  - 1 | alerts - Immediate action needed.
  - 2 | critical - Critical conditions.
  - 3 | errors - Error conditions.
  - 4 | warnings - Warning conditions.
  - 5 | notification - Normal but significant conditions.
  - 6 | informational - Informational messages.
  - 7 | debugging – Debugging messages.

>

- buffered - Limits Syslog messages displayed from an internal buffer. This size ranges between 1 and 200 entries.

>

Mode	Global Configuration Mode

logging-service

Command Objective	This command enables/disables syslog server.
Syntax	logging-service { enable | disable }
Parameter Description	● enable - Syslog enabled. ● disable - Syslog disabled. > >
Mode	Global Configuration Mode

clear logs

Command Objective	This command clears the system syslog buffers.
Syntax	clear logs
Mode	Global Configuration Mode

syslog filename-one

Command Objective	This command configures a first file to store the syslog messages locally. The maximum size of the file name is 32.
Syntax	syslog filename-one <string(32)>
Mode	Global Configuration Mode

logging-file

Command Objective	This command adds an entry which is flash_log in the file table.
Syntax	logging-file <short(0-191)> flash_log
Parameter Description	● <short(0-191)> - Sets the priority of syslog messages. 0-lowest priority, 191-highest priority
Mode	Global Configuration Mode

logging-server

Command Objective

This command configures a server table to log an entry in it. The no form of command deletes an entry from the server table.

Syntax

```
logging-server {facility {local0 | local1 | local2 | local3 | local4 |
local5 | local6 | local7}} {severity { emergencies | alerts | critical |
errors | warnings | notification | informational| debugging}} {ipv4
<ucast_addr> |ipv6 <ip6_addr> | <string>} [ port
<integer(0-65535)>]
```

```
no logging-server {facility {local0 | local1 | local2 | local3 |
local4 | local5 | local6 | local7}} {severity { emergencies | alerts
| critical | errors | warnings | notification | informational|
debugging}} {ipv4 <ucast_addr> |ipv6 <ip6_addr> | <string>
```

Parameter Description

- facility - The facility that is indicated in the message. Can be one of the following values: local0, local1, local2, local3, local4, local5, local 6, local7..

- severity - Message severity level. Messages with severity level equal to or high than the specified value are printed asynchronously. This can be configured using numerical value or using the available option. The options are:

  - 0 | emergencies - System is unusable
  - 1 | alerts - Immediate action needed.
  - 2 | critical - Critical conditions.

  - 3 | errors - Error conditions.
  - 4 | warnings - Warning conditions.
  - 5 | notification - Normal but significant conditions.
  - 6 | informational - Informational messages.
  - 7 | debugging – Debugging messages.
- ipv4 <ucast_addr> - Sets the server address type as internet protocol version 4.
- ipv6 <ip6_addr> - Sets the server address type as internet protocol version 6.
- <string> - Configures the host name for a server to log an entry.
- port<integer(0-65535)> - Sets the port number through which it sends the syslog message. The value ranges between 0 and 65535.

>

Mode	Global Configuration Mode

ACL

ip access-list extend

Command Objective

This command creates IP ACLs and enters the IP Access-list configuration mode.

The no form of the command deletes the IP access-list.

Syntax

ip access-list extended <string(31)>

no ip access-list extended <string(31)>

Parameter Description

- <string(31)> –Configures the extended access-list name.

>

Mode

Global Configuration Mode

permit- ip/ospf/pim/protocol type

Command Objective

This command allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched.

Syntax

permit { ip | ospf | pim | <protocol-type (1-255)> | IPinIP | egp | igp | hmp | rdp | ipv6 | ipv6:route | ipv6:frag | rsvp | ipv6:icmp | l2tp} { any | host <src-ip-address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-ip-address> <mask> } ace-priority <integer (1-2147483647)> [dscp <value (0-63)>]

Parameter Description

- ip| ospf|pim|<protocol-type (1-255)>| IPinIP | egp | igp | hmp | rdp | ipv6 | ipv6:route | ipv6:frag | rsvp | ipv6:icmp | l2tp - Type of protocol for the packet. It can also be a protocol number.
- any| host <src-ip-address>|<src-ip-address> <mask> - Source IP address can be
  - 'any' or
  - the dotted decimal address or
  - the IP Address of the network or the host that the packet is from and the network mask to use with the source address.
- any|host <dest-ip-address>|<dest-ip-address> <mask> - Destination IP address can be
  - 'any' or
  - the dotted decimal address or
  - the IP Address of the network or the host that the packet is destined for and the network mask to use with the destination address
- ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules.
- dscp <short (0-63)> - Differentiated services code point provides the quality of service control.

>

Mode

IPV4 ACL Extended Access List Configuration Mode

deny- ip/ospf/pim/protocol type

Command Objective

This command denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched.

