User's Guide

TRENDnet®

12-Port 10G Layer 2 Managed SFP+ Switch

TL2-F7120

Contents

Product Overview

TL2-F7120

Package Contents

In addition to your switch, the package includes:

- Quick Installation Guide
- Power cord
- RJ-45 to RS-232 console cable (1.5m / 5 ft.)
- Rackmount kit

If any package contents are missing or damaged, please contact the retail store, online retailer, or reseller/distributor from which the product was purchased.

Features

TRENDnet's 12-Port 10G Layer 2 Managed SFP+ Switch, model TL2-F7120, offers advanced traffic management controls to meet the evolving demands of SMB networks. This rack-mountable IPv6-ready managed switch comes with an intuitive web-based interface. Advanced management features on this ultra-fast 10G SFP+ switch include LACP to increase bandwidth between switches by grouping ports together, VLANs for segmenting and isolating virtual LAN groups, QoS for traffic prioritization, port bandwidth controls, and SNMP monitoring, making this a powerful solution for any SMB network. Improve voice performance by isolating and prioritizing VoIP traffic from normal data traffic with an easy-to-use voice VLAN feature.

Free up router resources by offloading routing processes to this 10G managed SFP+ switch by using the L2+ IPv4/IPv6 static routing feature to efficiently route traffic at the switch level. Take advantage of the available multicast and IGMP/MLD snooping features to optimize IP surveillance system performance, and minimize network traffic.

TRENDnet's 10G SFP+ switch features 12 x 10GSFP+ slots for high-speed network uplinks or downlink NAS/access server connections, providing a cost-effective solution in adding 10G link capability to an SMB network.

Hardware Design

The 10Gb fiber switch provides 12 x 10G SFP+ slots, a built-in power supply, and 1U rackmount brackets

Switching Capacity

Supports a 240Gbps switch capacity

Smart Fan

The smart fan on the 10G SFP+ switch saves energy and eliminates distracting operating noise by auto adjusting the fan speed and use based on cooling needs

LED Indicators

LED indicators on the 10G SFP+ switch convey port status

Jumbo Frame

Sends larger packets, or Jumbo Frames (up to 9KB) for increased performance

Rackmount Design

Save rack space by mounting 2 x TL2-F7120 into 1U space with the optional ETH-F71 dual mount bracket (sold separately)

IPv6 Ready

This 10G SFP+ switch supports Ipv6 configuration and Ipv6 neighbor discovery

IP Routing

Supports inter-VLAN routing and Ipv4/Ipv6 static routing

Traffic Management

A broad range of network configurations are supported by this 10G managed SFP+ switch: 802.1ax link aggregation, , 802.1Q VLAN, Voice VLAN, RSTP, MSTP, Loopback Detection, GVRP, 802.1p Class of Service (CoS), port bandwidth management, and QoS queue scheduling

Troubleshooting

A convenient cable diagnostic test and traffic statistics aid in network troubleshooting

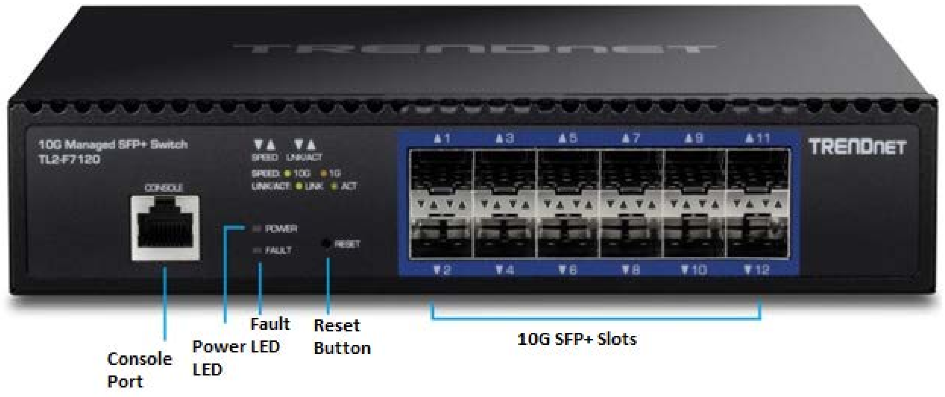
Access Control

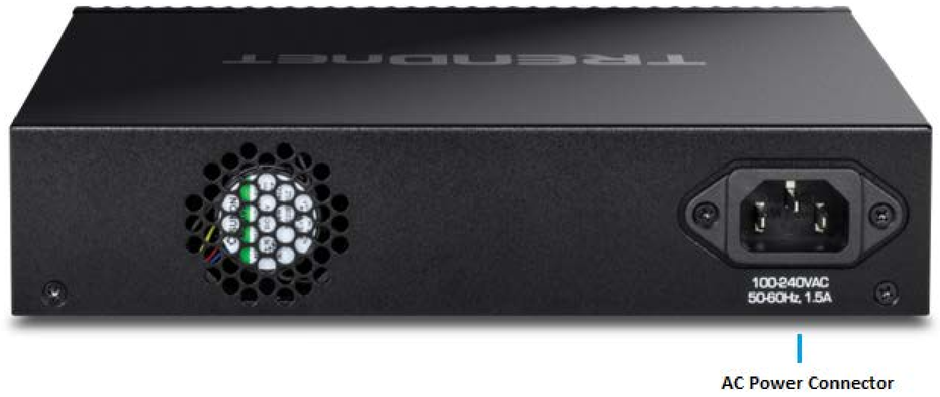
Features such as IPv4/IPv6 ACL, port security (mac entry restriction), 802.1X, TACACS+, and RADIUS are compatible with layered access controls

Monitoring

RMON, SNMP, SNMP Trap, and Port Mirroring, and DDM are supported on the 10G SFP+ switch

Product Hardware Features





- **AC Power Connector –** Connect the AC power cord to the connector and the other side into a power outlet. (Input: 100~240VAC, 50/60Hz)
- **Reset Button –** Press and hold this button for 15 seconds and release to reset the switch to factory defaults.
- **10G SFP+ Slots (1-12) –** Supports 1000BASE-X (Gigabit Ethernet over fiber) or 10GBASE-X (10 Gigabit Ethernet over fiber SFP/mini-GBIC modules for connectivity.
- **Console port –** Use the included RJ-45 to RS-232 serial console cable to access the out-of-band command line interface management.

- **Diagnostic LED Indicators**

Power LED

On (Green) :	The device is receiving power and operating normally.
Blinking (Green)	The device is booting and performing a system self-test.
Off :	The device is not receiving power and turned off.

Fault LED

On (Orange) :	Indicates that there is a hardware issue with the device.
Off :	Indicates no hardware issues detected and the device hardware is operating normally.

- **10G SFP+ Slots 1-12 Speed / Link & Activity**

On (Green) :	The link speed is established at 10Gbps (10,000Mbps) (Left side LED per slot)
On (Orange) :	The link speed is established at 1Gbps (1000Mbps). (Left side LED per slot)
Blinking :	The SFP/SFP+ slot is transmitting or receiving data. (Right side LED per slot)
Off	The SFP/SFP+ link is disconnected or not established.

Key Features

High-Speed 10G SFP+

Offers 12 x 10G SFP+ slots for high-speed network uplinks or downlink NAS/access server connections providing a cost-effective solution in adding 10G link capability to an SMB network.

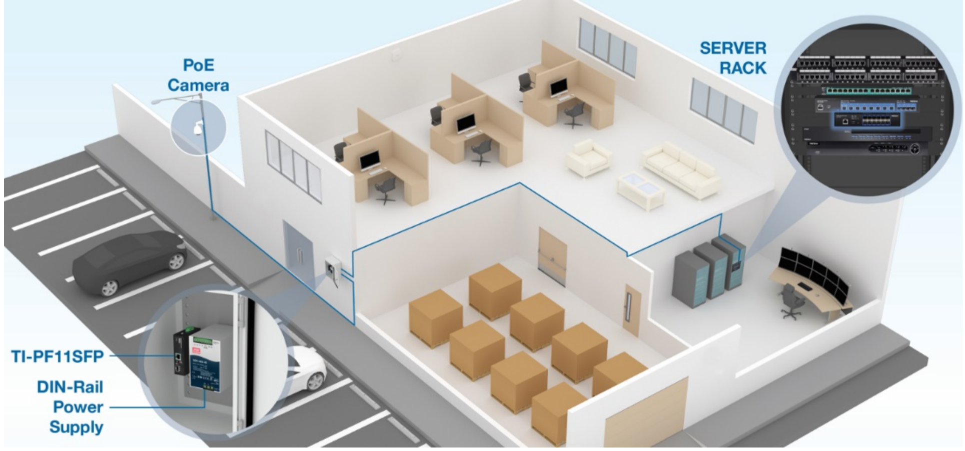
L2 Management

Fully configurable using the web-based management interface or CLI for management flexibility and streamlining configuration deployment to multiple switches.

