Panasonic®

CLI Reference

Layer2 Ethernet Switch

Model Number: ZLP91089/ZLP91249
ZLP91240

The target model for this CLI reference is as follows.

Model Name	Model Number	Firmware Version
GA-MU8TPoE+	ZLP91089	1.0.0-2.03.17 or higher
XG-MU24TPoE+	ZLP91249	1.0.0-3.03.17 or higher
XG-MU24T	ZLP91240	1.0.0-3.03.17 or higher

Regarding the function compatible with each model, refer to its specification.

Table of Contents

1 Key Conventions

1.1 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.

1.2 Others

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

2 CLI Command Modes

2.1 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 Configruration	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 command **vlan vlan-id** is used to enter the Config-VLAN mode.	< *Switch Name* >(config-vlan)#
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)#

Command Mode	Access Method	Prompt
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 MSTP configuration mode.	< *Switch Name* >(config-qc-mst)#
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)#

3 System Commands

3.1 help

This command displays a brief description for the given command.

Syntax

- help [command]

Default

None.

Command Mode

All Mode.

Usage Guideline

None.

Example

This example shows how to display a brief description for the **vlan** command.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# help vlan

CONFIGURE commands :
  vlan <vlan-id/vfi_id>
  [Desc]: Configures a VLAN

  vlan range <vlan-range>
  [Desc]: Selects the range of IVR to be configured

  vlan_trunk { enable | disable }
  [Desc]: Enables / Disables Vlan trunking port in the switch

XX-MUxxTPoE+(config)#
```

3.2 clear screen

This command clears all the contents from the screen.

Syntax

- clear screen

Default

None.

Command Mode

All Modes.

Usage Guideline

None.

Example

This example shows how to clear all the contents from the screen like terminal software.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# vlan 10
XX-MUxxTPoE+(config-vlan)# clear screen




XX-MUxxTPoE+(config-vlan)#
```

3.3 end

Exit to Privileged EXEC Mode from any mode.

Syntax

- **end**

Default

None.

Command Mode

All Modes.

Usage Guideline

None.

Example

This example shows how to display the return to Privileged EXEC Mode from Config-VLAN mode.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# vlan 10
XX-MUxxTPoE+(config-vlan)# end
XX-MUxxTPoE+#
```

3.4 logout

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

Default

None.

Command Mode

Privileged EXEC/User EXEC Mode.

Usage Guideline

None.

Example

This example shows how to logout from the console session.

```
XX-MUxxTPoE+# logout
XX-MUxxTPoE+ login:
```

3.5 show privilege

Show current privilege level.

Syntax

- **show privilege**

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to display the current privilege level.

```
XX-MUxxTPoE+# show privilege

Current privilege level is 15
XX-MUxxTPoE+#
```

3.6 show cli

This command displays TTY line information such as EXEC timeout.

Syntax

- **show cli**

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to display TTY line information.

```
XX-MUxxTPoE+# show cli
CLI Session Timeout (in mins) = 30
XX-MUxxTPoE+#
```

3.7 exit

This command exits the current mode and reverts to the mode used prior to the current mode.

Syntax

- exit

Default

None.

Command Mode

All Modes.

Usage Guideline

None.

Example

This example shows how to return to privileged EXEC mode from global configure mode.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# exit
XX-MUxxTPoE+#
```

3.8 configure terminal

This command enters to Global Configuration Mode which allows the user to execute all the commands that supports global configuration mode.

Syntax

- configure terminal

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to enter the Global Configuration mode from the Privileged EXEC mode.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)#
```

3.9 listuser

This command lists all the default and newly created users, along with their permissible mode.

Syntax

- **listuser**

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to display the list of all user entries.

```
XX-MUxxTPoE+#listuser

USER                PRIVILEGE
Sample                  15
manager                 15
XX-MUxxTPoE+#
```

3.10 show user

This command displays the information about the current user.

Syntax

- show users

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows the current user **manager** is connected by console and peer-address is **Local Peer.**

```
XX-MUxxTPoE+# show user

 Line            User            Peer-Address
  con            manager         Local Peer
XX-MUxxTPoE+#
```

3.11 lock

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

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

An unlock password is the password for the administrator user who locked CLI console.

Example

This example shows how to lock the CLI console and unlock CLI console.

```
XX-MUxxTPoE+# lock
CLI console locked
Enter Password to unlock the console:
XX-MUxxTPoE+#
```

3.12 show history

This command displays a list of recently executed commands.

Syntax

- show history

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

This command shows all recently executed commands you sent include incorrect commands. And commands that you send before logout are not displayed.

Example

This example shows how to display the list of recently executed commands.

```
XX-MUxxTPoE+# show history
 1  lock
 2  show history
XX-MUxxTPoE+#
```

3.13 username

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 <password>] [confirm password<confirm-password>][privilege <1-15>]
- no username < user-name >

Parameters

Parameters	Description
<user-name>	Specifies the login username to be created.
<password>	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.
<confirm-password>	Re-enter the password to confirm.
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.

Default

By default, username and password are manager, privilege level is 15.

Command Mode

Global Configuration Mode.

Usage Guideline

After entering the password and the default value "manager" and running it, you need to set the password.

Example

This example shows how to create the user that the login username is **Sample**, the login password is **sample**, and the privilege level is **15**.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)#username Sample password sample confirm-password sample
privilege 15
XX-MUxxTPoE+(config)#
```

3.14 line cli

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**

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None

Example

This example shows how to enter the line configuration mode.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# line cli
XX-MUxxTPoE+(config-line)#
```

3.15 logging synchronous

The logging synchronous command is used to manage how log messages are displayed on the device console or terminal. It helps in configuring the severity level of log messages that should be displayed, ensuring that only relevant logs are seen. Additionally, this command can limit the number of messages displayed, which is particularly useful in high-traffic environments where excessive logging could clutter the console and obscure important information.

Syntax

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

Parameters

severity level is can be set by numeric or keywords.

Parameters	Description
severity <short (0-7)> (0 = emergencies, 7 = debugging) <keywords (all | emergencies | critical | warnings | errors | notification | informational | debugging |	Defines the severity level of message. Numeric or keywords can be used to set.
limit <size (1-200)>	This parameter defined limit on the number of message displaying.

Default

By default, the option is informational and limit is 200.

Command Mode

Line Configuration Mode.

Usage Guideline

You cannot configure both the severity level and the limit on the number of messages at the same time.

Example

This example shows how to set the severity level to **alerts** and the limit on the number of the messages to 100.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)#line cli
XX-MUxxTPoE+(config-line)# logging synchronous severity alerts
XX-MUxxTPoE+(config-line)# logging synchronous limit 100
XX-MUxxTPoE+(config-line)#
```

3.16 exec-timeout

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 (1-10000)>
- no exec-timeout

Default

By default, this option is 30 Seconds.

Command Mode

Line Configuration Mode.

Usage Guideline

The shorter exec-timeout increase security but require freaquent logins, the longer exec-timeout offer more covenience but increase risks.

Example

This example shows how to set the time for EXEC line disconnection to 3600.

```
XX-MUxxTPoE+#c onfigure terminal
XX-MUxxTPoE+(config)# line cli
XX-MUxxTPoE+(config-line)# exec-timeout 3600
XX-MUxxTPoE+(config-line)#
```

3.17 set cli pagination

This command sets that whether to use "- - MORE - -" paging for too long content.

Syntax

- set cli pagination {on | off}

Default

By default, this option is set cli pagination on.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

Example

This example shows how to set the pagination off.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# set cli pagination off
XX-MUxxTPoE+(config)#
```

3.18 clear counters

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>]

Parameters

Parameters	Description
<interface - type(gigabitethernet | fastethernet | port-channel | tunnel | vlan)>	Configures the specified type of interface.
<interface - id (0/1 | 0/1 |channel-group number(1-65535)| vlan-id(1-4096)>	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to clear the interface counters from port 5.

```
XX-MUxxTPoE+# clear counters gigabitethernet 0/5
XX-MUxxTPoE+
```

3.19 interface range

This command selects the range of physical interfaces to be configured.

Syntax

- interface range {<interface - type> <slot/port - port>}

Parameters

Parameters	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.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

Example

This example shows how to enter the range of GigabitEthernet ports 1 to 5.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# interface range gigabitethernet 0/1-5
XX-MUxxTPoE+(config-if-range)#
```

3.20 interface

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>

Parameters

Parameters	Description
vlan <vlan - id>	VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094.
port - channel <integer(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.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

Example

The first example shows how to enter the interface configuration mode to configure the GigabitEthernet port 0/5.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# interface gigabitethernet 0/5
XX-MUxxTPoE+(config-if)#
```

The second example shows how to enter the VLAN's interface configuration mode to configure the VLAN-ID 10.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# interface vlan 10
XX-MUxxTPoE+(config-if)#
```

The third example shows how to enter the port-channel's interface configuration mode to configure the port-channel 1.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# interface port-channel 1
XX-MUxxTPoE+(config-if)#
```

3.21 set ip-management-vlan

This command configures the ip management vlan.

Syntax

- set ip-management-vlan <integer (1 - 4094)>

Default

By default, this option is set ip-management-vlan 1.

Parameters

Parameters	Description
integer <1 - 4094>	Vlan id.

Command Mode

Global Configuration Mode.

Usage Guideline

The VLAN setting as the IP management VLAN should not bind any network.

Example

This example shows how to set the VLAN 20 to ip management vlan.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# set ip-management-vlan 20
XX-MUxxTPoE+(config)#
```

3.22 shutdown

Set the AdminStatus of Interface down/up.

Syntax

- shutdown
- no shutdown

Default

By default, this option is no shutdown.

Command Mode

Interface Configuration Mode.

Usage Guideline

Set the AdminStatus of Interface down/up.

Example

This example shows how to shutdown the GigabitEthernet port 0/7.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# interface gigabitethernet 0/7
XX-MUxxTPoE+(config-if)# shutdown
XX-MUxxTPoE+(config-if)#
```

3.23 description

The description command allows network administrators to annotate interfaces with descriptive text, providing clarity and context about their role, connection, or purpose within the network.

Syntax

- description <description of this interface>
- no description

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

Descriptions about the interface.
Cancel the descriptions about the interface.

Example

This example shows how to add an interface description as **Example** for GigabitEthernet Port 0/7.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# interface gigabitethernet 0/7
XX-MUxxTPoE+(config-if)# description Example
XX-MUxxTPoE+(config-if)#
```

3.24 show interface port-security

This command shows the maximum number of learning address and lock mode.

Syntax

- show interface port-security [<iftype> <ifnum>]

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

You can use this command to display the current port-security status.
When setting port-security on a specific port, use the port-security command in chapter 3.34

Example

This example shows how to display the maximum number of learning addresses and lock mode.

```
XX-MUxxTPoE+# show interface port-security gigabitethernet 0/6

Gi0/6       Mac Limit is 10
XX-MUxxTPoE+#
```

3.25 show interface cable-diag

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>

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to display the diagnostic result for the port 1.

```
XX-MUxxTPoE+# show interface cable-diag gigabitethernet 0/1

Local Pair  Pair length      Pair status
----------  -----------      -----------
    A             0            OK
    B             0            OK
    C             0            OK
    D             0            OK
XX-MUxxTPoE+#
```

3.26 show interfaces

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 interfaces [{ [<interface-type> <interface-id>] [{ description | storm-control | flowcontrol | capabilities | status | port-security-state | rate-limit }]| {vlan <vlan-id> }

Parameters

Parameters	Description
<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.
<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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to display the status of Gigabit Ethernet port 5.

```
XX-MUxxTPoE+# show interfaces gigabitethernet 0/5

Gi0/5 up, line protocol is down (not connect)
Bridge Port Type: Customer Bridge Port

Interface SubType: gigabitEthernet
Interface Alias: Slot0/5

Hardware Address is 00:1A:2B:3C:4D:5E
MTU  1522 bytes, Full duplex, 1 Gbps,  Auto-Negotiation
HOL Block Prevention enabled.
CPU Controlled Learning disabled.
Auto-MDIX on
Input flow-control is off,output flow-control is off

Link Up/Down Trap is enabled

Reception Counters
   Octets                    : 0
   HC-Octets                 : 0
   Unicast Packets           : 0
   Discarded Packets         : 0
   Error Packets             : 0
   Unknown Protocol          : 0

Transmission Counters
   Octets                    : 0
   HC-Octets                 : 0
   Unicast Packets           : 0
   Discarded Packets         : 0
   Error Packets             : 0
RX Throughput:0 bytes/sec in last 5 min.
TX Throughput:0 bytes/sec in last 5 min.

XX-MUxxTPoE+
```

3.27 show interfaces counters

This command displays the interface statistics for each port.

Syntax

- show interfaces {counters | { <interface - type> <interface - id> counters }}

Parameters

Parameters	Description
counters	Displays the interface statistics for all the available interfaces.
<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.
<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

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to display Gigabit Ethernet port 0/1 statistics.

```
XX-MUxxTPoE+# show interfaces gigabitethernet 0/1 counters

Port      InOctet    InUcast    InDiscard  InErrs    InBcast    InMcast     InHCOctet
----     --------    --------   ---------- -------   --------   --------   ----------
Gi0/1     50424      9          0          0          35         268        50424
Port      OutOctet    OutUcast    OutDiscard  OutErrs     OutBcast    OutMcast    OutHCOctet
----      --------    --------    ----------  -------     --------    --------    ----------
Gi0/1     5474544     22          0           0           4716        37764       5474544
XX-MUxxTPoE+#
```

3.28 clear interface counters

This command displays the interface statistics for each port.

Syntax

- clear interfaces [<interface - type> <interface - id>] counters

Parameters

Parameters	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 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

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to clear the Gigabit Ethernet port 0/5 statistics.

```
XX-MUxxTPoE+# clear interfaces gigabitethernet 0/5 counters
XX-MUxxTPoE+#
```

3.29 show interface sfp - info

This command displays the SFP module information.

Syntax

- show interfaces sfp-info <interface - type> <interface - id>

Parameters

Parameters	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 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

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

This command is effective only on SFP port.

Example

This example shows how to display SFP module information on the port 11.

```
XX-MUxxTPoE+# show interface sfp-info gigabitethernet 0/11

SFP Module Information
Connector Type : LC  [ 0x07 ]
10G Ethernet Compliance Codes : Not compliant  [ 0x00 ]
Ethernet Compliance Codes : 1000-SX  [ 0x01 ]
Nominal Bit Rate : 1.3 Gbps
Laser Wavelength : 850 nm
Vendor OUI : 0x00 0x50 0x40
Vendor Name : Panasonic
Part Number : PN54021K
Revision Number : 0000
Serial Number : 35C31000083
Date Code : 01/01/2024
DDM Type : 0x58

DDM Information
Temperature : 20.00 C
Voltage : 3.35 V
Tx Laser Bias : 4.12 mA
Tx Power : -5.93 dBm
Rx Power : - infinite dBm
Tx Fault State : False
Rx LOS State : True
Alarm Flag : RxPWR Low.
 Warn Flag : RxPWR Low.

XX-MUxxTPoE+
```

3.30 show interface mtu

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> }]

Parameters

Parameters	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 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

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to display the MTU for Gigabit Ethernet port 0/1.

```
XX-MUxxTPoE+# show interface mtu gigabitethernet 0/1

Gi0/1       MTU size is 1522
XX-MUxxTPoE+#
```

3.31 show ip interface

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)>]}]

Parameters

Parameters	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 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
loopback	Loopback ID (0 - 100)

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to display the status and configuration of VLAN 1.

```
XX-MUxxTPoE+# show ip interface Vlan 1

vlan1 is up, line protocol is up
Internet Address is 172.16.100.1/24
Broadcast Address  172.16.100.255
XX-MUxxTPoE+
```

3.32 show flow-control

This command displays the flow-control information.

Syntax

- show flow-control [interface <interface-type> <interface-id>]

Parameters

Parameters	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 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

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to display the flow control information for Gigabit Ethernet port 0/11.

```
XX-MUxxTPoE+# show flow-control interface gigabitethernet 0/11

Port     Admin     Oper      Tx Pause    Rx Pause    HC TxPause      HC RxPause
         Tx   Rx   Tx   Rx
----     -------   -------   ---------   ---------   -----------     -----------
Gi0/11    on  on   off off   0           0           0               0
XX-MUxxTPoE+#
```

3.33 flowcontrol

This command is used to set the send or receive flow-control value for an interface.

Syntax

- flowcontrol { on | off }

Parameters

Parameters	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.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

The only guarantee provided by using this command is that the flow control feature is configured in the switch's software; it does not guarantee the actual behavior of the hardware. The actual behavior of the hardware may differ from the switch's configuration. This is because the determination of flow control functionality depends on both the local port/device and the device connected at the other end of the link, not just the local device.