Syntax

deny { ip | ospf | pim | <protocol-type (1-255)> | IPinIP | egp | igp | hmp | rdp | ipv6 | ipv6route | ipv6frag | rsvp | ipv6icmp | l2tp} { any | host <src-ip-address> | <src-ip-address> <mask> } { any | host <dest-ip-address> | <dest-ip-address> <mask> } ace-priority <integer (1-2147483647)> [dscp <value (0-63)>]

Parameter Description

● ip| ospf|pim|<protocol-type (1-255)>| IPinIP | egp | igp | hmp | rdp | ipv6 | ipv6route | ipv6frag | rsvp | ipv6icmp | l2tp - Type of protocol for the packet. It can also be a protocol number.

● any| host <src-ip-address>|<src-ip-address> <mask> - Source IP address can be

■ ‘any’ or

■ the dotted decimal address or

■ the IP Address of the network or the host that the packet is from and the network mask to use with the source address.

	● any|host <dest-ip-address>|<dest-ip-address> <mask> - Destination IP address can be ■ ‘any’ or ■ the dotted decimal address or ■ the IP Address of the network or the host that the packet is destined for and the network mask to use with the destination address ● ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. ● dscp <short (0-63)> - Differentiated services code point provides the quality of service control. >
Mode	IPV4 ACL Extended Access List Configuration Mode

permit tcp

Command Objective	This command specifies the TCP packets to be forwarded based on the associated parameters.
Syntax	permit tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> } [eq <port-number (1-65535)>] { any | host <dest-ip-address> | <dest-ip-address> <dest-mask> } [eq

	<port-number (1-65535)>] ace-priority <integer (1-2147483647)> [{ack | non_ack}] [{rst | non_rst}] [{psh | non_psh}] [{urg | non_urg}] [{syn | non_syn}] [{fin | non_fin}] [dscp <value (0-63)>]
Parameter Description	● tcp - Transport Control Protocol. ● any| host <src-ip-address>|<src-ip-address> <src-mask> - Source IP address can be ■ 'any' or ■ the dotted decimal address or ■ the IP Address of the network or the host that the packet is from and the network mask to use with the source address. ● eq <short (1-65535)> - Port Number. ● any|host <dest-ip-address>|<dest-ip-address> <dest-mask> - Destination IP address can be ■ 'any' or ■ the dotted decimal address or ■ the IP Address of the network or the host that the packet is destined for and the network mask to use with the destination address ● ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. ● ack | non_ack - TCP ACK bit to be checked against the packet. ● rst | non_rst - TCP RST bit to be checked against the packet.

- psh | non_psh - TCP PSH bit to be checked against the packet.
- urg | non_urg - TCP URG bit to be checked against the packet.
- syn | non_syn - TCP SYN bit to be checked against the packet.
- fin | non_fin - TCP FIN bit to be checked against the packet.
- dscp <short (0-63)> - Differentiated services code point provides the quality of service control.

>

Mode

IPV4 ACL Extended Access List Configuration Mode

deny tcp

Command Objective

This command specifies the TCP packets to be rejected based on the associated parameters.

Syntax

```
deny tcp {any | host <src-ip-address> | <src-ip-address>
<src-mask> } [eq <port-number (1-65535)>] { any | host <dest-
ip-address> | <dest-ip-address> <dest-mask> } [eq <port-number
(1-65535)>] ace-priority <integer (1-2147483647)> [{ack |
non_ack}] [{rst | non_rst}] [{psh | non_psh}] [{urg | non_urg}]
[{syn | non_syn}] [{fin | non_fin}] [dscp <value (0-63)>]
```

Parameter Description

- tcp - Transport Control Protocol.
- any| host <src-ip-address>|<src-ip-address> <src-mask> - Source IP address can be
  - 'any' or
  - the dotted decimal address or
  - the IP Address of the network or the host that the packet is from and the network mask to use with the source address.
- eq <short (1-65535)> - Port Number.
- any|host <dest-ip-address>|<dest-ip-address> <dest-mask> - Destination IP address can be
  - 'any' or
  - the dotted decimal address or
  - the IP Address of the network or the host that the packet is destined for and the network mask to use with the destination address
- ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules.
- ack | non_ack - TCP ACK bit to be checked against the packet.
- rst | non_rst - TCP RST bit to be checked against the packet.
- psh | non_psh - TCP PSH bit to be checked against the packet.
- urg | non_urg - TCP URG bit to be checked against the packet.
- syn | non_syn - TCP SYN bit to be checked against the packet.
- fin | non_fin - TCP FIN bit to be checked against the packet.

- dscp <short (0-63)> - Differentiated services code point provides the quality of service control.