Integration Flexibility

Managed features include access control lists, VLAN, IGMP snooping, QoS, RMON, SNMP trap, and syslog for monitoring and flexible network integration.

Application Diagram



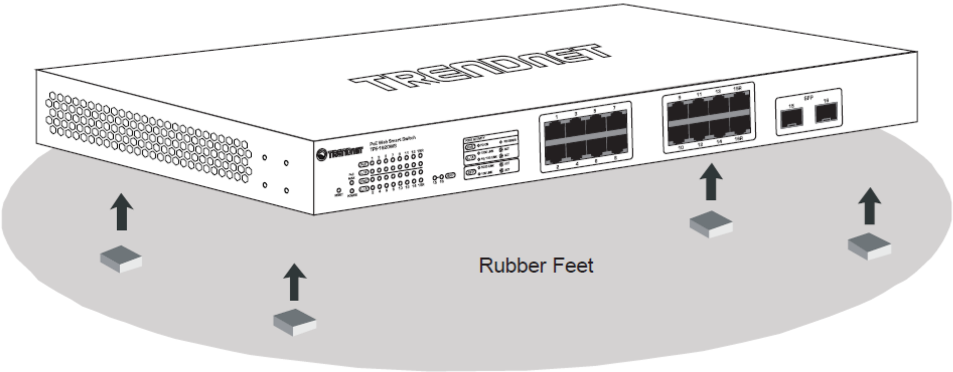
Switch Installation

Desktop Hardware Installation

Note: *The device images displayed below may be different from your switch model.*

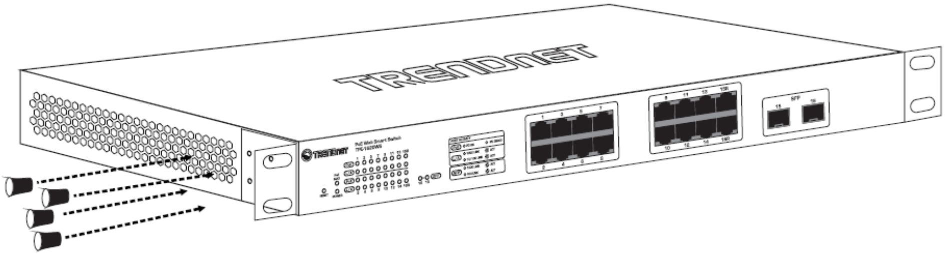
The site where you install the hub stack may greatly affect its performance. When installing, consider the following pointers:

- Install the Switch in a fairly cool and dry place.
- Install the Switch in a site free from strong electromagnetic field generators (such as motors), vibration, dust, and direct exposure to sunlight.
- Leave at least 10cm of space at the front and rear of the hub for ventilation.
- Install the Switch on a sturdy, level surface that can support its weight, or in an EIA standard-size equipment rack. For information on rack installation, see the next section, Rack Mounting.
- When installing the Switch on a level surface, attach the rubber feet to the bottom of each device. The rubber feet cushion the hub and protect the hub case from scratching.

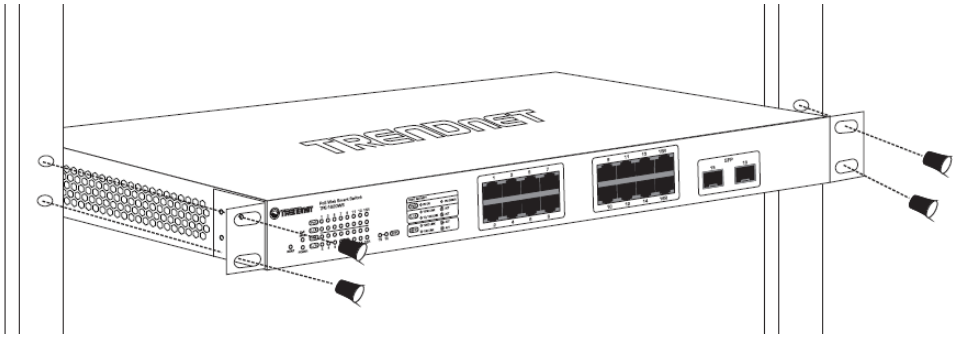


Rack Mount Hardware Installation

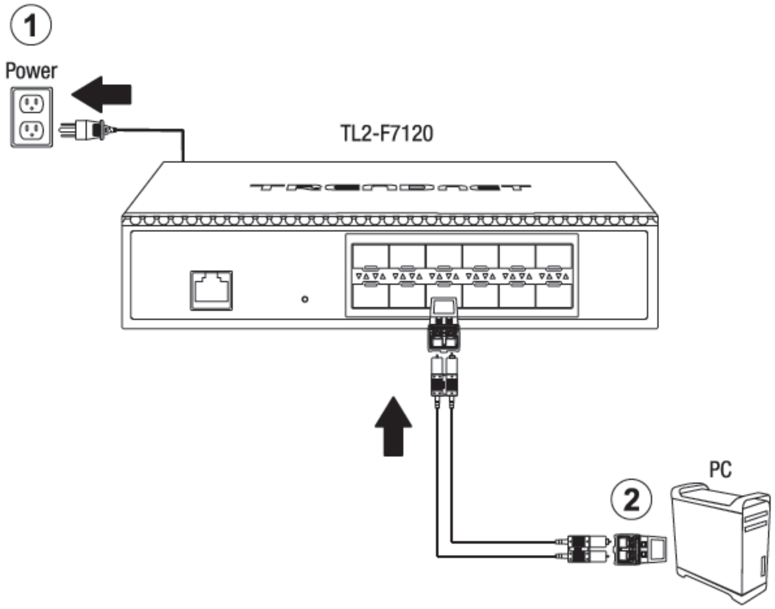
The switch can be mounted in an EIA standard-size, 19-inch rack, which can be placed in a wiring closet with other equipment. Attach the mounting brackets at the switch's front panel (one on each side), and secure them with the provided screws.



Then, use screws provided with the equipment rack to mount each switch in the rack.

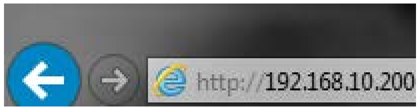


Basic Installation



3. Assign a static IP address to your computer's network adapter in the subnet of 192.168.10.x (e.g. 192.168.10.25) and a subnet mask of 255.255.255.0.

4. Open your web browser, and type the IP address of the switch in the address bar, and then press **Enter**. The default IP address is **192.168.10.200**.



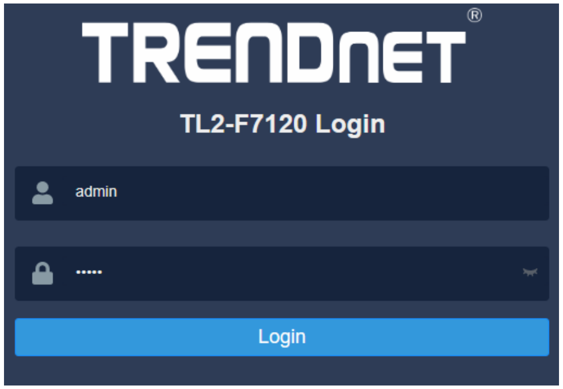
http://192.168.10.200

5. Enter the User Name and Password, and then click **Login.** By default:

User Name: **admin**

Password: **admin**

Note: *User name and password are case sensitive.*



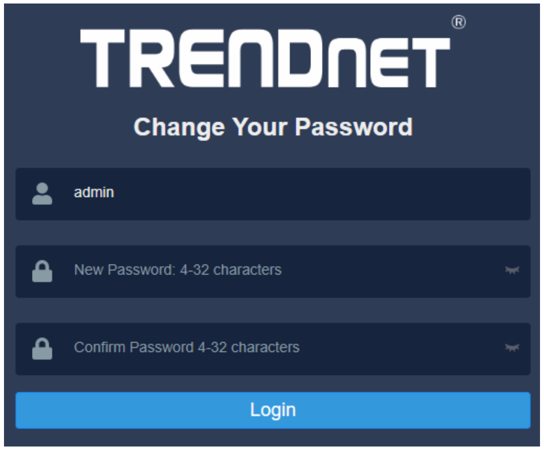
TL2-F7120 Login

admin

•••••

6. You will be prompted to change the default admin password. Enter the admin password in the fields provided and click **Login**.