Example

This example shows how to enable send and receive packet flow control.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# interface gigabitethernet 0/11
XX-MUxxTPoE+(config-if)# flowcontrol on
XX-MUxxTPoE+(config-if)#
```

3.34 port-security

This command configures the number of learning address on certain interface port.

Syntax

- port-security <limit-size(1-256)>
- no port-security

Parameters

Parameters	Description
<limit-size (1-256)>	Range is 1 to 256.

Default

By default, this option is no port-security.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is applicable in PORT Interface Mode.

Example

This example shows how to configure the maximum number of MAC addresses to 8 for Gigabit Ethernet port 10.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# interface gigabitethernet 0/10
XX-MUxxTPoE+(config-if)# port-security 8
XX-MUxxTPoE+(config-if)#
```

3.35 system mtu

Configures the Maximum Transmission Unit (MTU) for all interfaces.

Syntax

- system mtu <frame-size(1522-10240)>
- no system mtu <frame-size(1522-10240)>

Parameters

Parameters	Description
<frame-size(1522-10240)>	Range is 1522 to 10240.

Default

By default, this value is 1522.

Command Mode

Global Configuration Mode.

Usage Guideline

When you change the MTU frame size, be carefull to ensure that the new MTU size is compatible with other devices.
If there is no compatible, packets may be fragmented or cause communication errors.

Example

This example shows how to set the frame size of the MTU to 10240 for all interfaces.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# system mtu 10240
XX-MUxxTPoE+(config)#
```

3.36 system name

This command sets the system name.

Syntax

- system name <systemname>

Default

By default, the system name is the product name (GA-MU8TPoE+, XG-MU24TPoE+, XG-MU24T).

Command Mode

Global Configuration Mode.

Usage Guideline

None.

Example

This example shows how to set the system name to changed_name on the whole switch.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# system name changed_name
changed_name(config)#
```

3.37 no user-defined system name

This command sets the system name information to the default value.

Syntax

- no user-defined system name

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

Example

This example shows how to reset the system name to the default value. (default value:XX-MUxxTPoE+ in this example)

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# system name changed_name
changed_name(config)# no user-defined system name
XX-MUxxTPoE+(config)#
```

3.38 system contact

This command sets the contact information such as the phone number of system manager, email address and management organization.

Syntax

- system contact <contact info>

Default

By default, this option is Default Contact.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

Example

This example shows how to set the phone number of system manager as XXX-XXX-XXX.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# system contact XXX-XXX-XXX
XX-MUxxTPoE+(config)#
```

3.39 system location

This command sets the location name and indicates the position where the switch is installed.

Syntax

- system location <location name>

Default

By default, this option is Default Location.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

Example

This example shows how to set the location name to server_room_1.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# system location server_room_1
XX-MUxxTPoE+(config)#
```

3.40 sntp

This command enters to SNTP configuration mode which allows the user to execute all the commands that supports SNTP configuration mode.

Syntax

- sntp

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

Example

This example shows how to enter the SNTP configuration mode.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# sntp
XX-MUxxTPoE+(config-sntp)#
```

3.41 set sntp client

This command either enables or disables SNTP client module.

Syntax

- set sntp client {enabled | disabled}

Parameters

Parameters	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.

Default

By default, this option is enbled.

Command Mode

SNTP Configuration Mode.

Usage Guideline

None.

Example

This example shows how to disabled the SNTP client module.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# sntp
XX-MUxxTPoE+(config-sntp)# set sntp client disabled
XX-MUxxTPoE+(config-sntp)#
```

3.42 set sntp client time-zone

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

Parameters

Parameters	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	Disables SNTP client module and no request is sent to the host for time synchronization. • +00:00 to +14:00 • -00:00 to -12:00

Default

By default, this option is +00:00.

Command Mode

SNTP Configuration Mode.

Usage Guideline

None.

Example

This example shows how to set the system time to IST with SNTP client.
India Standard Time (IST) is UTC +5:30.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# sntp
XX-MUxxTPoE+(config-sntp)# set sntp client time-zone +05:30
XX-MUxxTPoE+(config-sntp)#
```

3.43 set sntp client clock-summer-time

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

Parameters

Parameters	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

Default

By default, this option is no sntp client clock summer-time.

Command Mode

SNTP Configuration Mode.

Usage Guideline

None.

Example

This example shows how to enable DST and set the summertime from the First Monday of June at 9 o'clock AM to the Last Friday of September at 6 o'clock PM.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# sntp
XX-MUxxTPoE+(config-sntp)#  set sntp client clock-summer-time First-Mon-Jun,09:00
Last-Fri-Sep,18:00
XX-MUxxTPoE+(config-sntp)#
```

3.44 set sntp unicast-server

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> | domain-name <string(64)>} [port <integer(1-65535)>]
- no sntp unicast-server {ipv4 <ucast_addr> | domain-name <string(64)>}

Parameters

Parameters	Description
ipv4 <ucast_addr>	Sets the address type of the unicast-server as Internet Protocol Version 4.
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.

Default

None.

Command Mode

SNTP Configuration Mode.

Usage Guideline

None

Example

This example shows how to set 192.168.10.1 as the SNTP unicast server.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# sntp
XX-MUxxTPoE+(config-sntp)# set sntp unicast-server ipv4 192.168.10.1
XX-MUxxTPoE+(config-sntp)#
```

3.45 show sntp clock

This command displays the current time.

Syntax

- show sntp clock

Default

None.

Command Mode

User / Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to display the current SNTP clock and configure time-zone.

```
XX-MUxxTPoE+# show sntp clock

        current time : Mon Aug 05 2024 22:14:58 (UTC +05:30 )
XX-MUxxTPoE+#
```

3.46 show sntp status

This command displays SNTP status.

Syntax

- show sntp status

Default

None.

Command Mode

User / Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to display the current SNTP status.

```
XX-MUxxTPoE+# show sntp status
sntp client is enabled
sntp client clock format is 24 hours
sntp client dst start time is not set
sntp client dst end time is not set
unicast primary server address is 192.168.33.58
unicast primary server port is 123
XX-MUxxTPoE+
```

3.47 clock set

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)>

Parameters

Parameters	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

Default

By default, this option is 00:00:00 01 january 2019.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

Example

This example shows how to set the clock to **August 7th, 2024 12:34:56 PM.**

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# clock set 12:34:56 7 august 2024
XX-MUxxTPoE+(config)#
```

3.48 show clock

This command displays the system date and time.

Syntax

- **show clock**

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to display the system clock.

```
XX-MUxxTPoE+# show clock

 Wed Aug 07 12:44:31 2024
XX-MUxxTPoE+#
```

3.49 show system information

This command displays system information.

Syntax

- **show system information**

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to display system information.

```
XX-MUxxTPoE+# show system information
Firmware Version                  : 2.03.09
Cloud Version                     : 1.0.0
Switch Name                       : XX-MUxxTPoE+
System Contact                    : Default Contact
System Location                   : Default Location
Logging Option                    : Console Logging
Login Authentication Mode         : Local
Config Save Status                : Successful
Remote Save Status                : Not Initiated
Config Restore Status             : Successful
Traffic Separation Control        : none
Serial Nums                       : 24302PC1M7DH
Loader Version                    : 01.00.03
Protocol Version                  : 2.03.474
MAC Address                       : bc:69:cb:2f:6b:ad
System Uptime                     : 3 days, 1 hours, 24 mins
Hardware Version                  : 1.0.0

XX-MUxxTPoE+#
```

3.50 show system utilization

This command displays the system utilization.

Syntax

- **show system utilization**

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to display system utilization.

```
XX-MUxxTPoE+# show system utilization
CPU Utilization:
usr                  : 7.92 %
nice                 : 0.00 %
sys                  : 14.85 %
idle                 : 77.23 %
iowait               : 0.00 %
irq                  : 0.00 %
soft                 : 0.00 %
steal                : 0.00 %
guest                : 0.00 %

Memory Utilization:
total                : 247 MB
used                 : 212 MB
free                 : 35 MB
shared               : 0 MB
buffers              : 0 MB
XX-MUxxTPoE+#
```

3.51 reboot

This command restarts the switch.

Syntax

- reboot

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

When you enter the **reboot** command, a reboot will be executed immediately. Please be aware that any unsaved configuration will be lost.

Example

This example shows how to reboot the switch.

```
XX-MUxxTPoE+# reboot
shutdown pana_cloud
Stop pana_cloud before reboot
XX-MUxxTPoE+#
```

3.52 reboot-flick

This command restarts the switch but not reset PoE.

Syntax

- reboot-flick

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

This command is used to update switch firmware without the powerdown of the PoE device such as a camera.

Example

This example shows how to reboot without PoE reset.

```
XX-MUxxTPoE+# reboot-flick
shutdown pana_cloud
Stop pana_cloud before reboot
XX-MUxxTPoE+#
```

3.53 restore-defaults

This command restores default configuration.

Syntax

- restore-defaults

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to restore the default configuration.

```
XX-MUxxTPoE+# restore-defaults
Would you reboot the device and restore to default config? <y/n>

Restore to default
shutdown pana_cloud
Stop pana_cloud before reboot

Factory Reset
XX-MUxxTPoE+#
```

3.54 restore-default-without-IP

This command restore default configuration without IP address.

Syntax

- restore-default-without-IP

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

In addition to the IP address, user name, password, VLAN, PVID, VLAN interface IP address, management VLAN, port name configured on the VLAN, and ARP information will also be maintained without being initialized.

Example

This example shows reset to factory default excluding IP address.

```
XX-MUxxTPoE+# restore-default-without-IP
Would you reboot the device and restore to default config without IP? <y/n>
shutdown pana_cloud
Stop pana_cloud before reboot
Building configuration ...
[OK]
------------------------------------------------------------------------------
  NIC probe (unit 0)
  L2Ntfy probe (unit 0): (found)
  Watchdog init (unit 0)
 watchdog_init had already been initialized!




XX-MUxxTPoE+ login:
```

3.55 show telnet server

This command displays the telnet server status.

Syntax

- show telnet server

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows status when the telnet server is enabled.

```
XX-MUxxTPoE+# show telnet server
telnet service enabled
XX-MUxxTPoE+#
```

3.56 show http server status

This command displays the http server status and HTTP port.

Syntax

- show http server status

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows the status when the HTTP(S) server is enabled.

```
XX-MUxxTPoE+# show http server status

HTTP server status              : Enabled
HTTP port is                    : 8080
HTTP Requests In                : 0
HTTP Invalids                   : 0
XX-MUxxTPoE+#
```

3.57 port speed - duplex

This command configures the speed and duplex operation.

Syntax

- speed { 10 | 100 | 1000 | 10000 } duplex { full | half }
- no speed
- no duplex

Parameters

Parameters	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.

Default

Speeds are automatically set on all ports.

Command Mode

Interface Configuration Mode.

Usage Guideline

Before you set port speed, disable the auto-negotiation function for a specific port by using no negotiation command.

Example

This example shows how to set the port speed to **1000Mbps** and **full-duplex** for port 8.

```
XX-MUxxTPoE+#configure terminal
XX-MUxxTPoE+(config)# interface gigabitethernet 0/8
XX-MUxxTPoE+(config-if)# no negotiation
XX-MUxxTPoE+(config-if)# speed 1000 duplex full
XX-MUxxTPoE+(config-if)#
```

3.58 extended-speed

This command enables extended speed on the port.

Syntax

- extended-speed

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

None.

Example

This example shows how to enable extended speed on port 8.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# interface gigabitethernet 0/8
XX-MUxxTPoE+(config-if)# extended-speed
XX-MUxxTPoE+(config-if)#
```

3.59 negotiation

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

Default

By default, this option is negotiation.

Command Mode

Interface Configuration Mode.

Usage Guideline

None.

Example

This example shows how to enable the auto-negotiation for port 8.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# interface gigabitethernet 0/8
XX-MUxxTPoE+(config-if)# negotiation
XX-MUxxTPoE+(config-if)#
```

3.60 set switch-name

This command sets the name of the switch.

Syntax

- **set switch-name <switchname>**

Default

By default, the system name is the product name (GA-MU8TPoE+, XG-MU24TPoE+, XG-MU24T).

Command Mode

Global Configuration Mode.

Usage Guideline

None.

Example

This example shows how to set the switch-name to **Test_Switch**.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# set switch-name Test_Switch
XX-MUxxTPoE+(config)#
```

3.61 set system description

This command configures the system description.

Syntax

- set system description <switchname>

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

Example

This example shows how to set the description for the switch.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# set system description EXAMPLE_SWITCH
XX-MUxxTPoE+(config)#
```

3.62 set ip http

This command enables/disables HTTP in the switch.

Syntax

- set ip http {enable | disable}

Parameters

Parameters	Description
enable	Enables HTTP in the switch.
disable	Disables HTTP in the switch.

Default

By default, this option is enable.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

Example

This example shows how to enable HTTP server function.

```
XX-MUxxTPoE+#configure terminal
XX-MUxxTPoE+(config)# set ip http enable
XX-MUxxTPoE+(config)#
```

3.63 ip telnet server

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

Default

By default, this option is ip telnet server.

Command Mode

Global Configuration Mode.

Usage Guideline

An IP address is required to establish a TELNET connection.
Before you connect the switch by TELNET, configuration an IP address.

Enable

This example shows how to enable the IP telnet server.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# ip telnet server
XX-MUxxTPoE+(config)# interface vlan 1
XX-MUxxTPoE+(config-vlan)# ip address 172.16.222.100 255.255.0.0
```

3.64 firmware upgrade

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>

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to update the switch firmware from a remote location using TFTP.

```
XX-MUxxTPoE+#  firmware upgrade tftp://172.16.2.100/PANASONIC-RTL83xx_fw_1.0.0-
2.03.09_20240726-1408.imag flash:fallback image 2
 ...Completed: 10 %, Time: 01:20(M:S) ...
 ...Completed: 20 %, Time: 01:20(M:S) ...
 ...Completed: 30 %, Time: 01:20(M:S) ...
 ...Completed: 40 %, Time: 01:20(M:S) ...
 ...Completed: 50 %, Time: 01:20(M:S) ...
 ...Completed: 60 %, Time: 01:20(M:S) ...
 ...Completed: 70 %, Time: 01:20(M:S) ...
 ...Completed: 80 %, Time: 01:20(M:S) ...
 ...Completed: 90 %, Time: 01:20(M:S) ...
BUG: soft lockup - CPU#0 stuck for 81s! [mtd_debug:3134]
Modules linked in: rtcore
Cpu 0
$ 0   : 00000000 7fa76158 48000000 08000000
$ 4   : b8001208 b8001208 00000001 000000b5
$ 8   : ffffffff 00151453 000000bc 05000000
$12   : 00000001 00000000 ffffffff 00401134
$16   : 40000000 02000000 01c30000 000000dc
$20   : 001f0000 8f4c9800 8f4c9620 8f505c80
$24   : 00000000 8011b454
$28   : 8f504000 8f505c38 8f505d00 80129bfc
Hi    : 00000000
Lo    : 000000b5
epc   : 80128b94 __spi_commands+0x3a4/0x13ec
    Not tainted
ra    : 80129bfc __get_spi_SR+0x20/0x30
Status: 10107c03    KERNEL EXL IE
Cause : 5080c000
PrId  : 00019070 (MIPS 4KEc)
% Firmware upgrade successful ..!!!
XX-MUxxTPoE+#
```

3.65 save

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**

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to save the running-config to startup-config.

```
XX-MUxxTPoE+# save
Building configuration ...
[OK]
XX-MUxxTPoE+#
```

3.66 copy startup-config

This command is used to copy the current startup-config of the switch to a remote directory using TFTP.

Syntax

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

Parameters

Parameters	Description
tftp://ip-address/filename	Configures the TFTP details for 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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to copy the startup-config file to tftp_server as test_startup_config.

```
XX-MUxxTPoE+# copy startup-config tftp://192.168.10.1/test_startup_config
current_config/SNCSR.conf
current_config/users
current_config/privil
current_config/passwd_j
magic number: 0x60d24600
header crc: 0xb8ba0d86
date: 2024/1/1 00:00
filesize: 47104
company:
Data crc: 0x7a15e439
version: 2.03.218
Module: IMG-2.03.474
Model: /####
```

3.67 copy

This command is used to download and copy the configuration file from a remote directory as the startup-config using TFTP.