>

Mode

IPV4 ACL Extended Access List Configuration Mode

permit udp

Command Objective

This command specifies the UDP packets to be forwarded based on the associated parameters.

Syntax

permit udp { any | host <src-ip-address> | <src-ip-address> <src-mask>} [eq <port-number (1-65535)>] { any | host <dest-ip-address> | <dest-ip-address> <dest-mask> } [eq <port-number (1-65535)>] ace-priority <integer (1-2147483647)> [dscp <value (0-63)>]

Parameter Description

- udp - User Datagram Protocol.
- any| host <src-ip-address>|<src-ip-address> <src-mask> - Source IP address can be
  - 'any' or
  - the dotted decimal address or
  - the IP Address of the network or the host that the packet is from

and the network mask to use with the source address.

- eq <short (1-65535)> - Port Number.

- any|host <dest-ip-address>|<dest-ip-address> <dest-mask> - Destination IP address can be

■ 'any' or

■ the dotted decimal address or

■ the IP Address of the network or the host that the packet is destined for and the network mask to use with the destination address

- ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules.

- dscp <short (0-63)> - Differentiated services code point provides the quality of service control.

>

Mode

IPV4 ACL Extended Access List Configuration Mode

deny udp

Command Objective

This command specifies the UDP packets to be rejected based on the associated parameters.

Syntax

deny udp { any | host <src-ip-address> | <src-ip-address> <src-mask>} [eq <port-number (1-65535)>] { any | host <dest-ip-address> | <dest-ip-address> <dest-mask> } [eq <port-number (1-65535)>] ace-priority <integer (1-2147483647)> [dscp < value (0-63)>]

Parameter Description

- udp - User Datagram Protocol.
- any| host <src-ip-address>|<src-ip-address> <src-mask> - Source IP address can be
  - ‘any’ or
  - the dotted decimal address or
  - the IP Address of the network or the host that the packet is from and the network mask to use with the source address.
- eq <short (1-65535)> - Port Number.
- any|host <dest-ip-address>|<dest-ip-address> <dest-mask> - Destination IP address can be
  - ‘any’ or
  - the dotted decimal address or
  - the IP Address of the network or the host that the packet is destined for and the network mask to use with the destination address
- ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules.
- dscp <short (0-63)> - Differentiated services code point

provides the quality of service control.

>

Mode

IPV4 ACL Extended Access List Configuration Mode

permit icmp

Command Objective

This command specifies the ICMP packets to be forwarded based on the IP address and the associated parameters.

Syntax

permit icmp {any |host <src-ip-address>|<src-ip-address> <mask>} {any | host <dest-ip-address> | <dest-ip-address> <mask> } [type <message-type (0-255)>] [code <message-code (0-255)>] ace-priority <integer (1-2147483647)> [dscp <integer (0-63)>]

Parameter Description

- icmp - Internet Control Message Protocol.
- any| host <src-ip-address>|<src-ip-address> <mask> - Source IP address can be
  - ‘any’ or
  - the dotted decimal address or
  - the IP Address of the network or the host that the packet is from

and the network mask to use with the source address.

● any|host <dest-ip-address>|<dest-ip-address> <mask> - Destination IP address can be

■ ‘any’ or

■ the dotted decimal address or

■ the IP Address of the network or the host that the packet is destined for and the network mask to use with the destination address

● type <short (0-255)> - message type

● code <short (0-255)> - message code

● ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules.

● dscp <short (0-63)> - Differentiated services code point provides the quality of service control.

>

Mode	IPV4 ACL Extended Access List Configuration Mode

deny icmp

Command Objective	This command specifies the ICMP packets to be rejected based on the IP address and associated parameters.

Syntax

deny icmp {any |host <src-ip-address>|<src-ip-address> <mask>} {any | host <dest-ip-address> | <dest-ip-address> <mask> }

[type <message-type (0-255)>] [code <message-code (0-255)>] ace-priority <integer (1-2147483647)> [dscp <integer (0-63)>]

Parameter Description

- icmp - Internet Control Message Protocol.
- any| host <src-ip-address>|<src-ip-address> <mask> - Source IP address can be
  - ■ ‘any’ or
  - ■ the dotted decimal address or
  - ■ the IP Address of the network or the host that the packet is from and the network mask to use with the source address.
- any|host <dest-ip-address>|<dest-ip-address> <mask> - Destination IP address can be
  - ■ ‘any’ or
  - ■ the dotted decimal address or
  - ■ the IP Address of the network or the host that the packet is destined for and the network mask to use with the destination address
- type <short (0-255)>   - message type
- code <short (0-255)> - message code
- ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules.