Note: *You will need to login to the switch management with updated password moving forward.*



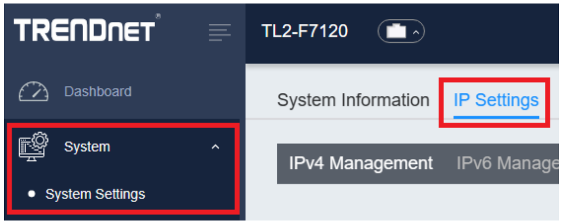
Change Your Password

admin

New Password: 4-32 characters

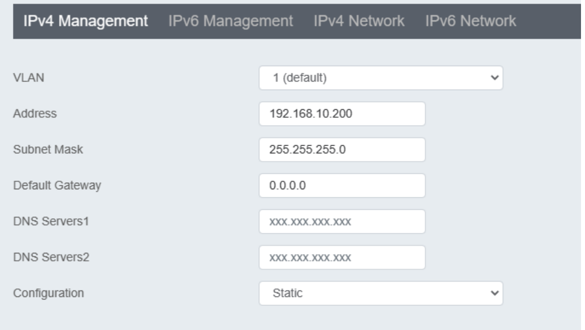
Confirm Password 4-32 characters

7. Click **System,** click **System Settings,** and then click **IP Settings**.



8. Configure the switch IP address settings to be within your network subnet, then click **Apply.**

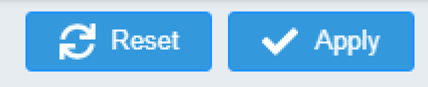
Note: *You may need to modify the static IP address settings of your computer's network adapter to IP address settings within your subnet in order to regain access to the switch.*



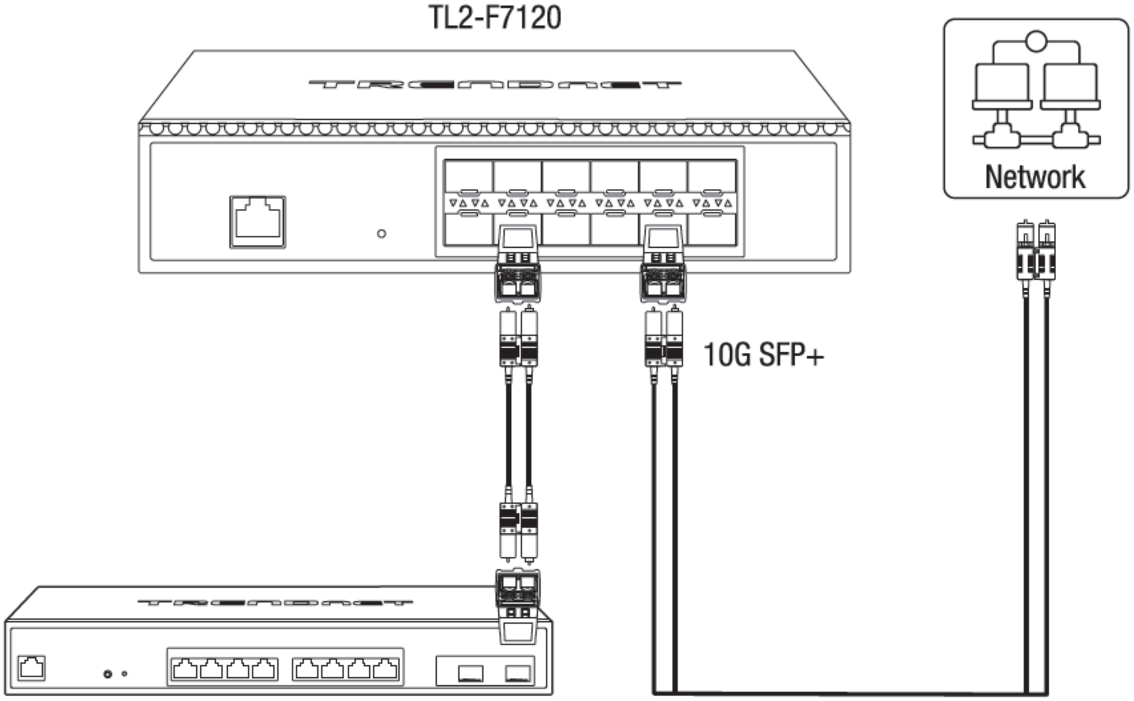
VLAN	1 (default)
Address	192.168.10.200
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Servers1	xxx.xxx.xxx.xxx
DNS Servers2	xxx.xxx.xxx.xxx
Configuration	Static

9. To save configuration setting, click **Apply** at the top right of the page.

Note: *You can also click* ***Reset*** *to discard your changes and revert back to the previous configurations ettings.*



Connectivity Example

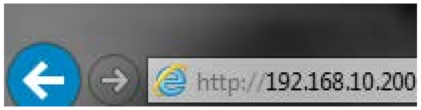


Configure your switch (Web-based UI)

Access your switch management page

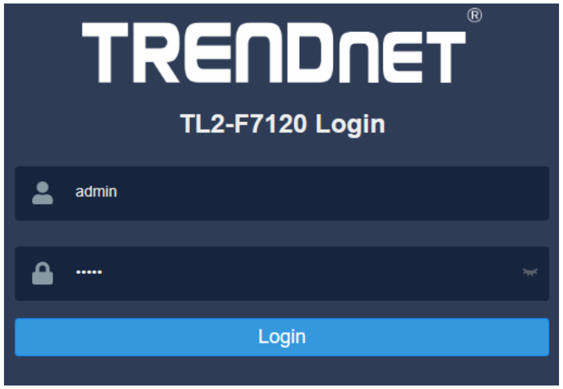
Note: *Your switch default management IP address* *http://192.168.10.200* *is accessed through the use of your Internet web browser (e.g. Microsoft Edge®, Firefox®, Chrome™, Safari®, and Opera™) and will be referenced frequently in this User's Guide.*

1. Open your web browser and go to the IP address http://192.168.10.200. Your switch will prompt you for a user name and password.



2. Enter the user name and password. By default:

   User Name: **admin**
   Password: **admin**
   Note: *User Name and Password are case sensitive.*



System Info

View your switch status information

Dashboard

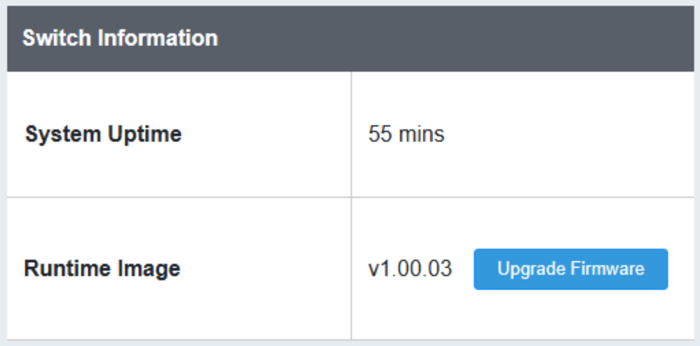
You may want to check the general system information of your switch such as firmware version, CPU/memory utilization, IP/MAC information, and system uptime. Other information includes H/W version, RAM/Flash size, administration information, general feature status, and fan status.

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Dashboard**.

System Information

- **System Uptime** – The duration your switch has been running continuously without a restart/power cycle (hard or soft reboot) or reset.
- **Runtime Image:** The current software or firmware version your switch is running. Clicking the Upgrade Firmware button will open the firmware update page to upload device firmware.