Syntax

- copy {tftp://ip-address/filename} [startup-config]

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to download the configuration file **test_file** as startup-config of the switch from the IP address 192.168.10.1.

```
XX-MUxxTPoE+# copy tftp://192.168.10.1/test_file startup-config
 ...Completed: 30 %, Time: 08:20(M:S) ...
 ...Completed: 60 %, Time: 08:20(M:S) ...
total 1
drwxr-xr-x    4 root     root             0 Aug  8 14:43 .
drwxr-xr-x    3 root     root             0 Jan  1  1970 ..
drwxr-xr-x    3 root     root             0 Aug  8 14:44 current_config
-rw-r--r--    1 root     root            29 Jan  1  1970 debug_flag.txt
File Copied Successfully
XX-MUxxTPoE+#
```

3.68 show activepartition

This command displays the active image partition.

Syntax

- show activepartition

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to display active image partition.

```
XX-MUxxTPoE+# show activepartition

Acitivepartition is partition 1.

XX-MUxxTPoE+#
```

3.69 boot system

This command Set system boot image partition.

Syntax

- boot system { image1 | image2 }

Default

By default, this option is boot system image1.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to set the system boot image partition to image 2.

```
XX-MUxxTPoE+# boot system image2
Setup partition 2 as active
XX-MUxxTPoE+#
```

3.70 show current running-config

This command displays the currently operating configuration in the system.

Syntax

- show current running-config

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

The information displayed is so long that it is recommended to use other “show” commands.

Example

This example shows how to display the entire current running-config in the system.

```
XX-MUxxTPoE+# show current running-config

!

cli exec-timeout 60

snmp user "noAuthUser"

snmp group "iso" user "noAuthUser" security-model v1

snmp group "iso" user "noAuthUser" security-model v2c

snmp group "noAuthUser" user "noAuthUser" security-model v3

snmp access "iso" v1 read "iso" write "iso" notify "iso"

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
interface port-channel 6

vlan_trunk port disable

!

interface port-channel 7

vlan_trunk port disable

!

interface port-channel 8

vlan_trunk port disable

!

set controller disable

!

wired client list enable


end
```

3.71 ip http port

This command set the HTTP port.

Syntax

- ip http port <port-number(1-65535)>

Parameters

Parameters	Description
<port-number(1-65535)>	HTTP port.

Default

By default, this option is 80 ports.

Command Mode

Global Configuration Mode.

Usage Guideline

When you change the HTTP port number, it is recommended to restart the HTTPS server function by using the **no ip http server** command followed by the **ip http server** command in chapter **2.2.4.**

Example

This example shows how to set the HTTP port number to **80**.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# ip http port 80

HTTP port number will take effect only when HTTP is disabled and enabled again.
XX-MUxxTPoE+(config)#
```

3.72 ip http session-idle-timeout

This command set the HTTP session timeout (in minutes) for line disconnection.

Syntax

- ip http session-idle-timeout <minutes(0-10000)>

Parameters

Parameters	Description
<minutes(0-10000)>	EXEC timeout value(in minutes)

Default

By default, this option is 0 minutes.

Command Mode

Global Configuration Mode.

Usage Guideline

When you change the HTTP port number, it is recommended to restart the HTTPS server function by using the **no ip http server** command followed by the **ip http server** command in chapter **2.2.4.**

Example

This example shows how to set the HTTP session timeout to 60 minutes.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# ip http session-idle-timeout 60

HTTP session timeout will take effect only when HTTP is disabled and enabled again
XX-MUxxTPoE+(config)#
```

3.73 cli exec-timeout

This command sets the default EXEC timeout (in minutes) for line disconnection.

Syntax

- cli exec-timeout <minutes (0-10000)>

Parameters

Parameters	Description
<minutes(0-10000)>	EXEC timeout value(in minutes)

Default

By default, this option is 30 minutes.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

Example

This example shows how to set the period of CLI EXEC timeout to 60 minutes.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# cli exec-timeout 60
XX-MUxxTPoE+(config)#
```

3.74 no shutdown switch-instance-shared-port

This command starts Switch Instance Shared PortFeature(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

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

Example

This example shows how to start SISP in the switch.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# no shutdown switch-instance-shared-port
XX-MUxxTPoE+(config)#
```

3.75 ping

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)]

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to send the ping to **192.168.10.100** with 3 repetitions, a size of 1024 bytes, and a timeout of 3 seconds.

```
XX-MUxxTPoE+# ping 192.168.10.100 repeat 3 size 1024 timeout 3

ping 192.168.10.100 :
Reply Received From :192.168.10.100, TimeTaken : <1 msecs
Reply Received From :192.168.10.100, TimeTaken : 10 msecs
Reply Received From :192.168.10.100, TimeTaken : 20 msecs

--- 192.168.10.100 Ping Statistics ---
3 Packets Transmitted, 3 Packets Received, 0% Packets Loss

XX-MUxxTPoE+#
```

3.76 traceroute

This command traces route to the destination.

Syntax

- traceroute {<ip-address>| hostname | ipv6 <prefix>} [max-ttl <value (2-255)>]

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to display the route to the IP address 192.168.10.1.

```
XX-MUxxTPoE+# traceroute 192.168.10.1
Tracing Route to 192.168.10.1 with 15 hops max and 1 byte packets
[!N - Network Unreachable !H - Host Unreachable !P - Protocol Unreachable]

  1     192.168.10.1       11 ms           11 ms           11 ms
XX-MUxxTPoE+#
```

3.77 show device temperature

This command displays current device temperature.

Syntax

- show device temperature

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to display the temperature of the switch.

```
XX-MUxxTPoE+# show device temperature
Sensor local temperature   : 43 °C
Sensor remote temperature   : 40 °C
XX-MUxxTPoE+#
```

3.78 free

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**

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

The contents of each item are as follows.

name	mean
total	The size of physical memory on the switch.
used	The amount of memory used by the system.
free	The amount of memory not used by anything.
shared	The amount of shared memory used by tmpfs.
buffers	The amount of memory used by buffers.
Swap	The amount of virtual memory created on the storage device when the memory runs out.

Example

This example shows how to display the detailed report on the system's memory usage.

```
XX-MUxxTPoE+# free
             total         used         free       shared      buffers
Mem:        253488       217260        36228            0            0
-/+ buffers:             217260        36228
Swap:            0            0            0

XX-MUxxTPoE+#
```

3.79 mpstat

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

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

The contents of each item are as follows.

name	mean
CPU	Logical CPU id :ALL
%usr	CPU usage at the user level such as the application.
%nice	CPU usage for applications with a specified process scheduling priority referred to as “nice value”.
%sys	CPU usage at the system level such as the kernel
%iowait	Idle time waiting for disk I/O requests.
%irq	CPU usage for handling hardware interrupts.
%soft	CPU usage for handling software interrupts.
%steal	CPU usage for handling hypervisor tasks for other virtual CPUs.
%guest	CPU usage for virtual CPU tasks.
%idle	Idle time excluding the time spent waiting for disk I/O requests.

Example

This example shows how to display the processor statistics.

```
XX-MUxxTPoE+# mpstat

Linux 2.6.32.58 ((none))        08/08/24        _mips_   (1 CPU)

18:14:59   CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest   %idle
18:14:59   all    6.29    0.00    3.76    0.00    0.00    0.00    0.00    0.00   89.94
XX-MUxxTPoE+#
```

3.80 clock utc-offset

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

Parameters

Parameters	Description
+/-	Sets the client time zone as after or before UTC. Plus indicates forward time zone and minus indicates backward time 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

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

Example

This example shows how to set the clock to IST(UTC +05:30)

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# clock utc-offset +05:30
XX-MUxxTPoE+(config)#
```

3.81 show clock properties

This command displays the primary system clock properties.

Syntax

- **show clock properties**

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows the system NTP clock when the clock is set to IST(UTC +05:30).

```
XX-MUxxTPoE+# show clock properties

 System Clock Information
 ------------------------
 Variance : 0
 Class    : 248
 Accuracy : Unknown
 Source   : NTP
 Offset   : +05:30 (UTC)
 HoldOver : Enabled

Clock NOT in sync with time source

XX-MUxxTPoE+#
```

3.82 debug show tech-support

This command to display the information required by the technical support personnel.

Syntax

- show clock properties

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

To interrupt the display on the screen, please press “Shift + Q”

Example

This command shows how to display technical information.

```
XX-MUxxTPoE+#debug show tech-support

#-------------------------------------------------------------------------------
#8-Port Gigabit L2+ Managed PoE+ Switch with 2 Gigabit Uplink Ports and 2 SFP Slots
#                          Technical Support Information
#
#                            Firmware: Build V2.03.09
#                Copyright(C) 2024 Panasonic. All rights reserved.
#-------------------------------------------------------------------------------
*****************************   clock information   *****************************

 Thu Aug 01 23:45:67 2024

 System Clock Information
 ------------------------
 Variance : 0
 Class    : 248
 Accuracy : Unknown
 Source   : NTP
 Offset   : +05:30 (UTC)
 HoldOver : Enabled

Clock NOT in sync with time source


================================================================================
================================================================================


#-------------------------------------------------------------------------------
#             End of Technical Support Information for <XX-MUxxTPoE+>
#-------------------------------------------------------------------------------
XX-MUxxTPoE+#
```

3.83 show system fan status

This command displays the cooling fan status information.

Syntax

- show system fan status

Parameters

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to display the status of fans.

```
XX-MUxxTPoE+# show system fan status

System Fan Status: OK
XX-MUxxTPoE+#
```

3.84 Temperature Tolerance Mode

This command limits the maximum power supply capacity to allow PoE power delivery even in a 60 degrees Celsius.

Syntax

- **temperature tolerance mode {disable | enable}**

Parameters

Parameters	Description
disable	Disables Temperature Tolerance Mode.
enable	Enables Temperature Tolerance Mode.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode

Usage Guideline

The setting status of Temperature Tolerance Mode (disabled/enabled) can be checked using the "show power detail" command.

Example

This is an example when the Temperature Tolerance Mode is enabled.

```
XX-MUxxTPoE+(config)# temperature tolerance mode enable

Temperature tolerance mode is enabled
Power budget is limited to prevent overheating
XX-MUxxTPoE+(config)#
```

This is an example when the Temperature Tolerance Mode is disabled.

```
XX-MUxxTPoE+(config)# temperature tolerance mode disable

Temperature tolerance mode is disabled
Power budget is set to full (130 watts)
XX-MUxxTPoE+(config)#
```

4 EEE

4.1 eee

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

Default

By default, this option is no eee.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

4.2 show eee

This command displays the Energy Efficient Ethernet information of each port.

Syntax

- show eee

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

5 Secure Sockets Layer (SSL) Commands

5.1 show ip http secure server status

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

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

5.2 show ip http session-idle-timeout

This command displays web session timeout value.

Syntax

- show ip http session-idle-timeout

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

5.3 ip http secure server

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

Default

By default, this option is no ip http secure server.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

6 PoE (Power over Ethernet) Commands

6.1 set poe global power threshold

This command modifies Power over Ethernet(PoE) module global power budget in the switch.

Syntax

- set poe global power threshold <value>

Default

By default, the GA-MU8TPoE+ power threshold value is 130 W.
By default, the XG-MU24TPoE+ power threshold value is 410 W.

Command Mode

Global Configuration Mode.

Usage Guideline

This command is used to set the maximum power capacity for entire the switch. The unit for setting is watts(W).

Example

This example shows how to set the PoE module global power budget in switch to 65W.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# set poe global power threshold 65
XX-MUxxTPoE+(config)#
```

6.2 power inline

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 }

Default

By default, this option is enable.

Command Mode

Interface Configuration Mode.

Usage Guideline

By using the interface range configuration mode, you can configure multiple ports at once.

Example

This example shows how to disable power delivery through PoE for port 4.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# interface gigabitethernet 0/4
XX-MUxxTPoE+(config-if)# power inline disable
XX-MUxxTPoE+(config-if)#
```

6.3 power inline limit

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> }

Parameters

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.

Default

By default, this option is auto.

Command Mode

Interface Configuration Mode

Usage Guideline

The power limit must be less than 31 watt.
By using the interface range configuration mode, you can configure multiple ports at once.

Example

This example shows how to set the maximum amount of provide power on port 7 to 20W.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# interface gigabitethernet 0/7
XX-MUxxTPoE+(config-if)# power inline limit 20
XX-MUxxTPoE+(config-if)#
```

6.4 power inline priority

This command sets the priority of the Power Over Ethernet on the specified port.

Syntax

- power inline priority {critical | high | medium | low}

Parameters

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.

Default

By default, this option is medium.

Command Mode

Interface Configuration Mode.

Usage Guideline

By using the interface range configuration mode, you can configure multiple ports at once.
This command can't be set on ports without PoE enabled.

Example

This example shows how to set the priority of PoE on port 1 to **critical** and port 3 to **low.**

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# interface gigabitethernet 0/1
XX-MUxxTPoE+(config-if)# power inline priority critical
XX-MUxxTPoE+(config-if)# exit
XX-MUxxTPoE+(config)# interface gigabitethernet 0/3
XX-MUxxTPoE+(config-if)# power inline priority low
XX-MUxxTPoE+(config-if)#
```

6.5 show power detail

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

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

This command is used to display the PoE power supply status information.

Example

This example shows how to display the power supply status of PoE.

```
XX-MUxxTPoE+#show power detail

PSE Status
----------
PoE Global Admin State : Enabled
Temperature Tolerance Mode : Disabled
PSE Oper Status        : On
Max Power Supply       : 130 (watts)
Total Power Budget     : 65  (watts)
Total Power Consumed   : 1.2 (watts)

XX-MUxxTPoE+#
```

6.6 show power inline

This command displays the Power Over Ethernet power supply status information of each pse.

Syntax

- show power inline [{<interface-type> <interface-id>}]

Parameters

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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

This command is used to display the PoE power supply status information of each pse.
To display the status of all ports once, send the command without parameters.

Example

This example shows how to display the power supply status for each port.

```
XX-MUxxTPoE+# show power inline

PoE Port Info
-------------

Port  State  Priority   Power Limit Type   Status               Class   Voltage(V)  Current(mA)  Power(W)
----  -----  --------  ------------------ --------------------- ------  ----------  -----------  ----------
1      up     critical  Auto Class         Delivering            3       53.8        20           1.1
2      up     medium    Auto Class         Searching             -       0.0         0            0.0
3      up     low       Auto Class         Searching             -       0.0         0            0.0
4      down   medium    Auto Class         Disabled              0       0.0         0            0.0
5      down   medium    Auto Class         Disabled              0       0.0         0            0.0
6      down   medium    Auto Class         Disabled              0       0.0         0            0.0
7      up     medium    User defined 20(W) Searching             -       0.0         0            0.0
8      up     medium    Auto Class         Searching             -       0.0         0            0.0

XX-MUxxTPoE+#
```

7 SSH (Secure Shell) Commands

7.1 show ssh-configurations

This command displays the SSH server listening IP address and port information.

Syntax

- show ssh-configurations

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

This command is used to generate the RSA or DSA key pair.

7.2 ip ssh server

This command enables the ssh system. The no form of the command disables the ssh system.

Syntax

- ip ssh server
- no ip ssh server

Default

By default, this option is ip ssh server.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

8 PD(Powered Device) Lifeguard Commands

8.1 set pdlg

This command enables/disables PD Lifeguard module in the switch.
PD Lifeguard can switch the power supply to the port ON/OFF automatically using monitoring methods such as Ping and LLDP.

Syntax

- set pdlg {enable | disable}

Default

By default, this option is disable.

Command Mode

Global Configuration Mode.

Usage Guideline

This command is used to set the global configuration of PD Life Guard.

Example

This example shows how to enable PD Lifeguard on whole switch.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# set pdlg enable
XX-MUxxTPoE+(config)#
```

8.2 set pdlg port

This command enables/disables PD Lifeguard module on the specified port.

Syntax

- set pdlg port <integer(1-48)> {enable | disable}

Default

By default, this option is enable.

Command Mode

Global Configuration Mode.

Usage Guideline

This command is used to set the PD Lifeguard module on the specified port. By using the disable this option, you can achieve efficient power allocation.

Example

This example shows how to enable PD Lifeguard on port 1.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# set pdlg port 1 enable
XX-MUxxTPoE+(config)#
```

8.3 set pdlg port - mode

This command selects PD Lifeguard mode on the specified port.

Syntax

- set pdlg port <integer(1-48)> mode { auto | force-ping }

Parameters

Parameters	Description
auto	PD reachability is judged by LLDP packet (priority) or ping IP test.
force-ping	PD reachability is judged via ping IP test.

Default

By default, this option is auto.

Command Mode

Global Configuration Mode.

Usage Guideline

This command is used to select the monitoring method of PD Lifeguard.

Example

This example shows how to set PD Lifeguard mode into “force-ping” mode on port 1.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# set pdlg port 1 mode force-ping
XX-MUxxTPoE+(config)#
```

8.4 set pdlg port - ping ip

This command sets PD Lifeguard ping IP Address on the specified port.