	● dscp <short (0-63)> - Differentiated services code point provides the quality of service control. >
Mode	IPV4 ACL Extended Access List Configuration Mode

no ace-priority

Command Objective	This command deletes an ace entry.
Syntax	no ace-priority <integer (1-2147483647)>
Parameter Description	● ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. >
Mode	IPV4 ACL Extended Access List Configuration Mode

ipv6 access-list extend

Command Objective	This command creates ipv6 ACLs and enters the ipv6 Access-list configuration mode. The no form of the command deletes the ipv6 access-list.
Syntax	ipv6 access-list extended <string(31)> no ipv6 access-list extended <string(31)>
Parameter Description	● <string(31)> –Configures the access-list name.
Mode	Global Configuration Mode

permit ipv6

Command Objective	This command specifies IPv6 packets to be forwarded based on protocol and associated parameters.
Syntax	permit ipv6 {any | host <src-ipv6-addr> <src-prefix-len (0-128)> } { any | host <dst-ipv6-addr> <dst-prefix-len (0-128)> } ace-priority <integer (1-2147483647)> [dscp <short(0-63)>]

Parameter Description

- ipv6 – Ipv6 protocol.
- any | host <ip6_addr> <integer(0-128)> - Source address of the host / any host.
- any | host <ip6_addr> <integer(0-128)> - Destination address of the host / any host.
- ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules.
- dscp <short (0-63)> - Differentiated services code point provides the quality of service control.

>

Mode

IPV6 ACL Extended Access List Configuration Mode

deny ipv6

Command Objective

This command specifies IPv6 packets to be forwarded based on protocol and associated parameters.

Syntax

deny ipv6 {any | host <ip6_addr> <src-prefix-len (0-128)> } { any | host <ip6_addr> <dst-prefix-len (0-128)> } ace-priority <integer (1-2147483647)> [dscp <short(0-63)>]

Parameter Description	● ipv6 – Ipv6 protocol. ● any | host <ip6_addr> <integer(0-128)> - Source address of the host / any host. ● any | host <ip6_addr> <integer(0-128)> - Destination address of the host / any host. ● ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. ● dscp <short (0-63)> - Differentiated services code point provides the quality of service control. >
Mode	IPV6 ACL Extended Access List Configuration Mode

permit tcp

Command Objective	This command specifies the IPv6 TCP packets to be forwarded based on the associated parameters.
Syntax	> permit tcp {any | host <src-ipv6-addr> <src-prefix-len (0-128)} [eq <port-number (1-65535)>] {any | host <dst-ipv6-addr> <dst-prefix-len (0-128)>} [eq <port-number (1-65535)>] ace-priority <integer (1-2147483647)> [{ack |

	non_ack}] [{rst | non_rst}] [{psh | non_psh}] [{urg | non_urg}] [{syn | non_syn}] [{fin | non_fin}] [dscp <value (0-63)>] >
Parameter Description	● tcp - Transport Control Protocol. ● any | host <ip6_addr> <integer(0-128)> - Source address of the host / any host ● eq <short (1-65535)> - Port Number. ● any | host <ip6_addr> <integer(0-128)> - Destination address of the host / any host. ● ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. ● ack | non_ack - TCP ACK bit to be checked against the packet. ● rst | non_rst - TCP RST bit to be checked against the packet. ● psh | non_psh - TCP PSH bit to be checked against the packet. ● urg | non_urg - TCP URG bit to be checked against the packet. ● syn | non_syn - TCP SYN bit to be checked against the packet. ● fin | non_fin - TCP FIN bit to be checked against the packet. ● dscp <short (0-63)> - Differentiated services code point provides the quality of service control. >
Mode	IPV6 ACL Extended Access List Configuration Mode

deny tcp

Command Objective

This command specifies the IPv6 TCP packets to be forwarded based on the associated parameters.

Syntax

```
>    deny tcp {any | host <src-ipv6-addr> <src-prefix-len (0-128)}
>    [eq <port-number (1-65535)>] {any | host <dst-ipv6-addr>
>    <dst-prefix-len (0-128)>} [eq <port-number (1-65535)>]
>    ace-priority <integer (1-2147483647)> [{ack | non_ack}] [{rst
     |
>    non_rst}] [{psh | non_psh}] [{urg | non_urg}] [{syn |
     non_syn}] [{fin | non_fin}] [dscp <value (0-63)>]
>
```

Parameter Description

- tcp - Transport Control Protocol.
- any | host <ip6_addr> <integer(0-128)> - Source address of the host / any host
- eq <short (1-65535)> - Port Number.
- any | host <ip6_addr> <integer(0-128)> - Destination address of the host / any host.
- ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the

packet matches with more than one filter rules.