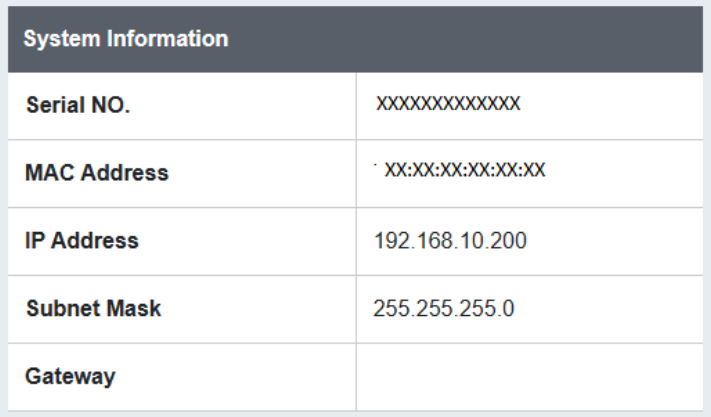


Switch Information

System Uptime	55 mins
Runtime Image	v1.00.03

System Information

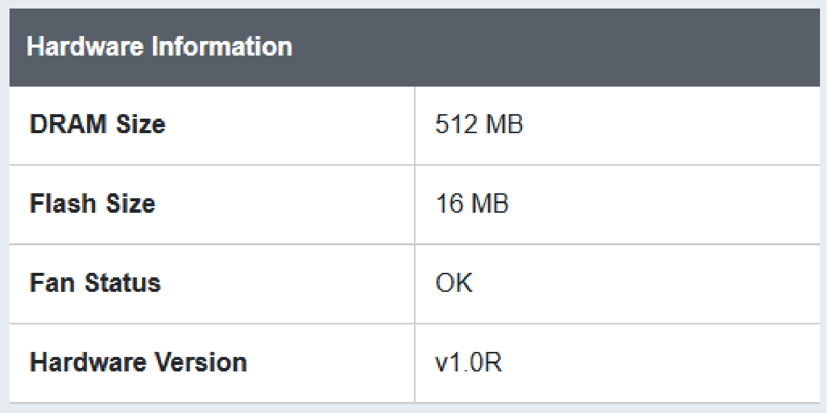
- **Serial NO.** – Displays the switch serial number.
- **MAC Address:** Displays the switch system MAC address.
- **IP Address** – Displays the current IPv4 address assigned to your switch.
- **Subnet Mask** – Displays the current IPv4 subnet mask assigned to your switch.
- **Gateway** – Displays the current gateway address assigned to your switch.



System Information	
Serial NO.	XXXXXXXXXXXXX
MAC Address	XX:XX:XX:XX:XX:XX
IP Address	192.168.10.200
Subnet Mask	255.255.255.0
Gateway	

Hardware Information

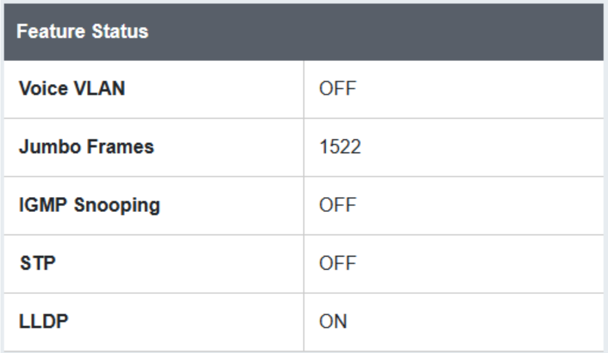
- **DRAM Size:** Displays your switch RAM memory size.
- **Flash Size:** Displays your switch Flash memory size.
- **Fan Status:** Displays the current status of the switch fan.
- **Hardware Version:** Displays your switch hardware version.
-



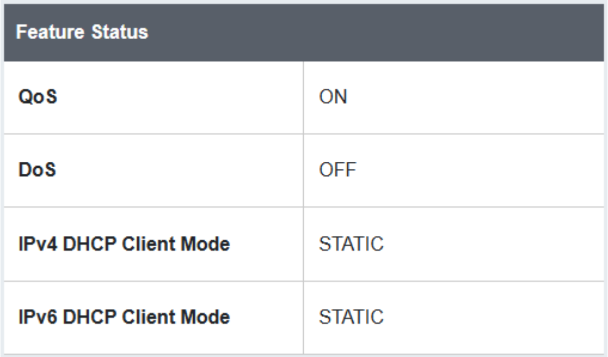
Hardware Information	
DRAM Size	512 MB
Flash Size	16 MB
Fan Status	OK
Hardware Version	v1.0R

Feature Status

- **Voice VLAN:** Displays if the voice VLAN feature is enabled or disabled on your switch.
- **Jumbo Frames:** Displays the current jumbo frame size configured on your switch. 1522 bytes is the default indicating that jumbo frames is disabled.
- **IGMP Snooping/STP/LLDP/QoS/DoS**: Displays if these features are enabled or disabled on your switch.
- **IPv4 DHCP Client Mode:** Displays if the switch is to IPv4 DHCP client mode automatic IPv4 addressing. Static indicates that the switch using a static IPv4 address configuration.
- **IPv6 DHCP Client Mode:** Displays if the switch is to IPv6 DHCP client mode automatic IPv6 addressing. Static indicates that the switch using a static IPv6 address configuration.



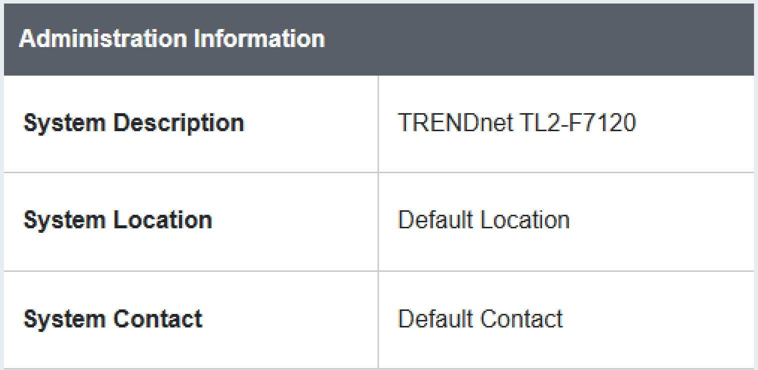
Feature Status	
Voice VLAN	OFF
Jumbo Frames	1522
IGMP Snooping	OFF
STP	OFF
LLDP	ON



Feature Status	
QoS	ON
DoS	OFF
IPv4 DHCP Client Mode	STATIC
IPv6 DHCP Client Mode	STATIC

Administration Information

- **System Description:** Displays the identifying system description of your switch. This information can be modified under the **System > System Settings > System Information** section.
- **System Location** - Displays the identifying system location of your switch. This information can be modified under the **System > System Settings > System Information** section.
- **System Contact –** Displays the identifying system contact or system administrator of your switch. This information can be modified under the **System > System Settings > System Information** section.



Administration Information	
System Description	TRENDnet TL2-F7120
System Location	Default Location
System Contact	Default Contact

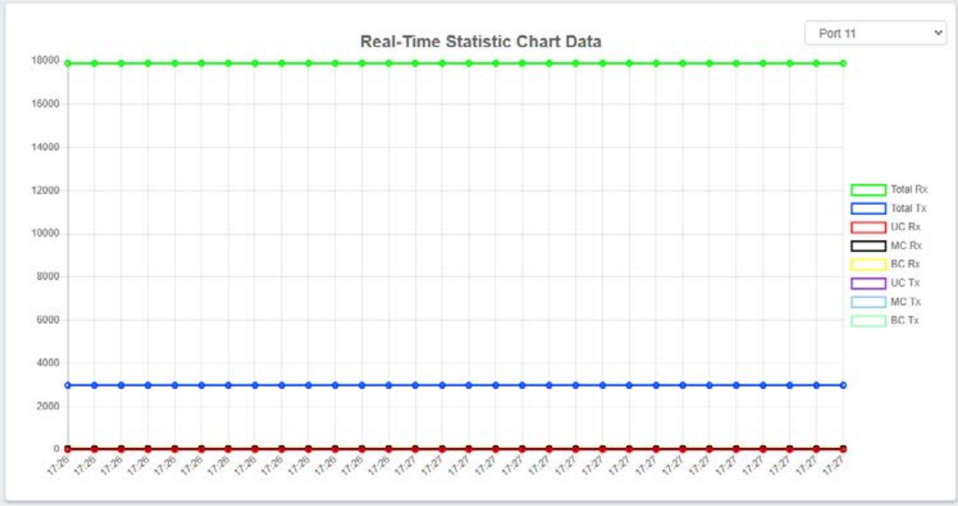
Real-Time Statistics

Dashboard > Real-Time Statistic

Dashboard Real-Time Statistic

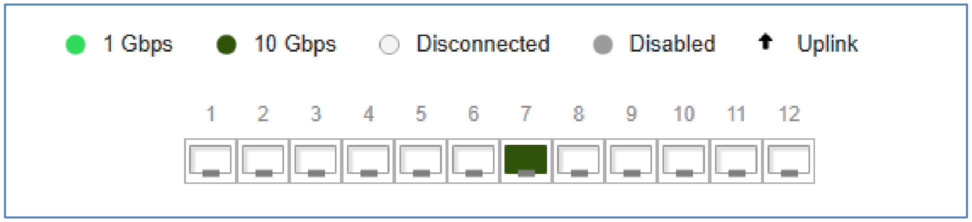
The graph displays real-time statistics data by port and the following information.

- **Total Rx**: Total amount of data received the selected port.
- **Total Tx**: Total amount of data transmitted by the selected port.
- **UC Rx**: Total amount of unicast frames received the port.
- **MC Rx**: Total amount of multicast frames received the port.
- **BC Rx**: Total amount of broadcast frames received the port.
- **UC Tx**: Total amount of unicast frames transmitted the port.
- **MC Tx**: Total amount of multicast frames transmitted the port.
- **BC Tx**: Total amount of broadcast frames transmitted the port.