Syntax

- set pdlg port <integer(1-48)> ping ip <ucast_addr>

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

This command is used to set the PD Lifeguard monitoring configuration using Ping.

Example

This example shows how to set PD Lifeguard ping IP address on port 1.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# set pdlg port 1 ping ip 192.168.100.254
XX-MUxxTPoE+(config)#
```

8.5 set pdlg port - ping interval

This command sets PD Lifeguard ping IP Interval on the specified port.

Syntax

- set pdlg port <integer(1-48)> ping interval <integer(1-3600)>

Default

By default, the ping interval value is 10.

Command Mode

Global Configuration Mode.

Usage Guideline

This command is used to set the PD Lifeguard monitoring interval using Ping.

Example

This example shows how to set PD Lifeguard ping interval on port 3 to 60 seconds.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# set pdlg port 3 ping interval 60
XX-MUxxTPoE+(config)#
```

8.6 set pdlg port - ping max-try

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)>

Default

By default, the ping max-try value is 30.

Command Mode

Global Configuration Mode.

Usage Guideline

This command is used to set the maximum retries of PD Lifeguard using Ping. Ping timeout count exceeds the maximum Ping count, the device determines the PD device is non-functional and attempts to reboot automatically.

Example

This example shows how to set the maximum count of PD Lifeguard ping to 10 on port 1.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# set pdlg port 1 ping max-try 10
XX-MUxxTPoE+(config)#
```

8.7 set pdlg port - reboot interval

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)>

Default

By default, the reboot interval value is 300.

Command Mode

Global Configuration Mode.

Usage Guideline

This command is used to set the interval for toggling power ON and OFF for the PD Lifeguard.
If the reboot of the PD device does not go smoothly, the interval should be adjusted.

Example

This example shows how to set the PD Lifeguard reboot interval to 300 on port 2.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# set pdlg port 2 reboot interval 300
XX-MUxxTPoE+(config)#
```

8.8 set pdlg port - reboot max-try

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)>

Default

By default, the ping max-try value is 3.

Command Mode

Global Configuration Mode.

Usage Guideline

This command is used to set the maximum number of times the PD Lifeguard can repeatedly reboot the PD device.

Example

This example shows how to set the maximum counts of PD Lifeguard reboot to 3 on port 4.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# set pdlg port 4 reboot max-try 3
XX-MUxxTPoE+(config)#
```

8.9 set pdlg port - reboot refresh

This command resets PD Lifeguard reboot retry count on the specified port.

Syntax

- set pdlg port <integer(1-48)> reboot refresh

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

When the number of reboot retries reaches “reboot max-try”, the pdlg reboot function is temporarily suspended.
So please initialize the reboot try count using this command.

Example

This example shows how to reset the reboot retry count on port 3.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# set pdlg port 3 reboot refresh
XX-MUxxTPoE+(config)#
```

8.10 set pdlg port - reboot

This command sets PD Lifeguard reboot allowed or denied on the specified port.

Syntax

- set pdlg port <integer(1-48)> reboot {allow | deny}

Parameters

Parameters	Description
allow	allow reboot (reboot + system log).
deny	deny reboot (system log only).

Default

By default, this option is allow.

Command Mode

Global Configuration Mode.

Usage Guideline

This command is used to set the behavior when the switch determines that the PD device is non-functional on the specified port.

Example

This example shows how to configure the PD Lifeguard reboot on port 5 to deny.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# set pdlg port 5 reboot deny
XX-MUxxTPoE+(config)#
```

8.11 set pdlg port - pd-boot-time

This command sets PD Lifeguard PD boot up time on the specified port.

Syntax

- set pdlg port <integer(1-48)> pd-boot-time <integer(50-1200)>

Parameters

Parameters	Description
set pdlg port <integer(1-48)> 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)

Default

By default, the pd-boot-time value is 300.

Command Mode

Global Configuration Mode.

Usage Guideline

This command is used to set the boot up time on the specified port.

Example

This example shows how to set PD boot up time on port 6 to 600 seconds.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# set pdlg port 6 pd-boot-time 600
XX-MUxxTPoE+(config)#
```

8.12 show pdlg port

This command shows PD Lifeguard per port status.

Syntax

- show pdlg port <integer(1-48)>

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

This command is used to display the status of PD Lifeguard on the specified port.

Example

This example shows how to display the pdlg settings for port 1.

```
XX-MUxxTPoE+# show pdlg port 1

PD Lifeguard Status for port 1:
Global Status : Enabled
Port Status   : Enabled
Port Mode     : Force Ping
Auto Camera Lifeguard(ACLG) : Enabled
Power Status  : Not Delivering
LLDP Status   : Not Working
Mac Address   : None
IP Address    : 192.168.100.254(Specified. Invalid to ping/Unused)
Ping Max Count: 10(Will ping 10 more time(s) before reboot)
Ping Interval : 60
Action Type   : Reboot with Syslog
Reboot Max Retry Count         : 3(Has rebooted 0 time(s))
Reboot Recovery Interval       : 10 s
PD Boot Up Time                : 50 s
ACLG/LLDP Expiry Pending Time : 30 s

----------End----------

XX-MUxxTPoE+#
```

8.13 show pdlg detail

This command shows PD Lifeguard status in detail.

Syntax

- show pdlg detail

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

This command is used to display the details of PD Lifeguard status.

Example

This example shows how to display the pdlg status in detail.

```
XX-MUxxTPoE+# show pdlg detail


PD Lifeguard Status
-----------------------------
Global Status Enabled
-----------------------------
Delivering Port:
Port      Status     Mode       LLDP Working     ACLG/Working        MAC Address              Ping IP
8         Enabled    Force Ping      No      No(ONVIF disabled)    00:1A:2B:3C:4E:5D  172.16.2.173(Manual)Ping IP

Action Taken
,reboot and syslog.
-----------------------------

PD Lifeguard Config End
XX-MUxxTPoE+#
```

9 Link Aggregation Commands

9.1 no shutdown port-channel

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.

Syntax

- no shutdown port-channel

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

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.

9.2 lacp system-priority

This command configures the LACP priority associated with actor's system ID.

Syntax

- lacp system-priority <short(0-65535)>
- no lacp system-priority

Default

By default, the port-priority value is 32768.

Command Mode

Global Configuration Mode.

Usage Guideline

The switch with the lowest LACP decides the standby and active links in the LA.

9.3 port-channel load-balance

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}

Parameters

Parameters	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.

Parameters	description
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.

Default

By default, the port-channel load-balancing is src-dst-mac.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

9.4 channel-group

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

Parameters

Parameters	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.

Parameters	description
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 - Assign the interface to channel-group statically without LACP negotiate.

Default

By default, the port-channel is no channel-group.

Command Mode

Interface Configuration Mode (Physical Interface Mode)
This command is applicable in PORT Interface Mode.

Usage Guideline

Some settings that can be configured on physical ports are disabled when the physical port joins a channel-group.

Example

This command shows how to assign port 2 to channel-group 1, and statically enable the logical group.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# interface gigabitethernet 0/2
XX-MUxxTPoE+(config-if)# channel-group 1 mode on
XX-MUxxTPoE+(config-if)#
```

9.5 lacp timeout

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

Parameters

Parameters	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.

Default

By default, the lacp timeout is long.

Command Mode

Interface Configuration Mode (Physical Interface Mode)
This command is applicable in VLAN Interface Mode.

Usage Guideline

None.

9.6 show etherchannel

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}]

Parameters

Parameters	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.

Parameters	description
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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

10 Mirror Commands

10.1 monitor session - destination

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]

Parameters

Parameters	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.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

If you only set the **monitor session - destination** command it will not be displayed in the **show current running-config**.
Please configure it together with the **monitor session - source command**.

Example

This example shows the procedure for mirroring traffic from port 1 to port 2.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# monitor session 1 destination interface gigabitethernet 0/2
XX-MUxxTPoE+(config)# monitor session 1 source interface gigabitethernet 0/1
XX-MUxxTPoE+(config)#
```

10.2 monitor session - source

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}]}}

Parameters

Parameters	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.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

If you only set the **monitor session - source** command it will not be displayed in the **show current running-config**.
Please configure it together with the **monitor session - destination command**.

Example

This example shows the procedure for mirroring traffic from port 1 to port 2.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# monitor session 1 destination interface gigabitethernet 0/2
XX-MUxxTPoE+(config)# monitor session 1 source interface gigabitethernet 0/1
XX-MUxxTPoE+(config)#
```

10.3 no monitor session

This command is used to remove the mirroring configuration.

Syntax

- no monitor session {session-id (1-3)}

Parameters

Parameters	Description
session-id	Specifies the ID of mirroring session to be deleted in the range from 1 to 3.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

10.4 show monitor

This command displays the mirroring information present in the system.

Syntax

- show monitor { session <session-id (1-3)> | all } [detail]

Parameters

Parameters	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.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

11 STP (Spanning Tree Protocol) Commands

11.1 spanning-tree

This command enables the spanning tree operation in the switch for the selected spanning tree Mode. 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.

Syntax

- spanning-tree
- no spanning-tree

Default

By default, this option is no spanning-tree.

Command Mode

Global Configuration Mode.

Usage Guideline

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 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.

11.2 spanning-tree mode

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}

Parameters

Parameters	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.

Default

By default, this mode is mst.

Command Mode

Global Configuration Mode.

Usage Guideline

- The spanning-tree mode setting is mutually exclusive, meaning you can configure either mst or rst, but not both at the same time.
- If spanning-tree mode mst is configured, any command intended for rst will be automatically converted and applied as an mst command.
- When switching from spanning-tree mode mst to rst, any values previously modified under mst will not be carried over; instead, the default values for rst will be applied.

11.3 spanning-tree transmit hold-count

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.

Syntax

- spanning-tree transmit hold-count <value (1-10)>
- no spanning-tree transmit hold-count

Parameters

Parameters	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.

Default

By default, this value is 6 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

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.

11.4 spanning-tree forward-time

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.

Syntax

- spanning-tree forward-time <seconds(4-30)>
- no spanning-tree forward-time

Default

By default, value of the forward-time is 15 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

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.

11.5 spanning-tree max-age

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.

Syntax

- spanning-tree max-age <seconds(6-40)>

- no spanning-tree max-age

Default

By default, value of the max-age is 20 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

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.

11.6 spanning-tree hello-time

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

Default

By default, value of the hello-time is 2 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

11.7 spanning-tree mst forward-time

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.

Syntax

- spanning-tree mst forward-time <seconds(4-30)>
- no spanning-tree mst forward-time

Default

By default, value of the forward-time is 15 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

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.

11.8 spanning-tree mst max-age

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.

Syntax

- spanning-tree mst max-age <seconds(6-40)>
- no spanning-tree mst max-age

Default

By default, value of the max-age is 20 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

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.

11.9 spanning-tree mst hello-time

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 mst hello-time<value(1-2)>
- no spanning-tree mst hello-time

Default

By default, value of the hello-time is 2 seconds.

Command Mode

Global Configuration Mode / PORT Interface Mode.

Usage Guideline

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.

11.10 clear spanning-tree counters

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

Syntax

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

Parameters

Parameters	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.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

11.11 spanning-tree priority

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.

Syntax

- spanning-tree [mst <instance-id>] priority <value(0-61440)>
- no spanning-tree [mst <instance-id(1-64)>] priority

Parameters

Parameters	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.

Default

By default, this value is 32768.

Command Mode

Global Configuration Mode.

Usage Guideline

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.

11.12 spanning-tree mst max-instance

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.

Syntax

- spanning-tree mst max-instance <short(1-64)>
- no spanning-tree mst max-instance

Default

By default, this option value is 4.

Command Mode

Global Configuration Mode.

Usage Guideline

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.

11.13 spanning-tree mst root

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.

Syntax

- spanning-tree mst {instance-id <instance-id(1-64)>} root {primary | secondary}
- no spanning-tree mst {instance-id <instance-id(1-64)>} root

Parameters

Parameters	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.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

This command executes only if

- instance is created
- spanning tree Mode is set as mst.

11.14 spanning-tree mst configuration

This command enters into MSTP configuration Mode, where instance specific and MST region configuration can be done.

Syntax

- spanning-tree mst configuration

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

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.

11.15 name

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

Default

By default, this option is Device MAC address.

Command Mode

MSTP Configuration Mode.

Usage Guideline

None.

11.16 revision

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

Parameters

None.

Default

By default, this value is 0.

Command Mode

MSTP Configuration Mode.

Usage Guideline

None.

11.17 instance

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>]

Default

By default, this instance value is 1.
By default, vlan mapped are 1-1024, 1025-2048, 2049-3072, 3073-4094.

Command Mode

MSTP configuration Mode.

Usage Guideline

None.

11.18 spanning-tree auto-edge

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.

Syntax

- spanning-tree auto-edge
- no spanning-tree auto-edge

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

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

11.19 spanning-tree - Properties of an interface

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.

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}]

Parameters

Parameters	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

Default

By default, value of the cost is 0.
By default, the link-type is no spanning-tree link-type.
By default, value of the port-priority is 128.
By default, the portfast is no spanning-tree portfast.

Command Mode

Interface Configuration Mode.

Usage Guideline

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.

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

11.20 spanning-tree mst- Properties of an interface for MSTP

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.

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}

Parameters

Parameters	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.

Default

By default, value of the cost is 20000.
By default, value of the port-priority is 128.

By default, this option is disable.

Command Mode

Interface Configuration Mode.

Usage Guideline

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

11.21 show spanning-tree - Summary,Blockedports, Pathcost

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.

Syntax

- **show spanning-tree [{ summary | blockedports | pathcost method }] [switch <context_name>]**

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

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.

11.22 show spanning-tree detail

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.

Syntax

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

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

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.

11.23 show spanning-tree active

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.

Syntax

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

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

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.

11.24 show spanning-tree interface

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.

Syntax

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

Parameters

Parameters	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.

Parameters	Description
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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

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.

11.25 show spanning-tree root

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.

Syntax

- **show spanning-tree root [{ address | cost | forward-time | id | max-age | port | priority | detail }] [switch <context_name>]**

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

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.

11.26 show spanning-tree bridge

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.

Syntax

- show spanning-tree bridge [{ address | forward-time | hello-time | id | max-age | protocol | priority | detail }] [switch <context_name>]

Parameters

Parameters	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 root 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 root priority, address, maximum age time and forward delay time for the bridge.
switch <context_name>	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

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.

11.27 show spanning-tree mst - CIST or specified mst Instance

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.

Syntax

- show spanning-tree mst [<instance-id(1-64 | 4094)>] [detail] [switch <context_name>]

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

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.

11.28 show spanning-tree mst configuration

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.

Syntax

- show spanning-tree mst configuration [switch <context_name>]

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

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.

11.29 show spanning-tree mst - Port Specific Configuration

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.

Syntax

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

Parameters

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

Parameters	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.
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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

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.

12 LBD(Loop back Detection) Commands

12.1 lbd

This command enables/disables loop back detection on whole devices.

Syntax

- lbd { enable | disable }

Default

By default, this option is enable.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

12.2 lbd ports

This command enables/disables the loop back detection(lbd) on specified ports or all ports.

Syntax

- lbd ports {<port_list> | all} {enable | disable}

Parameters

Parameters	Description
<port_list>	A collection of specific ports where LBD can be turned on or off.
all	Indicates that the command is applicable to every port.
enable	Turns on loop back detection for the specified ports.
disable	Turns off loop back detection for the specified ports.

Default

By default, all ports are disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

Example

This example shows how to enable the loop back detection on ports 1 to 6.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# lbd ports 1-6 enable
XX-MUxxTPoE+(config)#
```

And shows how to disable it on all ports.

```
XX-MUxxTPoE+#configure terminal
XX-MUxxTPoE+(config)# lbd ports all disable
XX-MUxxTPoE+(config)#
```

12.3 lbd interval_time/lbd lbd_recover_time

This command configures the loop back detection timing and recovery timing.

Syntax

- **lbd interval_time <short(1-32767)>**
- **lbd lbd_recover_time {none | <short(60-10000)>}**

Parameters

Parameters	Description
<short(1-32767)>	Configure the interval time for LBD checks in seconds. Acceptable values range from 1 to 32767.
none	when the **none** is set, disable automatic recovery from loop conditions.
<short(60-10000)>	Configure the recovery time after a loop occurs. Sets the recovery time in seconds, with a range of 60 to 10000.

Default

By default, the **interval_time** is configured to 2 seconds and the recover time is configured to 60 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

When the **lbd neverRecover** feature is enabled, this setting has no effect.
In the event of manual recovery, please execute the **no shutdown** command on the relevant port.