- ack | non_ack - TCP ACK bit to be checked against the packet.
- rst | non_rst - TCP RST bit to be checked against the packet.
- psh | non_psh - TCP PSH bit to be checked against the packet.
- urg | non_urg - TCP URG bit to be checked against the packet.
- syn | non_syn - TCP SYN bit to be checked against the packet.
- fin | non_fin - TCP FIN bit to be checked against the packet.
- dscp <short (0-63)> - Differentiated services code point provides the quality of service control.

>

Mode

IPV6 ACL Extended Access List Configuration Mode

permit udp

Command Objective

This command specifies the IPv6 TCP packets to be forwarded based on the associated parameters.

Syntax

> permit udp {any | host <src-ipv6-addr> <src-prefix-len (0-128)>} [eq <port-number (1-65535)>] {any | host <dst-ipv6-addr>

	> <dst-prefix-len (0-128)>} [eq <port-number (1-65535)>] > ace-priority <integer (1-2147483647)> [dscp <value (0-63)] >
Parameter Description	● udp - User Datagram Protocol. ● any | host <ip6_addr> <integer(0-128)> - Source address of the host / any host ● eq <short (1-65535)> - Port Number. ● any | host <ip6_addr> <integer(0-128)> - Destination address of the host / any host. ● ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. ● dscp <short (0-63)> - Differentiated services code point provides the quality of service control. >
Mode	IPV6 ACL Extended Access List Configuration Mode

deny udp

Command Objective	This command specifies the IPv6 TCP packets to be forwarded based on the associated parameters.

Syntax

> deny udp {any | host <src-ipv6-addr> <src-prefix-len (0-128)>} [eq <port-number (1-65535)>] {any | host <dst-ipv6-addr> <short(0-128)>} [eq <port-number (1-65535)>]

> ace-priority <integer (1-2147483647)> [dscp <value (0-63)>]

>

Parameter Description

- udp - User Datagram Protocol.
- any | host <ip6_addr> <integer(0-128)> - Source address of the host / any host
- eq <short (1-65535)> - Port Number.
- any | host <ip6_addr> <integer(0-128)> - Destination address of the host / any host.
- ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules.
- dscp <short (0-63)> - Differentiated services code point provides the quality of service control.

>

Mode

IPV6 ACL Extended Access List Configuration Mode

permit icmpv6

Command Objective

This command specifies the IPv6 TCP packets to be forwarded based on

	the associated parameters.
Syntax	> permit icmpv6 {any | host <src-ipv6-addr> > <src-prefix-len (0-128)>} {any | host <dst-ipv6-addr> > <dst-prefix-len (0-128)} ace-priority <integer (1-2147483647)> [type <short(0-255)>] [code <short(0-255)>] > [dscp <value (0-63)>]
Parameter Description	● icmpv6 - Internet Control Message Protocol. ● any | host <ip6_addr> <integer(0-128)> - Source address of the host / any host ● any | host <ip6_addr> <integer(0-128)> - Destination address of the host / any host. ● ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. ● type <short (0-255)> - message type ● code <short (0-255)> - message code ● dscp <short (0-63)> - Differentiated services code point provides the quality of service control. >
Mode	IPV6 ACL Extended Access List Configuration Mode

deny icmpv6

Command Objective

This command specifies the IPv6 TCP packets to be forwarded based on the associated parameters.

Syntax

- deny icmpv6 {any | host <src-ipv6-addr>
- <src-prefix-len (0-128)>} {any | host <dst-ipv6-addr> <dst-prefix-len (0-128)>} ace-priority <integer (1-2147483647)> [type <short (0-255)>] [code <short (0-255)>] [dscp <value (0-63)>]

Parameter Description

- icmpv6 - Internet Control Message Protocol.
- any | host <ip6_addr> <integer(0-128)> - Source address of the host / any host
- any | host <ip6_addr> <integer(0-128)> - Destination address of the host / any host.
- ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules.
- type <short (0-255)> - message type
- code <short (0-255)> - message code
- dscp <short (0-63)> - Differentiated services code point provides the quality of service control.

Mode	IPV6 ACL Extended Access List Configuration Mode

no ace-priority

Command Objective	This command deletes an ace entry.
Syntax	no ace-priority <integer (1-2147483647)>
Parameter Description	● ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. >
Mode	IPV6 ACL Extended Access List Configuration Mode

mac access-list extend

Command Objective	This command creates mac ACLs and enters the mac Access-list configuration mode.