View SFP/SFP+ Status

At top of the switch configuration page, click the button to view the SFP/SFP+ link and slot status.



System

Set your system information

System > System Settings > System Information.

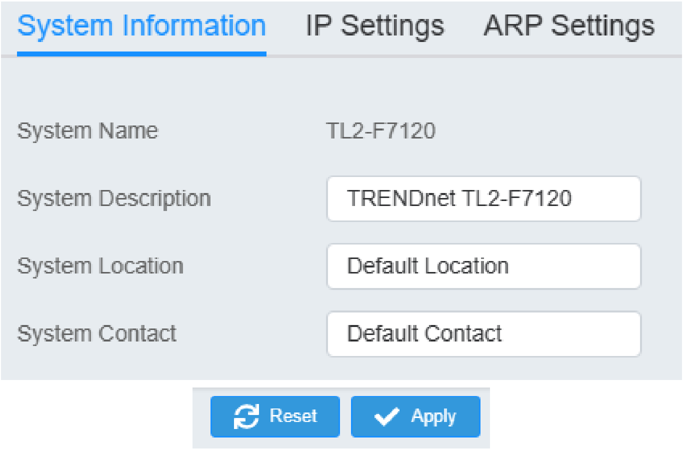
This section explains how to assign a description, location, and contact information for the switch. This information helps in identifying each specific switch among other switches in the same local area network. Entering this information is optional.

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System**, click **System Settings,** and click on **System Information**.

3. Review the settings. When you have completed making changes, click **Apply** at the top right to save the configuration settings.

- **System Name** - Specifies a name for the switch which is the model number and cannot be modified.
- **System Description** - Specifies the identifying description for the switch. The setting is optional.
- **System Location** - Specifies the location of the switch. The setting is optional.
- **System Contact** - Specifies the name of the network administrator responsible for managing the switch. The setting is optional.



System Name	TL2-F7120
System Description	TRENDnet TL2-F7120
System Location	Default Location
System Contact	Default Contact

Set your IPv4 settings

System > System Settings > IP Settings > IPv4 Management

This section allows you to change your switch IPv4 address settings. Typically, the IP address settings should be changed to match your existing network subnet in order to access the switch management page on your network.

Default Switch IPv4 Address: 192.168.10.200

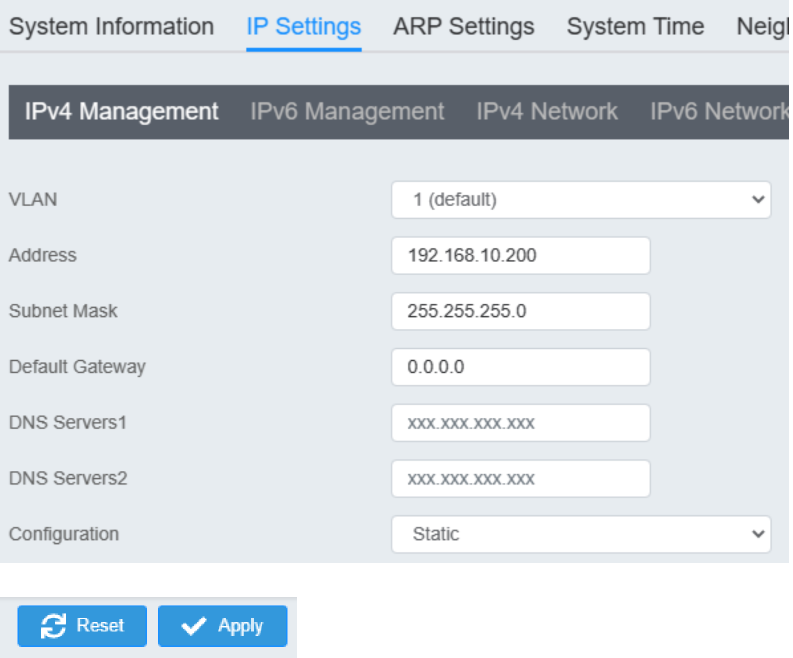
Default Switch IPv4 Subnet Mask: 255.255.255.0

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System**, click **System Settings**, click **IP Settings**, and click on **IPv4 Management**.

3. Review the settings. When you have completed making changes, click **Apply** at the top right to save the configuration settings.

- **VLAN:** Click the drop-down select the management VLAN ID. ***Note:*** *By default, the management VLAN ID is 1. Only one VLAN ID can be assigned as the management VLAN for the switch allowing access to the switch management configuration page and Telnet/SSH management.*
- **System IP Address:** Enter the new switch IP address. This is the IPv4 address of the management VLAN IP interface. (e.g. *192.168.200.200*)
- **System Subnet Mask:** Enter the new switch subnet mask. This is the IPv4 address of the management VLAN IP interface. (e.g. *255.255.255.0*)
- **System Default Gateway:** Enter the default gateway IP address of the switch. (e.g. 192.168.200.1 or typically your router/gateway to the Internet).
- **DNS Servers1:** Enter the IPv4 address of the primary DNS server.
- **DNS Servers2:** Enter the IPv4 address of the secondary DNS server.
- **Configuration:** Click the drop-down list and select **Static** to manually specify your IP address settings or **DHCP** to allow your switch to obtain IP address settings automatically from a DHCP server on your network.



VLAN	1 (default)
Address	192.168.10.200
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DNS Servers1	xxx.xxx.xxx.xxx
DNS Servers2	xxx.xxx.xxx.xxx
Configuration	Static

Set your IPv6 settings

System > System Settings > IP Settings > IPv4 Management

Internet Protocol version 6 (IPv6) is a new IP protocol designed to replace IP version 4 (IPv4). The IPv6 address protocol meets the current requirements of new applications and the never ending growth of the Internet. The IPv6 address space makes more addresses available but it must be approached with careful planning. Successful deployment of IPv6 can be achieved with existing IPv4 infrastructures. With proper planning and design, the transition between IP version 4 and 6 is possible today as well.

Use the **IPv6 System Settings** page to configure the IPv6 network interface, which is the logical interface used for in-band connectivity with the switch via all of the switch's front-panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front-panel ports through which traffic is switched or routed.

1. Log into your switch management page (see "Access your switch management page" on page 9).

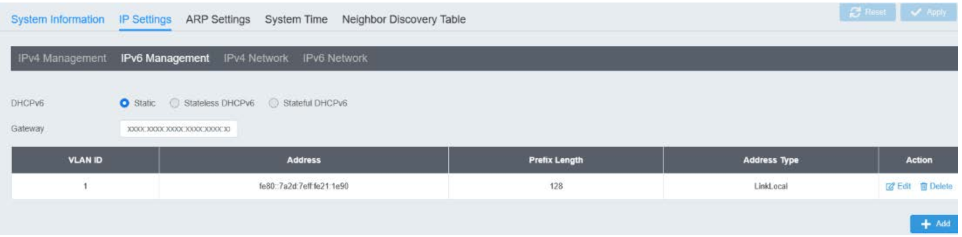
2. Click on **System**, click **System Settings**, click **IP Settings**, and click on **IPv6 Management**.

3. Review the settings. When you have completed making changes, click **Apply** to save the settings.

- **DHCPv6:** Select the IPv6 address configuration for the switch, **Static**, **Stateless DHCPv6,** or **Stateful DHCPv6.** If selecting **Static**, enter the IPv6 gateway address in the **Gateway** field.
    - **Static:** Assign a static IPv6 management interface address to the switch along with the IPv6 default gateway address.
    - **Stateless DHCPv6:** Obtain configuration settings automatically from a stateless DHCPv6 server along SLAAC server.
    - **Stateful DHCPv6:** Obtain IPv6 address and configuration settings automatically from stateful DHCPv6 server.

The default entry in the table is the IPv6 link local address assigned to the switch. You can click **Edit** next to the entry to edit or **Delete** to remove the entry.

Additionally, you can add a new IPv6 management interface address by click **Add** and entering the IPv6 address and the prefix length.