Example

This example shows how to set the interval time for LBD checks to 30 seconds.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# lbd interval_time 30

Success!
XX-MUxxTPoE+(config)#
```

And shows how to configure a recovery time of 600 seconds.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# lbd lbd_recover_time 600

Success!
XX-MUxxTPoE+(config)#
```

12.4 lbd neverRecover

This command enable/disable **lbd neverRecover** feature.
The feature prevents from the automatic recovering from a loop condition.

Syntax

- **lbd neverRecover {enable | disable}**

Parameters

Parameters	Description
enable	When **enable** is set, automatic recovery of ports that detect a loop will no longer occur.
disable	When **disable** is set, ports that detect a loop will automatically recover.

Default

By defaults, **lbd neverRecover** feature is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

When the **lbd neverRecover** feature is enabled, ports that detect a loop must be manually recovered.

Example

This example shows how to disable the **lbd neverRecover** feature.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# lbd neverRecover disable
XX-MUxxTPoE+(config)#
```

12.5 show lbd state

This command displays the loop back detection information.

Syntax

- show lbd state

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

12.6 show lbd port state

This command displays the loop back detection information of each port.

Syntax

- show lbd port state

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

13 MAC Address Table Commands

13.1 mac-address-table static unicast

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>

Parameters

Parameters	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.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

13.2 mac-address-table aging-time

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

Default

By default, this value is 300 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

13.3 clear mac-address-table dynamic

This command to delete a specific dynamic MAC address, all dynamic MAC addresses for a specific interface, all dynamic MAC addresses for a specific VLAN, or all dynamic MAC addresses for a MAC address table.

Syntax

- clear mac-address-table dynamic { interface {port-channel <port-channel-id (1-65535)> | <interface-type> <interface-id>} | vlan <vlan_vfi_id> | mac-address <HH:HH:HH:HH:HH:HH> | all }

Parameters

Parameters	description
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. • port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
vlan <vlan_vfi_id>	Configures the static unicast destination MAC address for the specified VLAN. This value ranges between 1 and 4094.
<vlan_vfi_id>	VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094
mac-address <HH:HH:HH:HH:HH:HH>	Deletes the specified dynamic MAC address.
all	Clear all dynamic MAC addresses.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

13.4 show mac-address-table

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)>}]

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

13.5 show mac-address-table count

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)>]

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

13.6 show mac-address-table static multicast/ unicast

This command displays the static multicast/unicast MAC address entries created in the FDB table.

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>}]

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

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.

13.7 show mac-address-table dynamic unicast

This command displays all dynamically learnt unicast entries from the MAC address table.

Syntax

- **show mac-address-table dynamic unicast [vlan <string(9)>] [address <ucast_mac>] [{interface <interface-type> <ifnum> | switch <string(32)>}]**

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

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.

13.8 show mac-address-table aging-time

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)>]

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

13.9 show dot1d mac-address-table

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.

Syntax

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

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

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

13.10 show dot1d mac-address-table static multicast

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

Syntax

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

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

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.

13.11 show dot1d mac-address-table static unicast

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

Syntax

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

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

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.

14 LLDP (Link Layer Discovery Protocol) Commands

14.1 set lldp

This command transmits or receives LLDP frames from the server to the LLDP module.

Syntax

- set lldp {enable | disable}

Parameters

Parameters	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.

Default

By default, this option is enable.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

14.2 set lldp version

This command enables the lldp version to be used on the system.

Syntax

- set lldp version {v1 | v2}

Parameters

Parameters	Description
v1	Enables LLDP 2005 version 1 on the port.
v2	Enables LLDP 2009 version 2 on the port.

Default

By default, this option is set lldp version v2.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

14.3 lldp transmit-interval

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.

Syntax

- lldp transmit-interval <seconds(5-32768)>
- no lldp transmit-interval

Default

By default, this value is 30 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

The no form of the command sets the transmission interval to the default value.

14.4 lldp holdtime-multiplier

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.

Syntax

- lldp holdtime-multiplier <value(2-10)>
- no lldp holdtime-multiplier

Default

By default, this value is 4 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

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.

14.5 lldp reinitialization-delay

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

Default

By default, this value is 2 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

14.6 lldp tx-delay

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.

Syntax

- lldp tx-delay <seconds(1-8192)>
- no lldp tx-delay

Default

By default, this value is 2 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

TxDelay should be less than or equal to (0.25 * Message Tx Interval).

14.7 show lldp

This command displays LLDP global configuration details to initialize on an interface.

Syntax

- show lldp

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

14.8 show lldp interface

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

Syntax

- show lldp interface [<interface-type> <interface-id>] [mac-address <mac_addr>]

Parameters

Parameters	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.

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

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

14.9 show lldp neighbors

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>][detail]

Parameters

Parameters	Description
chassis-id <string(255)>	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.
port-id <string(255)>	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.
port-id <string(255)>	Displays information about neighbors for the specified destination MAC address of the LLDP agent.

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

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

14.10 show lldp local

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]}

Parameters

Parameters	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.

Parameters	Description
<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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

14.11 show lldp peers

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]]

Parameters

Parameters	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.

Parameters	Description
<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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

15 IGMP (Internet Group Management Protocol) Snooping Commands

15.1 ip igmp querier-timeout

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. his 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>

Default

By default, this value is 125 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

15.2 snooping multicast-forwarding-mode

This command specifies the snooping multicast forwarding mode (IP based or MAC based).

Syntax

- snooping multicast-forwarding-mode {ip}

Parameters

Parameters	Description
ip	Configures the multicast forwarding mode as IP Address based. The PIM queries the IGS module to obtain the Portlist.

Default

By default, this option is snooping multicast-forwarding-mode ip.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

15.3 ip igmp snooping

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

Parameters

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

Default

By default, this option is no ip igmp snooping.

Command Mode

Global Configuration Mode / Config-VLAN Mode.

Usage Guideline

None.

15.4 ip igmp snooping static-group

This command configures the static group of IGMP snooping.
Use the **no** command to delete the static-group.

Syntax

- **ip igmp snooping static-group <mcast _addr> ports <ifXtype> <iface_list>**
- **no ip igmp snooping stattic-group <mcast_addr>**

Parameters

Parameters	Description
<mcast_addr>	Specify a multicast group address within the given VLAN for detailed information about that specific group.
<ifXtype>	Defines the type of interface to be configured as a static multicast group member. [fastethernet, gigabitethernet, extreme-ethernet, internal-lan, port-channel]
<iface_list>	Specifies the list of interfaces, depending on the selected interface type.

Default

None.

Command Mode

Config-VLAN Mode.

Usage Guideline

Using this command, users can create an IGMP snooping static group to prepare for situations where connected hosts do not support the IGMP protocol. Creating a static group allows multicast traffic to be forward to unlearned ports.

Example

This example shows how to configure the gigabitethernet interface to always forward traffic for a specific multicast group.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# vlan 1
XX-MUxxTPoE+(config-vlan)# ip igmp snooping static-group 225.1.0.1 ports gigabitethernet 0/1
XX-MUxxTPoE+(config-vlan)#
```

15.5 ip igmp snooping report-suppression interval

This command is used to configure the specified interface(s) as the multicast router ports or as forbidden to be multicast router ports on the Switch. Use the **no** form of this command to remove the interface(s) from router ports or forbidden multicast router ports.

Syntax

- **ip igmp snooping report-suppression-interval <(1 – 25) seconds>**
- **no ip igmp snooping report-suppression-interval**

Default

By default, this value is 5 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

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

15.6 ip igmp snooping group-query-interval

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

Default

By default, this value is 2 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

15.7 ip igmp snooping global version

This ip igmp snooping global version command configures the version of IGMP used by the IGMP snooping feature on a network switch. IGMP has several versions - IGMPv1, IGMPv2, and IGMPv3, each with its own set of functionalities and enhancements. IGMPv1 is the oldest and simplest, while IGMPv3 supports more advanced features like source filtering. By setting the IGMP version for snooping, the switch can effectively handle multicast traffic according to the capabilities and requirements of the specified IGMP version. This configuration is global and affects how the switch processes IGMP messages for all VLANs.

Syntax

- ip igmp snooping global version {v1 |v2 | v3}

Parameters

Parameters	Description
v1	Configures the version as IGMP snooping Version 1.
v2	Configures the version as IGMP snooping Version 2.
v3	Configures the version as IGMP snooping Version 3.

Default

By default, this option is ip igmp snooping version v3.

Command Mode

Global Configuration Mode.

Usage Guideline

When IGMPv3 snooping and multicast filtering function are enabled simultaneously, it may cause issues with the use of RIP/OSPF.
Please avoid placing MU series switching hubs with multicast filtering functionality in conjunction with IGMP snooping between L3 Switching hubs.

Example

This example shows how to set the IGMP snooping global version to v2.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# ip igmp snooping global version v2
XX-MUxxTPoE+(config)#
```

15.8 ip igmp snooping version

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}

Parameters

Parameters	Description
v1	Configures the version as IGMP snooping Version 1.
v2	Configures the version as IGMP snooping Version 2.
v3	Configures the version as IGMP snooping Version 3.

Default

By default, this option is ip igmp snooping version v3.

Command Mode

Config-VLAN Mode.

Usage Guideline

When IGMPv3 snooping and multicast filtering function are enabled simultaneously, it may cause issues with the use of RIP/OSPF.
Please avoid placing MU series switching hubs with multicast filtering functionality in conjunction with IGMP snooping between L3 Switching hubs.

Example

This example shows how to set the IGMP snooping version for vlan 10 to v3.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# vlan 10
XX-MUxxTPoE+(config-vlan)# ip igmp snooping version v3
XX-MUxxTPoE+(config-vlan)#
```

15.9 ip igmp snooping querier

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.

If multiple queries exist in the network, the querier election mechanism will automatically determine the active querier based on the lowest IP address. Only the active querier will send IGMP query messages, while other queriers will remain in a standby state.

Syntax

- ip igmp snooping querier
- no ip igmp snooping querier

Default

By default, this option is no ip igmp snooping querier.

Command Mode

Config-VLAN Mode.

Usage Guideline

None.

15.10 ip igmp snooping query-interval

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.

Syntax

- ip igmp snooping query-interval <(60 - 600) seconds>
- no ip igmp snooping query-interval

Default

By default, this value is 125 seconds.

Command Mode

Config-VLAN Mode.

Usage Guideline

The switch must be configured as a querier for this configuration to be imposed.

15.11 ip igmp snooping startup-query-interval

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.

Syntax

- ip igmp snooping startup-query-interval <(15 - 150) seconds>
- no ip igmp snooping startup-query-interval

Default

By default, this value is 15 seconds.

Command Mode

Config-VLAN Mode.

Usage Guideline

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 1/4 of the query interval.

15.12 ip igmp snooping startup-query-count

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.

Syntax

- ip igmp snooping startup-query-count <2 - 5>
- no ip igmp snooping startup-query-count

Default

By default, this value is 2.

Command Mode

Config-VLAN Mode.

Usage Guideline

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

15.13 no ip igmp snooping other-querier-present-interval

This command sets the other querier present interval to default value.

Syntax

- no ip igmp snooping other-querier-present-interval

Default

None.

Command Mode

Config-VLAN Mode.

Usage Guideline

None.

15.14 ip igmp snooping max-response-code

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

Default

By default, this value is 120 seconds.

Command Mode

Config-VLAN Mode.

Usage Guideline

None.

15.15 ip igmp snooping mrouter

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.

Syntax

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

Parameters

Parameters	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.

Default

By default, this option is no ip igmp snooping mrouter.

Command Mode

Config-VLAN Mode.

Usage Guideline

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.

15.16 ip igmp snooping blocked-router

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.

Syntax

- **ip igmp snooping blocked-router <interface-type> <0/a-b, 0/c, ...>**

Parameters

Parameters	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.

Parameters	Description
<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.

Default

None.

Command Mode

Config-VLAN Mode.

Usage Guideline

The ports to be configured as blocked router ports, must not be configured as static router ports.

15.17 ip igmp snooping leavemode

This command sets the mode for handling leave messages in IGMP snooping.

Syntax

- ip igmp snooping leavemode {fastLeave | normalleave}

Parameters

Parameters	Description
fastLeave	When **fastLeave** is enabled, it immediately stops multicast traffic upon receiving a leave message.
normalleave	When normalleave is enabled, it stops multicast traffic only after confirming that there are no other members requiring the multicast group following the receipt of a leave message.

Default

By default, this value is **fastLeave**.

Command Mode

Interface Configuration Mode

Usage Guideline

In the case that you set **fastLeave**, the switch assumes there are no other multicast group members and stop multicast traffic to a specific interface.

Example

This example shows how to set the IGMP snooping leave mode to **fastLeave** when receiving a leave message for port 2.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# interface gigabitethernet 0/2
XX-MUxxTPoE+(config-if)# ip igmp snooping leavemode fastLeave
XX-MUxxTPoE+(config-if)#
```

15.18 show ip igmp snooping mrouter

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>]

Parameters

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

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

15.19 show ip igmp snooping blocked-router

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>]

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

15.20 show ip igmp snooping globals

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>]

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

15.21 show ip igmp snooping

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>]

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

15.22 show ip igmp snooping groups

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>]]

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

15.23 show ip igmp snooping port-cfg

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>}]

Parameters

Parameters	Description
interface	Interface type and identifier.

Parameters	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.
<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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

15.24 show ip igmp snooping forwarding-database

show ip igmp snooping forwarding-database.

Syntax

- **show ip igmp snooping forwarding-database [Vlan <vlan-id>]**

Parameters

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

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

15.25 show ip igmp snooping statistics

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>]

Parameters

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

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

15.26 show ip igmp snooping multicast-vlan

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>]

Parameters

Parameters	Description
<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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

16 Multicast Filtering Commands

16.1 multicast-filtering

This command enable/disable multicast-filtering in the switch.

Syntax

- multicast-filtering {enable | disable}

Parameters

Parameters	Description
enable	Enables multicast-filtering.
disable	Disables multicast-filtering.

Default

By default, this option is disable.

Command Mode

Global Configuration Mode.

Usage Guideline

When multicast-filtering is enabled and there is a need to forward data to unlearned ports, please refer to "15.4 ip igmp snooping static group" to statically register the destination addresses.
In addition, multicast packets such as OSPF, RIP, and VRRP will be discarded regardless of their destination.

Example

This example shows how to enable the multicast-filtering.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# multicast-filtering enable
XX-MUxxTPoE+(config)#
```

16.2 show multicast-filtering status

This command displays the multicast filtering status.

Syntax

- show multicast-filtering status

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

17 Jumbo Frame

17.1 jumbo-frame

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)>

Parameters

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

Default

By default, this value is 1522 Bytes.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

17.2 show jumbo-frame

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

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

None.

18 SNMP Commands

18.1 snmp trap link-status

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**

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

None.

18.2 enable snmpagent

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**

Default

By default, this option is enable snmpagent.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

18.3 disable snmpagent

This command disables SNMP agent.

Syntax

- disable snmpagent

Default

By default, this option is enable snmpagent.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

18.4 snmp community

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 >

Parameters

Parameters	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.

Default

Community Name	Security Name	Transport Tag
NETMAN	noAuthUser	None
PUBLIC	noAuthUser	None

Command Mode

Global Configuration Mode.

Usage Guideline

None.

18.5 snmp group

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 }

Parameters

Parameters	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.

Default

Group Name	Security Mode	Security Name
iso	v1	noAuthUser
iso	v2c	noAuthUser
noAuthUser	v3	noAuthUser

Command Mode

Global Configuration Mode.

Usage Guideline

None.

18.6 snmp access

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}}

Parameters

Parameters	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.

Default

Group Name	Security Mode	Privilege Mode	Read View	Write View	Notify View
iso	v1	No Auth	iso	iso	iso
iso	v2c	No Auth	iso	iso	iso
noAuthUser	v3	No Auth	restricted	restricted	restricted

Command Mode

Global Configuration Mode.

Usage Guideline

None.

18.7 snmp engineid

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

Default

By default, This is a device-specific ID.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

18.8 snmp view

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>

Parameters

Parameters	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.

Default

Group Name	Subtree OID	Subtree Mask	View Type
iso	1	1	Included
restricted	1	1	Included

Command Mode

Global Configuration Mode.

Usage Guideline

None.

18.9 snmp targetaddr

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>

Parameters

Parameters	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.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

18.10 snmp targetparams

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>

Parameters

Parameters	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	Allows 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.