	The no form of the command deletes the mac access-list.
Syntax	mac access-list extended <string(31)> no mac access-list extended <string(31)>
Parameter Description	● <string(31)> –Configures the access-list name.
Mode	Global Configuration Mode

permit mac

Command Objective	This command specifies the packets to be forwarded based on the MAC address and the associated parameters, that is, this command allows non-IP traffic to be forwarded if the conditions are matched.
Syntax	> permit { any | host <src-mac-address> } { any | host <dest-mac-address> } {ace-priority <integer (1-2147483647)>} [ethertype <integer (1536-65535)>] [vlan <vlan-id (1-4094)>] [vlan-priority <value (0-7)>] >

Parameter Description

- any | host <src-mac-address > - Source MAC address to be matched with the packet
- any | host <dest-mac-address > - Destination MAC address to be matched with the packet
- ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules.
- ethertype <integer (1-65535)> - Specifies the non-IP protocol type to be filtered.
- vlan <integer (1-4094)> - VLAN value to match against incoming packets.
- vlan-priority <short (0-7)> - VLAN priority value to match against incoming packets.

>

Mode

MAC ACL Extended Access List Configuration Mode

deny mac

Command Objective

This command specifies the packets to be rejected based on the MAC address and the associated parameters.

Syntax

> deny { any | host <src-mac-address> } { any | host <dest-mac-address> } {ace-priority <integer

	(1-2147483647)>} [ethertype <integer (1536-65535)>] [vlan <vlan-id (1-4094)>] [vlan-priority <priority (0-7)>] >
Parameter Description	● any | host <src-mac-address > - Source MAC address to be matched with the packet ● any | host <dest-mac-address > - Destination MAC address to be matched with the packet ● ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. ● ethertype <integer (1-65535)> - Specifies the non-IP protocol type to be filtered. ● vlan <integer (1-4094)> - VLAN value to match against incoming packets. ● vlan-priority <short (0-7)> - VLAN priority value to match against incoming packets. >
Mode	MAC ACL Extended Access List Configuration Mode

no ace-priority

Command Objective	This command deletes an ace entry.

Syntax	no ace-priority <integer (1-2147483647)>
Parameter Description	● ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. >
Mode	MAC ACL Extended Access List Configuration Mode

ip access-group

Command Objective	This command enables access control for the packets on the interface. The no form of this command removes all access groups or the specified access group from the interface.
Syntax	ip access-group <string (31)> in no ip access-group [<string(31)>] in
Parameter	● <string(31)> - IP access control list name.

Description	
Mode	Interface Configuration Mode

ipv6 access-group

Command Objective	This command enables ipv6 access control for the packets on the interface. The no form of this command removes all access groups or the specified access group from the interface.
Syntax	Ipv6 access-group <string (31)> in no ipv6 access-group [<string(31)>] in
Parameter Description	● <string(31)> - IPv6 access control list name.
Mode	Interface Configuration Mode

mac access-group

Command Objective	This command applies a MAC access control list (ACL) to a Layer 2 interface. The no form of this command can be used to remove the MAC ACLs from the interface.
Syntax	mac access-group <string (31)> in no mac access-group [<string(31)>] in
Parameter Description	● <string(31)> - MAC access control list name.
Mode	Interface Configuration Mode

show access-lists

Command Objective	This command displays the access lists configuration.
Syntax	show access-lists [{ip | mac | ipv6 } [<string(31)>]]

Parameter Description	> ip - IP Access List > mac – MAC Access List > ipv6 – Ipv6 Access List > <string(31)> - Name of access list >
Mode	Privilege EXEC Mode

QoS

qos

Command Objective	This command enables or disables the QoS subsystem.
Syntax	qos {enable | disable}
Parameter Description	● enable - Enables QoS subsystem ● disable - Disables Qos subsystem >
Mode	Global Configuration Mode

qos trust

Command Objective	This command sets qos trust mode.
Syntax	qos trust {cos | dscp | cos-dscp}
Parameter Description	● cos – trust cos. ● dscp – trust dscp. ● cos-dscp – trust cos, if cos not set, trust dscp.

>

Mode	Global Configuration Mode

priority-map

Command Objective	This command sets the type of the incoming priority mapping to queue. The no form of the command sets default value.
Syntax	priority-map in-priority-type { vlanPri | ipDscp } <integer(0-63)> [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>] to <integer(1-8)> no priority-map in-priority-type { vlanPri | ipDscp } <integer(0-63)> [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>]
Parameter Description	● vlanPri– Vlan priority. ● ipDscp– DSCP. ● <integer(0-63)> – Priority value. (0-7) for vlanPri, (0-63) for ipDscp.