DHCPv6 ● Static ○ Stateless DHCPv6 ○ Stateful DHCPv6

Gateway xxxx:xxxx:xxxx:xxxx:xxxx:xx

VLAN ID	Address	Prefix Length	Address Type	Action
1	fe80::7a2d:7eff:fe21:1e90	128	LinkLocal	Edit Delete

Create additional IPv4 address interfaces

System > System Settings > IP Settings > IPv4 Network

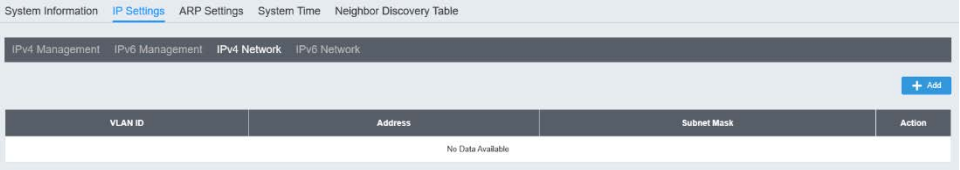
The switch supports layer 3 network features such as static IPv4/IPv6 routing and inter-VLAN routing but not dynamic routing protocols. This section allows you to create additional IPv4 address interfaces and assign to VLAN interfaces.

1. Log into your switch management page (see "Access your switch management page" on page 9).

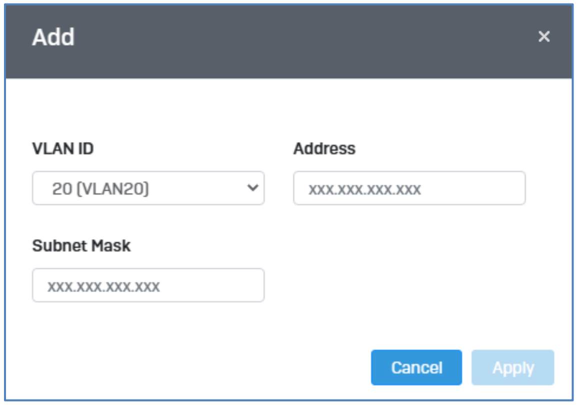
2. Click on **System**, click **System Settings**, click **IP Settings**, and click on **IPv4 Network**.

3. To add a new IPv4 address interface and assign to a VLAN, click **Add**.

Note: *Before you can assign IPv4 address interfaces to VLANs, you must create additional VLAN first. You can create VLANs under the Network > VLAN section.*



VLAN ID	Address	Subnet Mask	Action
No Data Available			



VLAN ID: 20 (VLAN20)

Address: xxx.xxx.xxx.xxx

Subnet Mask: xxx.xxx.xxx.xxx

- **VLAN ID:** Click the drop-down list to select a VLAN ID to assign the IPv4 address interface.
- **Address:** Enter the IPv4 address to assign to the VLAN. (ex: 192.168.20.254)
- **Subnet Mask:** Enter the IPv4 subnet mask to assign to the VLAN. (ex: 255.255.255.0)

Click **Apply** to save the settings.

Note: *After the IPv4 address interface is assigned to the VLAN, the local interface route is created automatically. Also, note that interface routes are not active until a physical link to the VLAN interface is detected on the switch.*

Create additional IPv6 address interfaces

System > System Settings > IP Settings > IPv6 Network

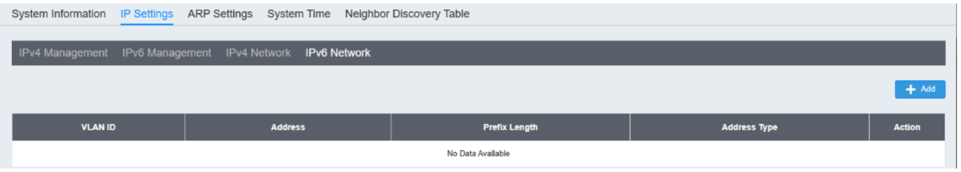
The switch supports layer 3 network features such as static IPv4/IPv6 routing and inter-VLAN routing but not dynamic routing protocols. This section allows you to create additional IPv6 address interfaces and assign to VLAN interfaces.

1. Log into your switch management page (see "Access your switch management page" on page 9).

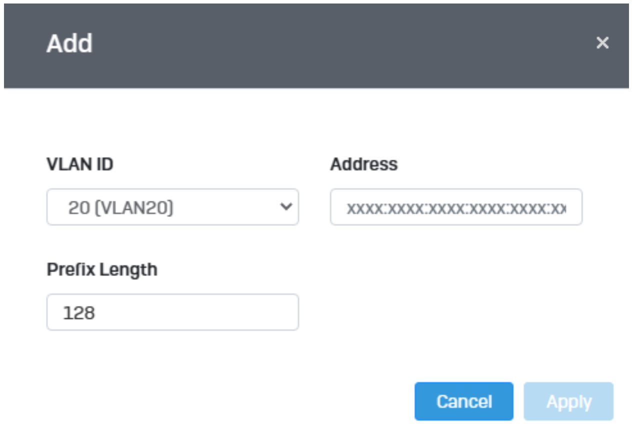
2. Click on **System**, click **System Settings**, click **IP Settings**, and click on **IPv6 Network**.

3. To add a new IPv6 address interface and assign to a VLAN, click **Add**.

Note: *Before you can assign IPv6 address interfaces to VLANs, you must create additional VLAN first. You can create VLANs under the Network > VLAN section.*



VLAN ID	Address	Prefix Length	Address Type	Action
No Data Available				



VLAN ID: 20 (VLAN20)

Address: xxxx:xxxx:xxxx:xxxx:xxxx:xx

Prefix Length: 128

- **VLAN ID:** Click the drop-down list to select a VLAN ID to assign the IPv6 address interface.
- **Address:** Enter the IPv6 address to assign to the VLAN. (ex: 192.168.20.254)
- **Prefix Length:** Enter the IPv6 prefix length.

Click **Apply** to save the settings.

Note: *After the IPv4 address interface is assigned to the VLAN, the local interface route is created automatically. Also, note that interface routes are not active until a physical link to the VLAN interface is detected on the switch.*

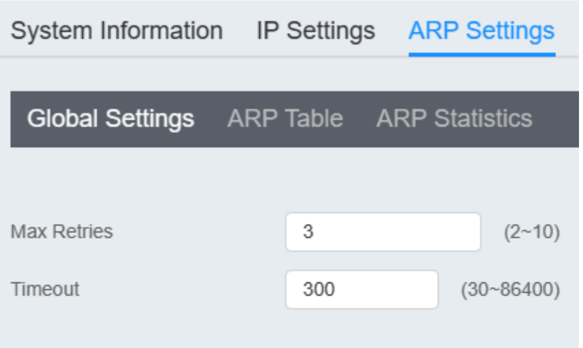
Configure ARP settings

System > System Settings > ARP Settings > Global Settings

The ARP configuration settings allow you to configure the ARP global settings of the switch, add static ARP entries, and check ARP statistics.

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System**, click **System Settings**, click **ARP Settings**, and click on **Global Settings**.



Max Retries	3	(2~10)
Timeout	300	(30~86400)

- **Max Retries:** Configures the max. number of retries to resolve ARP requests.
- **Timeout:** Configures the amount of time the dynamic ARP entry is removed from the ARP table when ARP cannot be resolved.

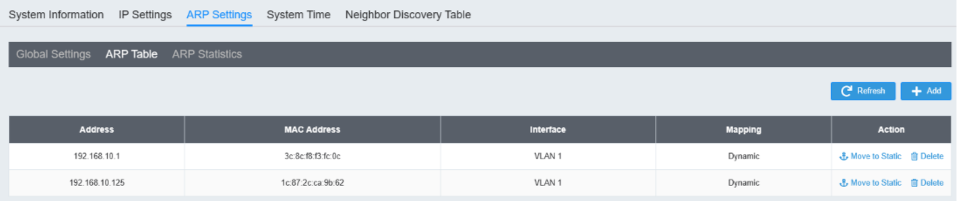
Add a static ARP entry

System > System Settings > ARP Settings > ARP Table

1. Log into your switch management page (see "Access your switch management page" on page 9).

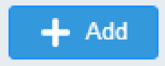
2. Click on **System**, click **System Settings**, click **ARP Settings**, and click on **ARP Table**.

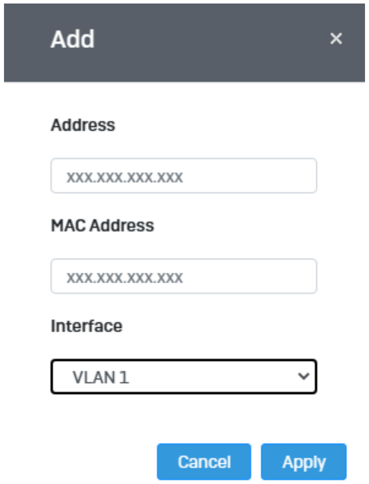
3. In the ARP table, you can view the dynamic and static ARP entries that already exist. If there is a dynamic ARP entry you would like to map as a static entry, next to the entry under the Action column, click **Move to Static.** You can also click **Delete** to remove the ARP entry from the ARP table.