Default

Target Parameter Name	Message Processing Model	Security Mode	Security Name	Privilege Mode
internet	v2c	v2c	noAuthUser	No Auth
test1	v2c	v1	noAuthUser	No Auth

Command Mode

Global Configuration Mode.

Usage Guideline

None.

18.11 snmp user

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>

Parameters

Parameters	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.

Default

By default, the snmp user name is noAuthUser.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

18.12 snmp notify

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>

Parameters

Parameters	Description
<NotifyName>	Configures a unique identifier associated with the entry.
tag<TagName>	Sets a notification tag, which selects the entries in the Target Address Table.
tag	• 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.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

18.13 show snmp

This command displays the status information of SNMP communications.

Syntax

- show snmp

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

18.14 show snmp community

This command displays the configured SNMP community details.

Syntax

- show snmp community

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

18.15 show snmp group

This command displays the configured SNMP groups.

Syntax

- show snmp group

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

18.16 show snmp group access

This command displays the configured SNMP group access details.

Syntax

- show snmp group access

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

18.17 show snmp engineid

This command displays the configured SNMP group access details.

Syntax

- show snmp group access

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

18.18 show snmp viewtree

This command displays the configured SNMP Tree views.

Syntax

- show snmp viewtree

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

18.19 show snmp targetaddr

This command displays the configured SNMP target Addresses.

Syntax

- show snmp targetaddr

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

18.20 show snmp targetparam

This command displays the configured SNMP Target Address Params.

Syntax

- show snmp targetparam

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

18.21 show snmp user

This command displays the configured SNMP users.

Syntax

- show snmp user

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

18.22 show snmp notif

This command displays the configured SNMP Notification types.

Syntax

- show snmp notif

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

18.23 show snmp inform statistics

This command displays the inform message statistics.

Syntax

- show snmp inform statistics

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

18.24 show snmp-server traps

This command displays the set of traps that are currently enabled.

Syntax

- show snmp-server traps

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

18.25 show snmp-server proxy-udp-port

This command displays the proxy udp port.

Syntax

- show snmp-server proxy-udp-port

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

18.26 show mib name

This command displays the name of the corresponding mib object identifier.

Syntax

- show mib name <Object OID. eg 1.3.6.1.6>

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

19 DNS Commands

19.1 ip name-server

This command configures default name server IP.

Syntax

- ip name-server {ipv4 <ucast_addr>}

Parameters

Parameters	Description
ipv4 <ucast_addr>	Sets the IP address for the domain name server in IPv4 address format.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

19.2 domain name-server

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>

Parameters

Parameters	Description
ipv4 <ucast_addr>	Sets the IP address for the domain name server in IPv4 address format.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

19.3 show ip dns name-server

This command displays the DNS name servers information.

Syntax

- show ip dns name-server

Default

None.

Command Mode

Privilege EXEC Mode.

Usage Guideline

None.

20 IP Commands

20.1 ip address

This command sets the IP address for an interface.

Syntax

- ip address <ucast_addr> <ip_mask>
- no ip address <ucast_addr>

Parameters

Parameters	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.

Default

The default IP address setting for the switch is DHCP client mode, which automatically assigns an IP address from a DHCP server. If an IP address cannot be obtained from the DHCP server within 2 minutes, it will be automatically changed to a fixed IP address (IP address: 192.168.0.239, subnet mask: 255.255.255.0).

Command Mode

Interface Configuration Mode
This command is applicable in VLAN Interface Mode / OOB Interface Mode.

Usage Guideline

When you set the IP address for the first time, please send [no ip address] on "Interface Configuration Mode"

Example

This example shows how to set the IP address manually for the first time.
If you set the IP address two or more times, you can also use this command.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# interface vlan 1
XX-MUxxTPoE+(config-if)# no ip address
XX-MUxxTPoE+(config-if)# ip address 192.168.33.77 255.255.255.0
XX-MUxxTPoE+(config-if)#
```

20.2 ip address dhcp

This command sets the DHCP IP address for an interface.

Syntax

- ip address dhcp
- no ip address

Parameters

Parameters	Description
dhcp	Get IP by using DHCP protocol.

Default

By default, this option is no ip address.

Command Mode

Interface Configuration Mode.

This command is applicable in VLAN Interface Mode / OOB Interface Mode.

Usage Guideline

To use DHCP IP address, it needs to specify the DHCP server.
So please specify the address of the DHCP server using **ip dhcp server** command.

Example

This example shows how to set DHCP IP address on VLAN 1.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# interface vlan 1
XX-MUxxTPoE+(config-if)# no ip address
XX-MUxxTPoE+(config-if)# ip address dhcp
XX-MUxxTPoE+(config-if)#
```

20.3 show ip source binding dhcp snooping

This command displays the dynamic IP binding updates through DHCP snooping.

Syntax

- show ip source binding dhcp-snooping [vlan <vlan-id (1-4094)>]

Parameters

Parameters	Description
vlan <vlan-range>	Displays the update information for dynamic IP binding of a specific VLAN.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

This command is used to display the dynamic IP binding updates through DHCP snooping.

Example

This example shows how to display VLAN 1 dynamic IP source binding DHCP snooping.

```
XX-MUxxTPoE+# show ip source binding dhcp-snooping vlan 1

Host Binding Information :

Vlan            HostMac           HostIP           Interface      Type
----            -------           ------           ---------      ----
1          00:1A:2B:3C:4D:5E    192.168.10.100       Gi0/9       dhcp
XX-MUxxTPoE+#
```

20.4 ip dhcp snooping

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)>]

Default

By default, this option is no ip dhcp snooping.

Command Mode

Global Configuration mode.

Usage Guideline

When the DHCP snooping feature is enabled, it monitors the received DHCP packets. In addition, it prevents DHCP spoofing by discarding invalid DHCP packets.

Example

This example shows how to enable DHCP sooping in VLAN 5.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# ip dhcp snooping vlan 5
XX-MUxxTPoE+(config)#
```

20.5 ip dhcp snooping verify mac-address

This command globally enables DHCP MAC verification in the switch.

Syntax

- ip dhcp snooping verify mac-address
- no ip dhcp snooping verify mac-address

Default

By default, this option is ip dhcp snooping verify mac-address.

Command Mode

Global Configuration mode.

Usage Guideline

By default, the DHCP snooping feature verifies that the source MAC address of the DHCP packet matches the MAC address of the DHCP client.

Example

This example shows how to enable DHCP MAC-address verification on whole switch.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# no ip dhcp snooping verify mac-address
XX-MUxxTPoE+(config)#
```

20.6 ip dhcp snooping

This command enables layer 2 DHCP snooping in the VLAN.

Syntax

- ip dhcp snooping
- no ip dhcp snooping

Default

By default, this option is no ip dhcp snooping.

Command Mode

Config-VLAN mode.

Usage Guideline

By using the ip dhcp snooping command in Config-VLAN mode,you can enable the DHCP snooping feature for each VLAN.

Example

This example shows how to enable DHCP snooping function on vlan 10.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# vlan 10
XX-MUxxTPoE+(config-vlan)# ip dhcp snooping
XX-MUxxTPoE+(config-vlan)#
```

20.7 ip dhcp snooping trust

This command configures the port as a trusted port.

Syntax

- ip dhcp snooping trust
- no ip dhcp snooping trust

Default

By default, this option is ip dhcp snooping trust.

Command Mode

Interface Configuration Mode.

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

Usage Guideline

This command is used to set the port connected DHCP server as trusted. When the DHCP snooping feature is enabled, it acts as a firewall between an untrusted port and the DHCP server.

Example

This example shows how to configure the port-channel 1 as a not trusted port.

```
XX-MUxxTPoE+#configure terminal
XX-MUxxTPoE+(config)# interface port-channel 1
XX-MUxxTPoE+(config-if)# no ip dhcp snooping trust
XX-MUxxTPoE+(config-if)#
```

20.8 show ip dhcp snooping globals

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

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

This command is used to display the global configuration of DHCP snooping.

Example

This example shows how to display the global configuration of DHCP snooping.

```
XX-MUxxTPoE+# show ip dhcp snooping globals

DHCP Snooping Global information
--------------------------------

Switch : default
-------  -------
Layer 2 DHCP Snooping is globally enabled
MAC Address verification is disabled

XX-MUxxTPoE+#
```

20.9 show ip dhcp snooping

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)>]

Paramater

Parameter	Description
vlan	Specify the VLAN ID for which you want to display the DHCP snooping information.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

This command is used to display the DHCP snooping configuration and statistics of all VLANs.
By using **vlan** parameter, you can display the information for the specified VLAN.

Example

This example shows how to display the DHCP snooping configuration for VLAN 5.

```
XX-MUxxTPoE+# show ip dhcp snooping vlan 5

DHCP Snooping Vlan information
------------------------------
VLAN                            : 5
Snooping status                 : Enabled
Number of Incoming Discovers    : 0
Number of Incoming Requests     : 0
Number of Incoming Releases     : 0
Number of Incoming Declines     : 0
Number of Incoming Informs      : 0
Number of Transmitted Offers    : 0
Number of Transmitted Acks      : 0
Number of Transmitted Naks      : 0
Total Number Of Discards        : 0
Number of MAC Discards          : 0
Number of Server Discards       : 0
Number of Option Discards       : 0

XX-MUxxTPoE+#
```

20.10 show ip route

This command displays the IP routing table.

Syntax

- show ip route [{<ip_addr> [<ip_mask>] | connected | static | summary | details}]

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

This command is used to display the IP route table.

Example

This example shows how to display all the IP route entries.

```
XX-MUxxTPoE+# show ip route

Codes: C - connected, S - static

C 192.168.0.0/24 is directly connected
S 192.168.10.0/24 via 192.168.100.254

XX-MUxxTPoE+#
```

20.11 show ip arp

This command displays IP ARP table.

Syntax

- show ip arp [{ Vlan <vlan_vfi_id> | <ucast_addr> | <ucast_mac> | summary | information | statistics }]

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

This command is used to display the IP ARP table.

Example

This example shows how to display all routes to the IP address 192.168.10.100.

```
XX-MUxxTPoE+# show ip arp 192.168.10.100

Address          Hardware Address   Type  Interface  Mapping   VRF Name
-------          ----------------   ----  ---------  -------  --------
192.168.10.100   00:1A:2B:3C:4D:5E  ARPA  vlan1      Dynamic   default

XX-MUxxTPoE+#
```

20.12 ip route

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>

Parameters

Parameters	Description
<ip-address>	Configures the IP Address of ARP Entry.
<ip-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.
<ucast_addr>	Configures the next hop IP Address. The next hop IP Address specifies the IP Address that can be used to reach the destination network.
<short (1-254)>	Configures the priority number of the route. If there are multiple routes available to reach the destination network, the route with the smaller priority number will be selected.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

To set the default gateway, configure the <ip-address> and <ip-mask> to 0.0.0.0, and set <ucast_addr> to the default gateway IP address.

Example

This example shows how to entry static ip route to 192.168.10.0/24.

192.168.100.254 is the gateway in subnet 192.168.100.0/24.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# ip route 192.168.10.0 255.255.255.0 192.168.100.254
XX-MUxxTPoE+(config)#
```

20.13 arp timeout

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

Default

By default, this value is 300 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

This command is used to set the ARP aging timer of the IP ARP table.

Example

This example shows how to set the term of arp table remains to 86400 seconds.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# arp timeout 86400
XX-MUxxTPoE+(config)#
```

20.14 arp

This command adds a static entry in the ARP cache.

Syntax

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

Parameters

Parameters	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.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

This command is used to add the static entry in the ARP cache.
By using the ARP cache, eliminates the need to repeatedly perform address resolution.

Example

This example shows how to add the ARP cache for IP address 192.168.10.100 and MAC address 00:1A:2B:3C:4D:5E in the ARP cache table.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# arp 192.168.10.100 00:1A:2B:3C:4D:5E
XX-MUxxTPoE+(config)#
```

20.15 ip arp max-retries

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

Parameters

Parameters	Description
<short (2-10)>	Configures the maximum number of ARP request entries. The value ranges between 2 and 10.

Default

By default, this value is 3.

Command Mode

Global Configuration Mode.

Usage Guideline

This command is used to set the maximum number of the IP ARP request retries.

Example

This example shows how to configure the maximum number of ARP requests retries to 5.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# ip arp max-retries 5
XX-MUxxTPoE+(config)#
```

21 DHCP Server Commands

21.1 show dhcp server

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

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

21.2 show dhcp-relay

This command displays DHCP relay agent configuration.

Syntax

- show dhcp-relay

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

21.3 service dhcp-relay

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.g.

Syntax

- service dhcp-relay
- no service dhcp-relay

Default

By default, this option is no service dhcp-relay.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

21.4 ip dhcp server

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>

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

21.5 ip dhcp client fast-access

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

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

22 VLAN

22.1 vlan

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>

Parameters

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

Default

The VLAN ID 1 exists in the system as the default VLAN.

Command Mode

Global Configuration Mode.

Usage Guideline

Use the **vlan** command to create VLANs. Entering the **vlan** command with a VLAN ID enters the Config-VLAN mode. Entering the VLAN ID of an existing VLAN does not create a new VLAN, but allows the user to modify the VLAN parameters for the specified VLAN. When the user enters the VLAN ID of a new VLAN, the VLAN will be automatically created.

Example

This example shows how to create VLAN ID 5 and enter into Config-VLAN Mode (VLAN 5).

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# vlan 5
XX-MUxxTPoE+(config-vlan)#
```

22.2 ports

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/ab,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])]

Parameters

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 anadministratively assigned string with the maximum size as 32.

Default

None.

Command Mode

Config-VLAN Mode.

Usage Guideline

By setting the ports command multiple times with different VLAN IDs, a port can be a tagged member port or an untagged member port of multiple VLANs.

Example

This example shows how to add port 3 and port 4 as member of VLAN 5, with port 3 configure as an untagged port, and its tie up as port channel 1.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# vlan 5
XX-MUxxTPoE+(config-vlan)# ports add gigabitethernet 0/3,0/4 port-channel 1
untagged gigabitethernet 0/3
XX-MUxxTPoE+(config-vlan)#
```

22.3 ports name

This command configures Vlan name.

Syntax

- ports name [<vlan-name>]

Default

By default, this option is default.

Command Mode

Config-VLAN Mode.

Usage Guideline

Use this command to specify the name of VLAN.
The VLAN name must be unique within administrative domain.

Example

This example shows how to configure the name of VLAN 5 to “office”.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# vlan 5
XX-MUxxTPoE+(config-vlan)# ports name office
XX-MUxxTPoE+(config-vlan)#
```

22.4 gvrp advertisement

This command sets Enables or Disables gvrp advertisement on this vlan.

Syntax

- gvrp advertisement {enable | disable}

Default

By default, this option is enable.

Command Mode

Config-VLAN Mode.

Usage Guideline

By enabling GVRP advertisement you can set the VLAN configuration automatically; however, when you need to set the VLAN configuration manually we recommend turning off the GVRP advertisement.

Example

This example shows how to disable gvrp advertisement on vlan 5.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# vlan 5
XX-MUxxTPoE+(config-vlan)# gvrp advertisement disable
XX-MUxxTPoE+(config-vlan)#
```

22.5 switchport pvid

This command configures the PVID on the specified port. ThePVID 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

Parameters

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.

Default

By default, the vlan-id value is 1.

Command Mode

Interface Configuration mode (Physical / Port channel).

Usage Guideline

The PVID you want to set have to exist as VLAN.
How to create VLAN is explained in “chapter 24.1 vlan”.

Example

This example shows how to set PVID 5 on port 4.

```
XX-MUxxTPoE+#configure terminal
XX-MUxxTPoE+(config)# interface gigabitethernet 0/4
XX-MUxxTPoE+(config-if)# switchport pvid 5
XX-MUxxTPoE+(config-if)#
```

22.6 switchport acceptable-frame-type

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.

Syntax

- switchport acceptable-frame-type {all | tagged | untaggedAndPrioritytagged }

Parameters

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.

Default

By default, this option is switchport acceptable-frame-type all.

Command Mode

Interface Configuration mode (Physical / Port channel).

Usage Guideline

This configuration does not affect VLAN independent BPDU frames such as GVRP BPDU and STP BPDU. It affects only the VLAN dependent BPDU frames.

Example

This example shows how to configure the type of acceptable frame as **tagged** for port 5.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# interface gigabitethernet 0/5
XX-MUxxTPoE+(config-if)# switchport acceptable-frame-type tagged
XX-MUxxTPoE+(config-if)#
```

22.7 switchport ingress-filter

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

Default

By default, this option is no switchport ingress-filter.

Command Mode

Interface Configuration mode (Physical / Port channel).

Usage Guideline

Use this command to enable ingress-filter for packets received by the interface. If ingress-filter is enabled, the packets will be dropped when the received port is not a member of the VLAN classified.