	● integer(1-8) – Queue id. >
Mode	Global Configuration Mode

scheduler

Command Objective	This command creates a Scheduler and configures the Scheduler parameters.
Syntax	scheduler sched-algo {strict-priority | {wrr [weight <integer(0-128)> <integer(0-128)> <integer(0-128)> <integer(0-128)> <integer(0-128)> <integer(0-128)> <integer(0-128)> <integer(0-128)>]}}
Parameter Description	● strict-priority – strictPriority. ● wrr –weightedRoundRobin.. ● weight <integer(0-128)> <integer(0-128)> <integer(0-128)> <integer(0-128)> <integer(0-128)> <integer(0-128)> <integer(0-128)> <integer(0-128)> – weight of wrr from queue 1 to queue 8. >
Mode	Global Configuration Mode

class-policy

Command Objective	This command creates a qos policy. The no form of the command deletes a qos policy.
Syntax	class-policy <name (23)> no class-policy <name (23)>
Parameter Description	● <name (23)> – Name of qos policy. >
Mode	Global Configuration Mode

qos interface

Command Objective	This command sets the default ingress user priority for the port.
Syntax	qos interface <iftype> <ifnum> def-user-priority <integer(0-7)>
Parameter Description	● iftype - Interface type. ● ifnum - Interface number.

	● def-user-priority - Default ingress user priority for the port. >
Mode	Global Configuration Mode

match policy – tcp/udp

Command Objective	This command specifies the TCP/UDP packets to be forwarded based on the associated parameters.
Syntax	match policy { any | host <src-mac-address> } { any | host <dest-mac-address>} [ethertype <integer (1-65535)>] [vlan <vlan-id (1-4094)>] [vlan-priority <value (0-7)>] { tcp | udp } {any | host <src-ip-address>| <src-ip-address> <src-mask> } [eq <port-number (1-65535)>] { any | host <dest-ip-address> | <dest-ip-address> <dest-mask> } [eq <port-number (1-65535)>] [dscp <dscp-value (0-63)>] [action { tos <tos-value(0-7)> | dscp <value (0-63)>}]
Parameter Description	● any | host <src-mac-address> - Source MAC address to be matched with the packet ● any | host <dest-mac-address> - Destination MAC address to be matched with the packet ● ethertype <integer (1-65535)> - Specifies the non-IP protocol type to be filtered. ● vlan <vlan-id (1-4094)> - VLAN value to match against

incoming packets.

- vlan-priority <value (0-7)> - VLAN priority value to match against incoming packets.
- tcp - Transport Control Protocol.
- udp - User Datagram Protocol.
- any | host <src-ip-address>| <src-ip-address> <src-mask> - Source IP address can be
  - ‘any’ or
  - the dotted decimal address or
  - the IP Address of the network or the host that the packet is from and the network mask to use with the source address.
- eq <port-number (1-65535)> - Port Number.
- any | host <dest-ip-address> | <dest-ip-address> <dest-mask> - Destination IP address can be
  - ‘any’ or
  - the dotted decimal address or
  - the IP Address of the network or the host that the packet is destined for and the network mask to use with the destination address.
- dscp <dscp-value (0-63)> - Differentiated services code point provides the quality of service control.
- tos <tos-value(0-7)> - set tos to value.
- dscp <value (0-63)> - set dscp to value.

>

Mode	Policy Map Configuration Mode

match policy – icmp

Command Objective	This command specifies the ICMP packets to be forwarded based on the associated parameters.
Syntax	match policy { any | host <src-mac-address> } { any | host <dest-mac-address>} [ethertype <integer (1-65535)>] [vlan <vlan-id (1-4094)>] [vlan-priority <value (0-7)>] icmp {any | host <src-ip-address>| <src-ip-address> <src-mask> } { any | host <dest-ip-address> | <dest-ip-address> <dest-mask> } [type <message-type (0-255)>] [code <message-code (0-255)>] [dscp <dscp-value (0-63)>] [action { vpt <tos-value(0-7)> | dscp <value (0-63)>}]
Parameter Description	● any | host <src-mac-address> - Source MAC address to be matched with the packet ● any | host <dest-mac-address> - Destination MAC address to be matched with the packet ● ethertype <integer (1-65535)> - Specifies the non-IP protocol type to be filtered. ● vlan <vlan-id (1-4094)> - VLAN value to match against incoming packets. ● vlan-priority <value (0-7)> - VLAN priority value to match

against incoming packets.

- any | host <src-ip-address>| <src-ip-address> <src-mask> - Source IP address can be
  - ‘any’ or
  - the dotted decimal address or
  - the IP Address of the network or the host that the packet is from and the network mask to use with the source address.
- any | host <dest-ip-address> | <dest-ip-address> <dest-mask> - Destination IP address can be
  - ‘any’ or
  - the dotted decimal address or
  - the IP Address of the network or the host that the packet is destined for and the network mask to use with the destination address.
- type <message-type (0-255)> - message type
- code <message-code (0-255)> - message code
- dscp <dscp-value (0-63)> - Differentiated services code point provides the quality of service control.
- vpt <tos-value(0-7)> - set tos to value.
- dscp <value (0-63)> - set dscp to value.

>

Mode	Policy Map Configuration Mode

match policy - ip/ospf/pim/protocol type

Command Objective

This command specifies the ip/ospf/pim/protocol type packets to be forwarded based on the associated parameters.