Address	MAC Address	Interface	Mapping	Action
192.168.10.1	3c:8c:f8:f3:fc:0c	VLAN 1	Dynamic	Move to Static Delete
192.168.10.125	1c:87:2c:ca:9b:62	VLAN 1	Dynamic	Move to Static Delete

To add a new static ARP entry that does not exist, click on **Add.**





Address

xxx.xxx.xxx.xxx

MAC Address

xxx.xxx.xxx.xxx

Interface

VLAN 1

- **Address:** Enter the IPv4 address for the static ARP entry.
- **MAC Address:** Enter the MAC address for the static ARP entry.
- **Interface:** Click the interface drop-down list and select the VLAN to assign the static ARP entry.

Click **Apply** to save the static ARP entry to the ARP table.

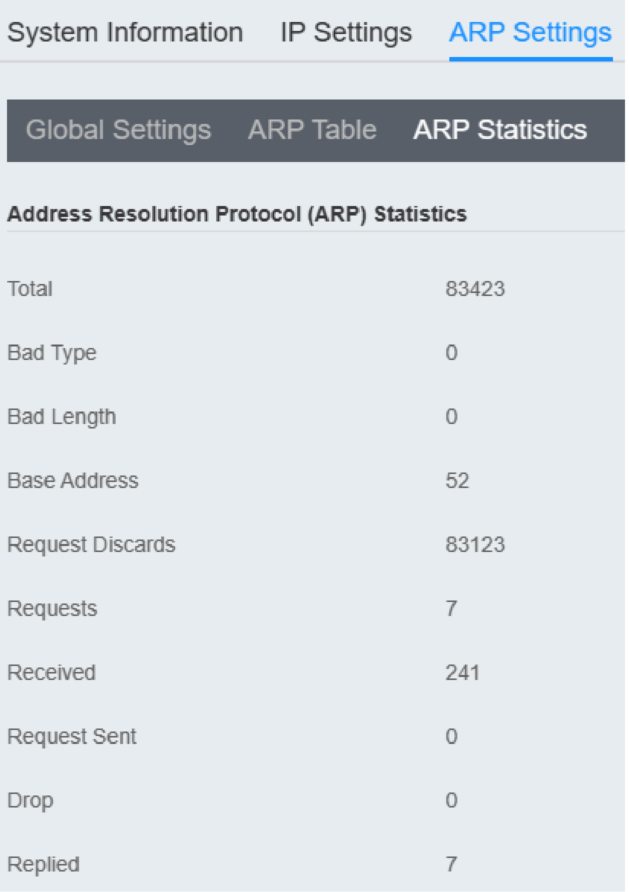
View ARP Statistics

System > System Settings > ARP Settings > ARP Statistics

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System**, click **System Settings**, click **ARP Settings**, and click on **ARP Statistics**.

3. You can view the ARP statistics in the information list.



Address Resolution Protocol (ARP) Statistics

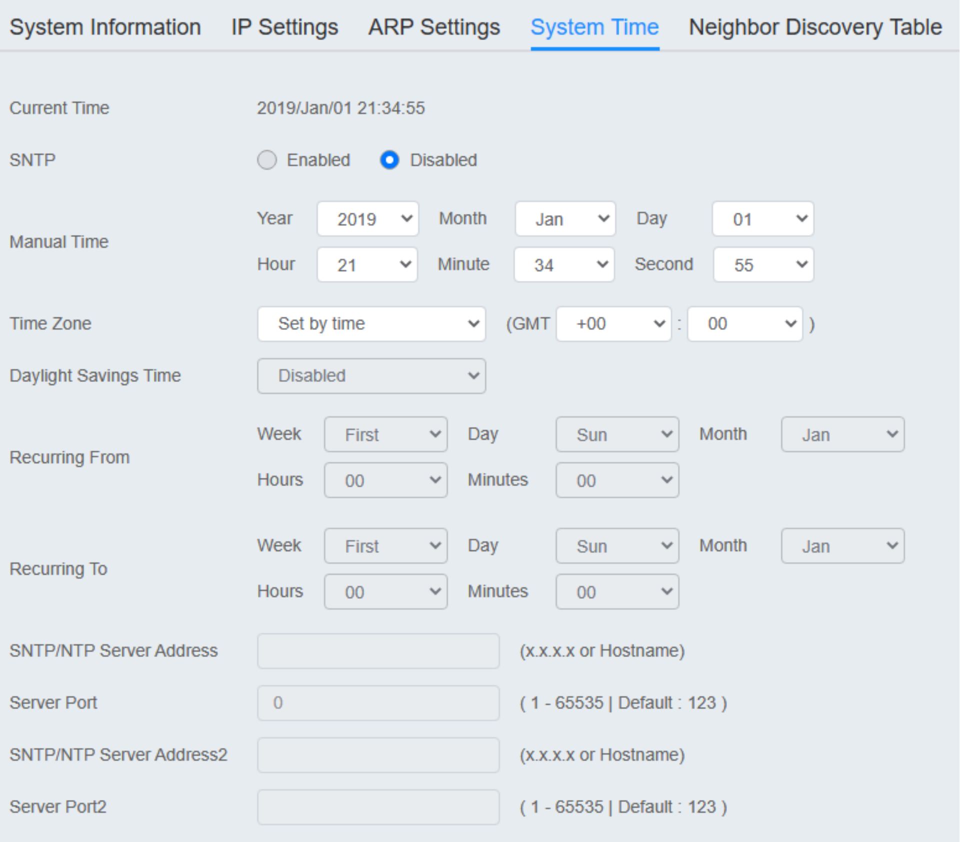
Total	83423
Bad Type	0
Bad Length	0
Base Address	52
Request Discards	83123
Requests	7
Received	241
Request Sent	0
Drop	0
Replied	7

Configure the system time and date settings

System > System Settings > System Time

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System**, click **System Settings** and click **System Time.**



Current Time	2019/Jan/01 21:34:55
SNTP	○ Enabled ● Disabled
Manual Time	Year 2019 Month Jan Day 01 Hour 21 Minute 34 Second 55
Time Zone	Set by time (GMT +00 : 00)
Daylight Savings Time	Disabled
Recurring From	Week First Day Sun Month Jan Hours 00 Minutes 00
Recurring To	Week First Day Sun Month Jan Hours 00 Minutes 00
SNTP/NTP Server Address	(x.x.x.x or Hostname)
Server Port	0 (1 - 65535 | Default : 123)
SNTP/NTP Server Address2	(x.x.x.x or Hostname)
Server Port2	(1 - 65535 | Default : 123)

- **Current Time:** Displays the current system time and date.
- **SNTP**: Select enabled to obtain time and date settings from an SNTP server.

***Note:** Ensure that the correct IP default gateway and DNS configuration are correct for the switch to reach the Internet and resolve host names settings before enable SNTP.*

- **Manual Time:** If SNTP is not used to obtain time and settings, you can manually enter the time and date settings in this section.
- **Time Zone:** Click the drop-down list to select your time zone which can be set by country or offset. This must be selected for both SNTP and manual time settings.
- **Daylight Savings Time:** If daylight savings time applies to your region, click the drop-down list and select Recurring, then specify the time period when daylight savings time should be applied in the Recurring From and Recurring To fields provided. This can be set for either SNTP or Manual time configuration.
- **SNTP/NTP Server Address:** If using SNTP, enter the primary SNTP or NTP server IP address or hostname.

  ***Note:** Ensure that the correct IP default gateway and DNS configuration are correct for the switch to reach the Internet and resolve host names settings before enable SNTP.*
- **Server Port:** If using SNTP, enter the primary SNTP server port. Default is 123.
- **SNTP/NTP Server Address2:** If using SNTP, enter the secondary SNTP or NTP server IP address or hostname.

  ***Note:** Ensure that the correct IP default gateway and DNS configuration are correct for the switch to reach the Internet and resolve host names settings before enable SNTP.*
- **Server Port2:** If using SNTP, enter the secondary SNTP server port. Default is 123.

Click **Apply** to save the configuration settings.

IPv6 Neighbor Discovery

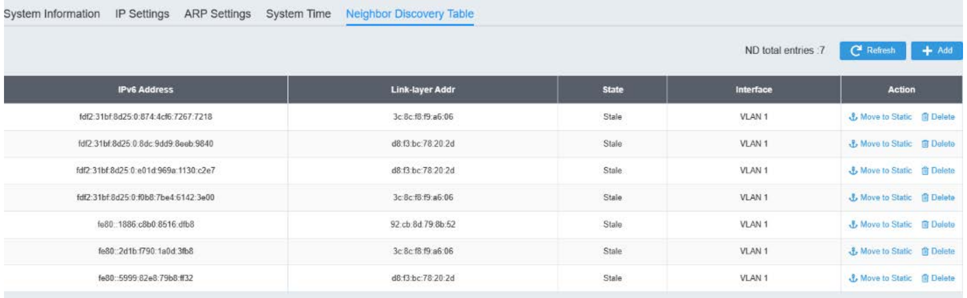
System > System Settings > Neighbor Discovery Table

The IPv6 neighbor discovery table allows you automatically discover IPv6 devices connected automatically.