Example

This example shows how to enable ingress filter function on port-channel 1.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# interface port-channel 1
XX-MUxxTPoE+(config-if)# switchport ingress-filter
XX-MUxxTPoE+(config-if)#
```

22.8 show forward-all

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

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

This command is used to display all entries in the VLAN forward all table.

Example

This example shows how to display all entries in the VLAN forward all table.

```
XX-MUxxTPoE+# show forward-all

Vlan Forward All Table
----------------------

Vlan ID: 1
ForwardAll Ports          : None
ForwardAll Static Ports   : None
ForwardAll ForbiddenPorts : None
------------------------------------------------------------
Vlan ID: 5
ForwardAll Ports          : None
ForwardAll Static Ports   : None
ForwardAll ForbiddenPorts : None
------------------------------------------------------------
XX-MUxxTPoE+#
```

22.9 show vlan

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]

Parameters

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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

- Use the **show vlan** command to display the effective member ports of VLAN(s).
- Use the **show vlan id** command to display specified VLAN.
- Use the **show vlan summary** command to display sum number of VLAN.

Example

The first example shows how to display the current entries of VLAN 5.
And the second example show how to display sum number of VLAN entries on specified switch.

```
XX-MUxxTPoE+# show vlan id 5

Vlan database
-------------
Vlan ID             :5
Member Ports        :Gi0/3,0/4, po1
Untagged Ports      :Gi0/3
Forbidden Ports     :None
Name                :office
Status              :Permanent
GVRP advertisment   :Disabled
-----------------------------------------------------

XX-MUxxTPoE+#
```

```
XX-MUxxTPoE+# show vlan summary

Number of vlans  : 2

XX-MUxxTPoE+#
```

22.10 show vlan device info

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

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

This command is used to display the VLAN global configuration applicable to all VLANs in the switch or all contexts.

Example

This example shows how to display VLAN global information.

```
XX-MUxxTPoE+# show vlan device info

Vlan device configurations
--------------------------
Vlan Status                         : Enabled
Vlan Oper status                    : Enabled
Gvrp status                         : Disabled
Gmrp status                         : Disabled
Gvrp Oper status                    : Disabled
Gmrp Oper status                    : Disabled
Mac-Vlan Status                     : Disabled
Subnet-Vlan Status                  : Disabled
Protocol-Vlan Status                : Enabled
Bridge Mode                         : Customer Bridge
Base-Bridge Mode                    : Vlan Aware Bridge
Traffic Classes                     : Enabled
Vlan Operational Learning Mode      : IVL
Hybrid Default Learning Mode        : IVL
Version number                      : 1
Max Vlan id                         : 4094
Max supported vlans                 : 1024
Global mac learning status          : Enabled
Filtering Utility Criteria          : Enabled
Unicast mac learning limit          : 7936
XX-MUxxTPoE+#
```

22.11 show vlan static

This command displays static VLAN global status for the specified VLAN range.

Syntax

- show vlan static [id <vlan-range>]

Parameters

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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

This command is used to display the static VLAN global status for the specified VLAN range.

Example

This example shows how to display the global status from VLAN 1to VLAN 5.

```
XX-MUxxTPoE+# show vlan static id 1-5

Vlan database
-------------
Vlan ID             : 1
Member Ports        : Gi0/1, Gi0/2, Gi0/3, Gi0/4, Gi0/5, Gi0/6
                      Gi0/7, Gi0/8, Gi0/9, Gi0/10, Gi0/11, Gi0/12
                      po1, po2, po3, po4, po5, po6
                      po7, po8
Untagged Ports      : Gi0/1, Gi0/2, Gi0/3, Gi0/4, Gi0/5, Gi0/6
                      Gi0/7, Gi0/8, Gi0/9, Gi0/10, Gi0/11, Gi0/12
                      po1, po2, po3, po4, po5, po6
                      po7, po8
Forbidden Ports     : None
Name                : default
Status              : Permanent
----------------------------------------------------
Vlan ID             : 5
Member Ports        : Gi0/3, Gi0/4, po1
Untagged Ports      : Gi0/3
Forbidden Ports     : None
Name                : office
Status              : Permanent
----------------------------------------------------

XX-MUxxTPoE+#
```

22.12 show vlan device capabilities

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

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

This command is used to display only the list of VLAN features.

Example

This example shows how to display the list of VLAN features suported in the switch/ all contexts.

```
XX-MUxxTPoE+# show vlan device capabilities
Vlan device capabilities
-------------------------

Extended filtering services
Traffic classes
Static Entry Individual port
IVL capable
SVL capable
Hybrid capable
Configurable Pvid Tagging
XX-MUxxTPoE+#
```

22.13 show vlan ports config

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 ports config [interface < interface-type > <ifnum>]

Parameters

Parameter	Description
interface <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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

By using the interface parameter, it is possible to specify a particular interface to display the configuration.

Example

This example shows how to display the VLAN-related port-specific information for port 3.

```
XX-MUxxTPoE+#show vlan ports config interface gigabitethernet 0/3

Vlan Port configuration table
-----------------------------
Port Gi0/3
 Bridge Port Type                    : Customer Bridge Port
 PVID                                : 1
 Port Acceptable Frame Type          : Admit All
 Port Mac Learning Status            : Enabled
 Port Ingress Filtering              : Disabled
 Port Priority-Tag Ingress Filtering : Disabled
 Port Mode                           : Hybrid
 Port Gvrp Status                    : Disabled
 Port Gmrp Status                    : Enabled
 Port Gvrp Failed Registrations      : 0
 Gvrp last pdu origin                : 00:00:00:00:00:00
 Port Restricted Vlan Registration   : Disabled
 Port Restricted Group Registration  : Disabled
 Mac Based Support                   : Disabled
 Subnet Based Support                : Disabled
 Port-and-Protocol Based Support     : Enabled
 Default Priority                    : 0
 Dot1x Protocol Tunnel Status        : Peer
 LACP Protocol Tunnel Status         : Peer
 Spanning Tree Tunnel Status         : Peer
 MVRP Protocol Tunnel Status         : Peer
 MMRP Protocol Tunnel Status         : Peer
 GVRP Protocol Tunnel Status         : Peer
 GMRP Protocol Tunnel Status         : Peer
 IGMP Protocol Tunnel Status         : Peer
 Filtering Utility Criteria          : Default
 Port Protected Status               : Disabled
 ----------------------------------------------------

XX-MUxxTPoE+#
```

22.14 show vlan statistics

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>]**

Parameters

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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

By using the **vlan** parameter, it is possible to specify a particular vlan to display the statistics.

Example

This example shows how to display the unicast and broadcast statistics details for vlan 5.

```
XX-MUxxTPoE+# show vlan statistics vlan 5
Software Statistics Disabled

Unicast/broadcast Vlan statistics
-------------------------------------
 Vlan Id                          : 5
 Unicast frames received          : 0
 Mcast/Bcast frames received      : 0
 Unknown Unicast frames flooded   : 0
 Unicast frames transmitted       : 0
 Broadcast frames transmitted     : 0
 Vlan Statistics Collection is Disabled
-------------------------------------
XX-MUxxTPoE+#
```

23 IPv6 Commands

23.1 ipv6 address - prefix and prefix length

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]

Parameters

Parameters	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.

Default

None.

Command Mode

Interface Configuration Mode.

This command is applicable in VLAN Interface Mode.

Usage Guideline

None.

23.2 ipv6 address dhcp

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

Default

By default, this option is no ipv6 address dhcp.

Command Mode

Interface Configuration Mode.

Usage Guideline

None.

23.3 ipv6 unicast-routing

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

Default

By default, this option is no ipv6 unicast-routing.

Command Mode

Global Configuration Mode / Interface Configuration Mode

Usage Guideline

None.

23.4 ipv6 route

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>]

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

23.5 ipv6 neighbor

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>}

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

23.6 clear ipv6 neighbors

This command removes all the entries in the IPv6 neighbor table.

Syntax

- clear ipv6 neighbors

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

23.7 clear ipv6 traffic

This command removes all the entries in the IPv6 traffic table.

Syntax

- clear ipv6 traffic

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

23.8 clear ipv6 traffic

This command removes all the entries in the IPv6 traffic table.

Syntax

- clear ipv6 traffic

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

23.9 clear ipv6 route

This command removes all the entries in IPv6 route table.

Syntax

- clear ipv6 route

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

23.10 ipv6 enable

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

Default

By default, this option is ipv6 enable.

Command Mode

Interface Configuration Mode.

Usage Guideline

None.

23.11 ipv6 address - prefix and prefix length

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]

Parameters

Parameters	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.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

None.

23.12 ipv6 address - link local

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

Parameters

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

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

None.

23.13 show ipv6 interface

This command displays the IPv6 interfaces.

Syntax

- show ipv6 interface [{vlan <vlan-id> [prefix]}]

Parameters

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

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

23.14 show ipv6 route

This command displays the IPv6 Routes.

Syntax

- show ipv6 route

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

23.15 show ipv6 route - summary

This command displays the summary of IPv6 Routes.

Syntax

- show ipv6 route summary

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

23.16 show ipv6 neighbors

This command displays the IPv6 Neighbor Cache Entries.

Syntax

- show ipv6 neighbors

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

23.17 ping ipv6

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)>]

Parameters

Parameters	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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

24 Voice-VLAN

24.1 voice vlan state

This command Enables / Disables voice vlan in the switch.

Syntax

- voice vlan state [{oui-enabled | disabled | auto}]

Parameters

Parameter	Description
oui-enable	Enable voice vlan with OUI.
disable	Disable voice vlan.
auto	Enable voice vlan with LLDP-MED.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

24.2 voice vlan id

This command specifies the voice VLAN.

Syntax

- voice vlan id <integer(1-4094)>

Parameters

Parameter	Description
<integer(1-4094)>	Vlan id.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

24.3 voice vlan aging-time

This command specifies the voice VLAN aging timeout interval in minutes.

Syntax

- voice vlan aging-time <integer(30-65535)>

Parameters

Parameter	Description
<integer(30-65535)>	Timeout in minutes.

Default

By default, this value is 1440 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

24.4 voice vlan cos

This command specifies the OUI Voice VLAN Class of Service (CoS).

Syntax

- voice vlan cos <integer(0-7)> [remark]

Parameters

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

Default

By default, this value is 5.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

24.5 voice vlan vpt

This command specifies the LLDP-MED vlan priority tag.

Syntax

- voice vlan vpt <integer(0-7)>

Parameters

Parameter	Description
<integer(0-7)>	vpt.

Default

By default, this value is 5.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

24.6 voice vlan dscp

This command specifies the LLDP-MED dscp.

Syntax

- voice vlan dscp <integer(0-63)>

Parameters

Parameter	Description
<integer(0-63)>	dscp.

Default

By default, this value is 46.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

24.7 voice vlan oui-table

This command specifies the voice vlan OUI table.

Syntax

- voice vlan oui-table {add <aa:aa:aa> [text] | remove <aa:aa:aa> }

Parameters

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.

Default

Index	OUI Address	Desciption
1	00:01:E3	SIEMENS
2	00:03:6B	CISCO
3	00:09:6E	AVAYA
4	00:0F:E2	Huawei-3COM
5	00:60:B9	NEC/Philips
6	00:D0:1E	PINTEL
7	00:E0:75	Veritel Polycom
8	00:E0:BB	3COM

Command Mode

Global Configuration Mode.

Usage Guideline

None.

24.8 voice vlan enable

This command specifies the OUI voice vlan enable/disable on interfaces.

Syntax

- voice vlan enable
- no voice vlan enable

Default

By default, this option is no voice enable.

Command Mode

Interface Configuration Mode

Usage Guideline

None.

24.9 voice vlan cos mode

This command specifies the OUI voice vlan cos mode on interfaces.

Syntax

- **voice vlan cos mode {src | all }**

Parameters

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.

Default

By default, this option is voice vlan cos mode src.

Command Mode

Interface Configuration Mode.

Usage Guideline

Packets from MAC addresses registered in the OUI list have their COS values changed only on interfaces where the **src** parameter is set. On interfaces where the **all** parameter is set, the COS values of all packets that pass through are changed if there are packets registered in the OUI list.

24.10 show voice vlan

Show voice vlan state.

Syntax

- show voice vlan [oui-table]

Parameters

Parameter	Description
[oui-table]	Specifies OUI table.

Default

None.

Command Mode

Privilege EXEC Mode.

Usage Guideline

None.

25 GVRP

25.1 set gvrp

This command enables/disables GVRP in the switch.

Syntax

- set gvrp {enable | disable}

Parameters

Parameter	Description
enable	Enables GVRP in the switch.
disable	Disables GVRP in the switch.

Default

By default, this option is disable.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

25.2 set port gvrp

This command enables/disables GVRP on the port.

Syntax

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

Parameters

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.

Default

By default, this option is disable.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

25.3 set garp timer

This command sets GARP timers on the port.

Syntax

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

Parameters

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).

Default

By default, the join value is 200 seconds.
By default, the leave value is 600 seconds.
By default, the leave-all-time value is 10000 seconds.

Command Mode

Interface Configuration Mode.

Usage Guideline

None.

25.4 vlan restricted

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

Syntax

- vlan restricted {enable | disable}

Parameters

Parameter	Description
enable	Enables the restricted VLAN registration.
disable	Disables the restricted VLAN registration.

Default

By default, this option is disable.

Command Mode

Interface Configuration Mode.

Usage Guideline

None.

25.5 show garp timer

This command displays GARP timer information on the interfaces.

Syntax

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

Parameters

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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

25.6 show gvrp statistics

This command displays GVRP statistics on the interfaces.

Syntax

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

Parameters

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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

26 PNAC (Port-based Network Access Control) Commands

26.1 dot1x system-auth-control

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

Default

By default, this option is no dot1x system-auth-control.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

26.2 shutdown dot1x

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

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

26.3 dot1x clear statistics

This command clears dot1x counters for all the ports on the switch.

Syntax

- dot1x clear statistics {interface <iftype> <ifnum> | all}

Parameters

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.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

26.4 dot1x guest-vlan

This command configures Dot1x Guest VLAN ID.

Syntax

- dot1x guest-vlan <short (1-4094)>
- no dot1x guest-vlan

Parameters

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

Default

By default, this option is no dot1x guest-vlan.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

26.5 dot1x default

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

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

None.

26.6 dot1x reauthentication

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

Default

By default, this option is no dot1x reauthentication.

Command Mode

Interface Configuration Mode.

Usage Guideline

None.

26.7 dot1x timeout

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}
- no dot1x timeout {quiet-period | reauth-period | server-timeout | supp-timeout | tx-period}

Parameters

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.

Default

By default, the dot1x timeout quiet-period value is 60 seconds.
By default, the dot1x timeout reauth-period value is 3600 seconds.
By default, the dot1x timeout server-timeout value is 30 seconds.
By default, the dot1x timeout supp-timeout value is 30 seconds.

Command Mode

Interface Configuration Mode.

Usage Guideline

None.

26.8 dot1x port-control

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

Parameters

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.

Default

By default, this option is dot1x port-control force-authorized.

Command Mode

Interface Configuration Mode.

Usage Guideline

None.

26.9 dot1x mab

This command configures the MAC authentication bypass (MAB) feature. MAB feature is a part of 802.1x port-based network access control.

Syntax

- dot1x mab {mab_mode | hybrid_mode | disable}

Parameters

Parameter	Description
mab_mode	MAC Authentication Bypass.
hybrid_mode	Username/Password and MAC Authentication Bypass.
disable	Username/Password authentication.

Default

By default, this option is disable.

Command Mode

Interface Configuration Mode.

Usage Guideline

The only authentication protocol supported by this product is EAP-MD5.

Example

This example shows how to configure the **dot1x mab hybrid_mode** for port 2.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# interface gigabitethernet 0/2
XX-MUxxTPoE+(config-if)# dot1x mab hybrid_mode
XX-MUxxTPoE+(config-if)#
```

26.10 dot1x guest-vlan enable

This command enables/disables guest-vlan feature.

Syntax

- dot1x guest-vlan enable
- no dot1x guest-vlan enable

Default

By default, this option is no dot1x guest-vlan enable.

Command Mode

Interface Configuration Mode.

Usage Guideline

None.

26.11 show dot1x

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 }]

Parameters

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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

26.12 show dot1x guest-vlan

Displays dot1x Guest Vlan information.

Syntax

- show dot1x guest-vlan

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

26.13 show dot1x dynamic-vlan

This command displays dot1x dynamic VLAN assignment information.

Syntax

- show dot1x dynamic-vlan

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

26.14 show dot1x authenticated host

This command displays dot1x authenticated host status.