Syntax

```
match policy { any | host <src-mac-address> } { any | host
<dest-mac-address>} [ ethertype <integer (1-65535)> ] [ vlan
<vlan-id (1-4094)>] [ vlan-priority <value (0-7)>] { ip | ospf | pim
| <protocol-type (1-255)>} {any | host <src-ip-address>|
<src-ip-address> <src-mask> } { any | host <dest-ip-address> |
<dest-ip-address> <dest-mask> } [dscp <dscp-value (0-63)>]
[action { vpt <tos-value(0-7)> | dscp <value (0-63)>}]
```

Parameter Description

- any | host <src-mac-address> - Source MAC address to be matched with the packet
- any | host <dest-mac-address> - Destination MAC address to be matched with the packet
- ethertype <integer (1-65535)> - Specifies the non-IP protocol type to be filtered.
- vlan <vlan-id (1-4094)> - VLAN value to match against incoming packets.
- vlan-priority <value (0-7)> - VLAN priority value to match against incoming packets.
- any | host <src-ip-address>| <src-ip-address> <src-mask> - Source IP address can be
  - 'any' or
  - the dotted decimal address or
  - the IP Address of the network or the host that the packet is

	from and the network mask to use with the source address. ● any | host <dest-ip-address> | <dest-ip-address> <dest-mask> - Destination IP address can be ■ ‘any’ or ■ the dotted decimal address or ■ the IP Address of the network or the host that the packet is destined for and the network mask to use with the destination address. ● dscp <dscp-value (0-63)> - Differentiated services code point provides the quality of service control. ● vpt <tos-value(0-7)> - set tos to value. ● dscp <value (0-63)> - set dscp to value. >
Mode	Policy Map Configuration Mode

no match policy

Command Objective	This command clears all policy configuration.
Syntax	no match policy
Mode	Policy Map Configuration Mode

show qos global info

Command Objective	This command displays QoS related global configurations.
Syntax	show qos global info
Mode	Privileged EXEC Mode

show priority-map

Command Objective	This command displays the priority mapping to queue.
Syntax	show priority-map in-priority-type { vlanPri | ipDscp }
Parameter **Description**	● vlanPri– Vlan priority. ● ipDscp– DSCP. >
Mode	Privileged EXEC Mode

show class-policy

Command Objective	This command displays the qos policy.
Syntax	show class-policy [{<name(23)> | interface <iftype> <ifnum>}]
Parameter Description	● <string(31)> –Name of qos policy. ● iftype - Interface type. ● ifnum - Interface number. >

Parameter Description	● <string(31)> –Name of qos policy. ● iftype - Interface type. ● ifnum - Interface number. >
Mode	Privileged EXEC Mode

show scheduler

Command Objective	This command displays the configured Scheduler.
Syntax	show scheduler
Mode	Privileged EXEC Mode

show qos def-user-priority

Command Objective	This command displays the configured default ingress user priority for a port.
Syntax	show qos def-user-priority [interface <iftype> <ifnum>]

Parameter Description	● iftype - Interface type. ● ifnum - Interface number. >
Mode	Privileged EXEC Mode

qos trust

Command Objective	This command enable/disable qos trust on port.
Syntax	qos trust {enable | disable}
Parameter Description	● enable –enable qos trust on port. ● disable - disable qos trust on port. >
Mode	Interface Configuration Mode

service-policy

Command Objective	This command enables qos policy on the interface.

	The no form of this command removes qos policy from the interface.
Syntax	service-policy <class-policy-name (31)> in no service-policy <class-policy-name (31)>
Parameter Description	● <class-policy-name (31)> – Name of qos policy. >
Mode	Interface Configuration Mode

Storm control

Storm-control

Command Objective

This command sets the storm control rate for broadcast, unknown-multicast and DLF packets.

The no form of the command sets storm control rate for broadcast, unknown-multicast and DLF packets to the default value.

Syntax

```
storm-control { broadcast | unknown-multicast | dlf } level
<rate-value>
```

```
no storm-control { broadcast | unknown-multicast | dlf } level
```

Parameter

Description

- broadcast - Broadcast packets.
- unknown-multicast –Unknown multicast packets.
- dlf - Unknown unicast packets.
- level - Storm-control suppression level as a total number of packets per second.

>

Mode

Interface Configuration Mode

Bandwidth control

Rate-limit

Command Objective

This command enables the rate limiting on an interface.

The no form of the command disables the rate limiting.

Syntax

rate-limit { output | input } [<integer(1-80000000)>]

no rate-limit { output | input }

Parameter Description

- output – egress limitation.
- input –ingress limitation.
- <integer(1-80000000)> -Line rate in kbps.

>

Mode

Interface Configuration Mode