Syntax

- show dot1x authenticated host

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

26.15 dot1x re-authenticate

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>]

Parameters

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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

26.16 dot1x radius-vlan-assignment

This command enabled radius vlan assignment function on port.

Syntax

- dot1x radius-vlan-assignment enable
- no dot1x radius-vlan-assignment

Default

By default, this option is no dot1x radius-vlan-assignment.

Command Mode

Interface Configuration Mode.

Usage Guideline

None.

27 Port Isolation

27.1 port-isolation

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

Default

By default, this option is disable.

Command Mode

Interface Configuration.

Usage Guideline

None.

28 Radius Server

28.1 radius-server host

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

Syntax

- radius-server host {ipv4-address} [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} [primary]

Parameters

Parameter	Description
ipv4-address	Configures the IPv4 address of the RADIUS server host.
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.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

The setting for **primary** is not displayed on the web GUI.
The order of the Index on the GUI may differ from the actual priority.

Example

This example shows how to add a RADIUS server with the IP address 172.16.222.100 as the primary server, setting the server's authentication UDP port to 1812 and configuring the response wait on UDP port 1812. Additionally, it sets the authentication timeout to 60 seconds, the maximum number of authentication requests to 3 and encryption key to test.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# radius-server host 172.16.222.100 auth-port 1812 acct-port 1812
timeout 60 retransmit 3 key test primary
XX-MUxxTPoE+(config)#
```

28.2 show radius server

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>]

Parameters

Parameter	Description
<ucast_addr>	Displays the related information of the specified unicast address of the RADIUS server host.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

28.3 show radius statistics

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

Syntax

- show radius statistics

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

29 Dos

29.1 security-suite

This command enables/disables DoS prevention.

Syntax

- **security-suite**
- **no security-suite**

Default

By default, this option is no security-suite.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

29.2 show security-suite

Displays Dos information.

Syntax

- **show security-suite**

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

30 RMON

30.1 set rmon

This command is used to enable or disable the RMON feature.

Syntax

- set rmon {enable | disable}

Parameters

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.

Default

By default, this option is enable.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

30.2 rmon alarm

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)>

Parameters

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.
<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.

Parameter	Description
<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.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

30.3 rmon event

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)>

Parameters

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.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

30.4 rmon collection stats

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)>

Parameters

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.

Default

None.

Command Mode

Interface Configuration Mode / Config VLAN Mode.

Usage Guideline

None.

30.5 rmon collection history

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)>

Parameters

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.

Default

None.

Command Mode

Interface Configuration Mode / Config VLAN Mode.

Usage Guideline

None.

30.6 show rmon

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]]

Parameters

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.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

31 Log

31.1 show logging-file

This command displays the priority and file name of all the three files configured in the syslog file table.

Syntax

- show logging-file

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

31.2 show logging-server

This command displays the information about the syslog logging server table.

Syntax

- show logging-server

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

31.3 show logging

This command displays all the logging status and configuration information.

Syntax

- show logging

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

31.4 logging

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)>]}

Parameters

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.

Default

facility	severity	buffered
local0	informational	200

Command Mode

Global Configuration Mode.

Usage Guideline

By configuring the facility, logs can be appropriately categorized.
Additionally, by using severity to record only the necessary logs, resources can be utilized efficiently.

Example

This example shows how to set the facility to local5 and severity to errors.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# logging facility local5
XX-MUxxTPoE+(config)# logging severity errors
XX-MUxxTPoE+(config)#
```

31.5 logging-service

This command enables/disables syslog server.

Syntax

- logging-service { enable | disable }

Parameters

Parameter	Description
enable	Syslog enabled.
disable	Syslog disabled.

Default

By default, this option is enable.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

31.6 clear logs

This command clears the system syslog buffers.

Syntax

- clear logs

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

31.7 syslog filename-one

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)>

Default

By default, the file-name is flash_log.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

31.8 logging-file

This command adds an entry which is flash_log in the file table.

Syntax

- logging-file <short(0-191)> flash_log

Parameters

Parameter	Description
<short(0-191)>	Sets the priority of syslog messages. 0-lowest priority, 191-highest priority.

Default

By default, this option is 130.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

31.9 logging-server

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>

Parameters

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.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

32 ACL

32.1 ip access-list extend

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)>

Parameters

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

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

32.2 permit- ip/ospf/pim/protocol type

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)>]

Parameters

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.

Default

None.

Command Mode

IPV4 ACL Extended Access List Configuration Mode.

Usage Guideline

None.

32.3 deny- ip/ospf/pim/protocol type

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)>]

Parameters

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.

Default

None.

Command Mode

IPV4 ACL Extended Access List Configuration Mode.

Usage Guideline

None.

32.4 permit tcp (ip access-list)

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)>]

Parameters

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.

Default

None.

Command Mode

IPV4 ACL Extended Access List Configuration Mode.

Usage Guideline

None.

32.5 deny tcp (ip access-list)

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 <destip-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)>]

Parameters

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.

Default

None.

Command Mode

IPV4 ACL Extended Access List Configuration Mode.

Usage Guideline

None.

32.6 permit udp (ip access-list)

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)>]

Parameters

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.

Default

None.

Command Mode

IPV4 ACL Extended Access List Configuration Mode.

Usage Guideline

None.

32.7 deny udp (ip access-list)

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 <destip-address> | <dest-ip-address> <dest-mask> } [eq <port-number (1-65535)>] ace-priority <integer (1-2147483647)> [dscp <value (0-63)>]

Parameters

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.

Default

None.

Command Mode

IPV4 ACL Extended Access List Configuration Mode.

Usage Guideline

None.

32.8 permit icmp

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)>]

Parameters

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.

Default

None.

Command Mode

IPV4 ACL Extended Access List Configuration Mode.

Usage Guideline

None.

32.9 deny icmp

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)>]

Parameters

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.

Default

None.

Command Mode

IPV4 ACL Extended Access List Configuration Mode.

Usage Guideline

None.

32.10 no ace-priority

This command deletes an ace entry.

Syntax

- no ace-priority <integer (1-2147483647)>

Parameters

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.

Default

None.

Command Mode

IPV4 ACL Extended Access List Configuration Mode.

Usage Guideline

None.

32.11 ipv6 access-list extend

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)>

Parameters

Parameter	Description
<string(31)>	Configures the access-list name.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

32.12 permit ipv6

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)>]

Parameters

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.

Default

None.

Command Mode

IPV6 ACL Extended Access List Configuration Mode.

Usage Guideline

None.

32.13 deny ipv6

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)>]

Parameters

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.

Default

None.

Command Mode

IPV6 ACL Extended Access List Configuration Mode.

Usage Guideline

None.

32.14 permit tcp (ipv6 access-list)

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)>]

Parameters

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.

Default

None.

Command Mode

IPV6 ACL Extended Access List Configuration Mode.

Usage Guideline

None.

32.15 deny tcp (ipv6 access-list)

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)>]

Parameters

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.

Default

None.

Command Mode

IPV6 ACL Extended Access List Configuration Mode.

Usage Guideline

None.

32.16 permit udp (ipv6 access-list)

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)]

Parameters

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.

Default

None.

Command Mode

IPV6 ACL Extended Access List Configuration Mode.

Usage Guideline

None.

32.17 deny udp (ipv6 access-list)

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)>]

Parameters

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.

Default

None.

Command Mode

IPV6 ACL Extended Access List Configuration Mode.

Usage Guideline

None.

32.18 permit icmpv6

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)>]

Parameters

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

Default

None.

Command Mode

IPV6 ACL Extended Access List Configuration Mode.

Usage Guideline

None.

32.19 deny icmpv6

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)>]

Parameters

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.

Default

None.

Command Mode

IPV6 ACL Extended Access List Configuration Mode.

Usage Guideline

None.

32.20 no ace-priority

This command deletes an ace entry.

Syntax

- no ace-priority <integer (1-2147483647)>

Parameters

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.

Default

None.

Command Mode

IPV6 ACL Extended Access List Configuration Mode.

Usage Guideline

None.

32.21 mac access-list extend

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)>

Parameters

Parameter	Description
<string(31)>	Configures the access-list name.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

32.22 permit mac

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)>]

Parameters

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.

Default

None.

Command Mode

MAC ACL Extended Access List Configuration Mode.

Usage Guideline

None.

32.23 deny mac

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)>]

Parameters

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.

Default

None.

Command Mode

MAC ACL Extended Access List Configuration Mode.

Usage Guideline

None.

32.24 no ace-priority

This command deletes an ace entry.

Syntax

- no ace-priority <integer (1-2147483647)>

Parameters

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.

Default

None.

Command Mode

MAC ACL Extended Access List Configuration Mode.

Usage Guideline

None.

32.25 ip access-group

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

Parameters

Parameter	Description
<string(31)>	IP access control list name.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

None.

32.26 ipv6 access-group

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

Parameters

Parameter	Description
<string(31)>	IPv6 access control list name.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

None.

32.27 mac access-group

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

Parameters

Parameter	Description
<string(31)>	MAC access control list name

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

None.

32.28 show access-lists

This command displays the access lists configuration.

Syntax

- show access-lists [{ip | mac | ipv6 } [<string(31)>]]

Parameters

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

Default

None.

Command Mode

Privilege EXEC Mode.

Usage Guideline

None.

33 QoS

33.1 qos

This command enables or disables the QoS subsystem.

Syntax

- qos {enable | disable}

Parameters

Parameter	Description
enable	Enables QoS subsystem
disable	Disables Qos subsystem

Default

By default, this option is enable.

Command Mode

Global Configuration Mode.

Usage Guideline

When disables QoS subsystem, QoS configuration parameter will be clear.
If you enables QoS subsystem after disables, please use the web UI.
How to configure QoS subsystem by web UI is in 11.1 "Global Settings" of chapter 11 "QoS" on Web Reference.

33.2 qos trust (Port trust state settings)

This command sets qos trust mode.

Syntax

- qos trust {cos | dscp | cos-dscp}

Parameters

Parameter	Description
cos	trust cos.
dscp	trust dscp.
cos-dscp	trust cos, if cos not set, trust dscp.

Default

By default, this option is qos trust cos-dscp.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

33.3 priority-map

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)>]

Parameters

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.

Default

- vlanPri

CoS	Queue
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

- ipDscp

DSCP	Queue
0	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	2
9	2
10	2
11	2
12	2
13	2
14	2
15	2
16	3
17	3

DSCP	Queue
18	3
19	3
20	3
21	3
22	3
23	3
24	4
25	4
26	4
27	4
28	4
29	4
30	4
31	4
32	5
33	5
34	5
35	5
36	5
37	5
38	5
39	5
40	6
41	6
42	6
43	6
44	6
45	6
46	6
47	6
48	7
49	7
50	7
51	7
52	7
53	7
54	7
55	7
56	8

DSCP	Queue
57	8
58	8
59	8
60	8
61	8
62	8
63	8

Command Mode

Global Configuration Mode.

Usage Guideline

None.

33.4 scheduler

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)>]}}

Parameters

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.

Default

By default, this option is scheduler sched-algo strict-priority.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

33.5 class-policy

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)>

Parameters

Parameter	Description
<name (23)>	Name of qos policy.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

None.

33.6 qos interface

This command sets the default ingress user priority for the port.

Syntax

- qos interface <iftype> <ifnum> def-user-priority <integer(0-7)>

Parameters

Parameter	Description
iftype	Interface type.
ifnum	Interface number.
def-user-priority	Default ingress user priority for the port.

Default

- 8 ports.

Port	def-user-priority
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0

- 24 ports.

Port	def-user-priority
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0

Port	def-user-priority
16	0
17	0
18	0
19	0
20	0
21	0
22	0
23	0
24	0
25	0
26	0
27	0
28	0

Command Mode

Global Configuration Mode.

Usage Guideline

None.

33.7 match policy - tcp/udp

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)>}]

Parameters

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.

Default

None.

Command Mode

Policy Map Configuration Mode.

Usage Guideline

None.

33.8 match policy - icmp

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 <VLAN-priority-value(0-7)> | dscp <value (0-63)>}]

Parameters

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 <VLAN-priority-value(0-7)>	set tos to value.
dscp <value (0-63)>	set dscp to value.

Default

None.

Command Mode

Policy Map Configuration Mode.

Usage Guideline

None.

33.9 match policy - ip/ospf/pim/protocol type

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-ipv4-address>| <src-ipv4-address> <src-mask> } { any | host <dest-ipv4-address> | <dest-ipv4-address> <dest-mask> } [dscp <dscp-value (0-63)>] [action { vpt <VLAN-priority-value(0-7)> | dscp <value (0-63)>}]

Parameters

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-ipv4-address>| <src-ipv4-address> <src-mask>	By specifying **any**, validation will be performed for all sources. By entering an IPv4 address after **host**, validation will be performed only for packets sent from that specific IPv4 address. By entering an IPv4 address along with a subnet mask, validation will be performed for packets sent from the specified network.
any | host <dest-ipv4-address> | <dest-ipv4-address> <dest-mask>	By specifying **any**, validation will be performed for all destination. By entering an IPv4 address after **host,** validation will be performed only for packets sent to that specific address. By entering an IPv4 address along with a subnet mask, validation will be performed for packets sent to the specified network.
dscp <dscp-value (0-63)>	Differentiated services code point provides the quality of service control.
vpt <VLAN-priority-value(0-7)>	set tos to value.
dscp <value (0-63)>	set dscp to value.

Default

None.

Command Mode

Policy Map Configuration Mode.

Usage Guideline

In the case that you specify both **any** and the other parameters for the source IP address, the parameters excluding **any** are ignored.

Example

This command shows how to match policy for packets with a source MAC address of 00:11:22:33:44:55 and a destination MAC address of 00:AA:BB:CC:DD:EE, belonging to VLAN 100, with a source IP address of

192.168.1.10 and any destination IP address, while setting the VLAN priority value to 5.

```
XX-MUxxTPoE+# configure terminal
XX-MUxxTPoE+(config)# class-policy test
XX-MUxxTPoE+(config-qc-ply)# match policy host 00:11:22:33:44:55 host
00:AA:BB:CC:DD:EE vlan 100 ip host 192.168.1.10 any action vpt 5
XX-MUxxTPoE+(config-qc-ply)#
```

33.10 no match policy

This command clears all policy configuration.

Syntax

- no match policy

Default

None.

Command Mode

Policy Map Configuration Mode.

Usage Guideline

None.

33.11 show priority-map in-priority-type

This command displays the priority mapping to queue.

Syntax

- show priority-map in-priority-type {vlanPri | ipDscp}

Parameters

Parameter	Description
vlanPri	Vlan priority.
ipDscp	DSCP.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

Example

This example shows how to display the VLAN priority of the priority-map.

```
XX-MUxxTPoE+# show priority-map in-priority-type vlanPri

QoS Priority Map Entries
------------------------
InPriorityType  : VlanPriority

InPriority                 : Queue
-------------------------- : -------------
0                          : 1

1                          : 2

2                          : 3

3                          : 4

4                          : 5

5                          : 6

6                          : 7

7                          : 8

XX-MUxxTPoE+#
```

33.12 show class-policy

This command displays the qos policy.

Syntax

- show class-policy [{<name(23)> | interface <iftype> <ifnum>}]

Parameters

Parameter	Description
<name(23)>	Name of qos policy.
iftype	Interface type.
ifnum	Interface number.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

33.13 show scheduler

This command displays the configured Scheduler.

Syntax

- show scheduler

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

33.14 show qos def-user-priority

This command displays the configured default ingress user priority for a port.

Syntax

- show qos def-user-priority [interface <iftype> <ifnum>]

Parameters

Parameter	Description
iftype	Interface type.
ifnum	Interface number.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

None.

33.15 qos trust

This command enable/disable qos trust on port.

Syntax

- qos trust {enable | disable}

Parameters

Parameter	Description
enable	enable qos trust on port.
disable	disable qos trust on port.

Default

By default, this option is qos trust disable.

Command Mode

Interface Configuration Mode.

Usage Guideline

None.

33.16 service-policy

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)>

Parameters

Parameter	Description
<class-policy-name (31)>	Name of qos policy.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

None.

34 Storm control

34.1 Storm-control

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

Parameters

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.

Default

By default, this option is disable.

Command Mode

Interface Configuration Mode.

Usage Guideline

None.

35 Bandwidth control

35.1 Rate-limit

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 }

Parameters

Parameter	Description
output	egress limitation.
input	ingress limitation.
<integer(1-80000000)>	Line rate in kbps.

Default

By default, this option is disable.

Command Mode

Interface Configuration Mode.

Usage Guideline

None.

Panasonic Electric Works Networks Co., Ltd.

P0424-4016