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System**, click **System Settings** and click **Neighbor Discovery Table.**

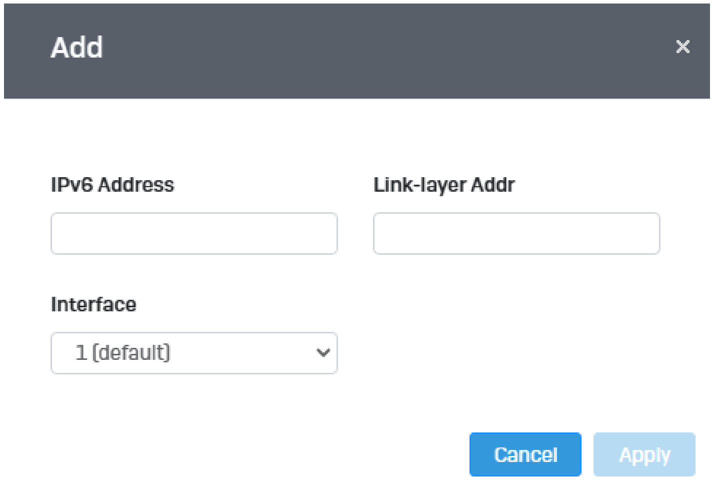
3. In the ARP table, you can view the dynamic and static IPv6 neighbor entries that already exist. If there is a dynamic IPv6 neighbor entry you would like to map as a static entry, next to the entry under the Action column, click **Move to Static.** You can also click **Delete** to remove the entry from the table.



ND total entries :7

IPv6 Address	Link-layer Addr	State	Interface	Action
fdf2:31bf:8d25:0:874:4cf6:7267:7218	3c:8c:f8:f9:a6:06	Stale	VLAN 1	Move to Static Delete
fdf2:31bf:8d25:0:8dc:9dd9:8eeb:9840	d8:f3:bc:78:20:2d	Stale	VLAN 1	Move to Static Delete
fdf2:31bf:8d25:0:e01d:969a:1130:c2e7	d8:f3:bc:78:20:2d	Stale	VLAN 1	Move to Static Delete
fdf2:31bf:8d25:0:f0b8:7be4:6142:3e00	3c:8c:f8:f9:a6:06	Stale	VLAN 1	Move to Static Delete
fe80::1886:c8b0:8516:dfb8	92:cb:8d:79:8b:52	Stale	VLAN 1	Move to Static Delete
fe80::2d1b:f790:1a0d:3fb8	3c:8c:f8:f9:a6:06	Stale	VLAN 1	Move to Static Delete
fe80::5999:82e8:79b8:ff32	d8:f3:bc:78:20:2d	Stale	VLAN 1	Move to Static Delete

To add a new static IPv6 neighbor entry that does not exist, click on **Add.**



- **IPv6 Address:** Enter the IPv6 address for the neighbor entry.
- **Link-layer Addr:** Enter the link-layer address for the neighbor entry.
- **Interface:** Click the drop-down list and select the VLAN interface to assign the IPv6 neighbor entry.

Click **Apply** to save the entry to the table.

Configure web timeout settings

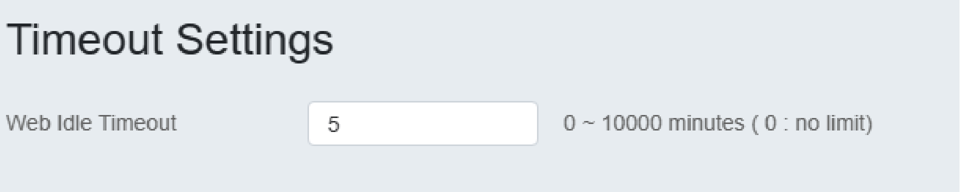
System > Timeout

The web timeout allows you to configure the maximum idle time allowed in the switch management configuration page before automatically logging out.

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System** and click **Timeout.**

3. Enter the amount of idle timeout in minutes before automatically logging out. You can also enter 0 to set no limit on idle time out.



Timeout Settings

Web Idle Timeout: 5 — 0 ~ 10000 minutes (0 : no limit)

Click **Apply** to save the web idle timeout settings.

View statistics data

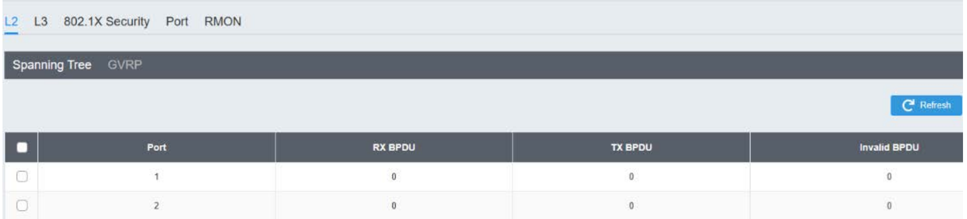
System > Statistics

This section will allow you to view packet statistics for L2 Spanning Tree & GVRP/L3 DHCP Snooping/802.1X/Port/RMON.

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System** and click **Statistics.**

3. Click on the sections to view packet statistics information based on the type of information to view. You can click **Refresh** to force refresh of the displayed content or clear to delete all statistics.



□	Port	RX BPDU	TX BPDU	Invalid BPDU
□	1	0	0	0
□	2	0	0	0

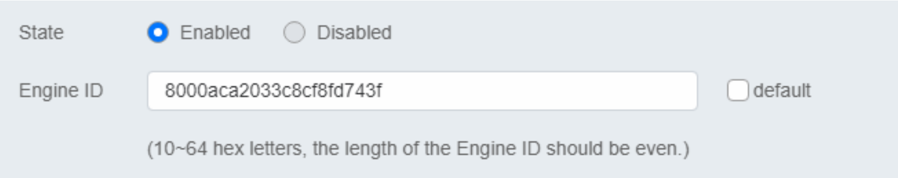
SNMP

Global Settings

System > SNMP > Global Setting

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System**, click on **SNMP,** and click on **Global Settings**.



State	● Enabled ○ Disabled	
Engine ID	8000aca2033c8cf8fd743f	□ default
	(10~64 hex letters, the length of the Engine ID should be even.)	

3. Select **Enabled** to enable SNMP or **Disabled** to disable it.

4. Input the SNMP OID engine

User List

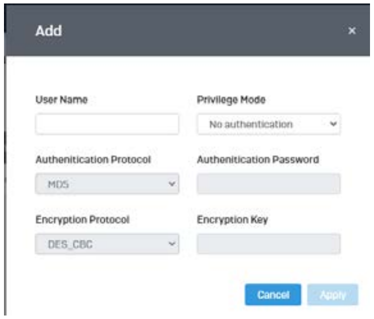
System > SNMP > User List

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System**, click on **SNMP,** and click on **User List**.

3. Click **Add** to add username to the user list.

4. Review the settings and click **Apply.**



Add

User Name	Privilege Mode
	No authentication
Authenitication Protocol	Authenitication Password
MD5	
Encryption Protocol	Encryption Key
DES_CBC	

- **User Name:** Enter the User Name to grant access to
- **Privilege Mode:** Select the level of privilege given
- **Authentication Protocol:** Select the type of protocol used for authentication
- **Authentication Password:** Input the password for the SNMP user
- **Encryption Protocol:** Select the encryption protocol type
- **Encryption Key:** Input the encryption key

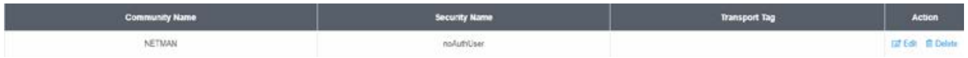
Community List

System > SNMP > Community List

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System**, click on **SNMP,** and click on **Community List**.

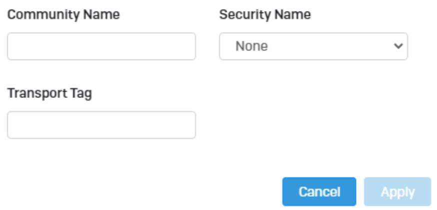
3. Select **Edit** to edit the selected community name or **Delete** to delete it.



Community Name	Security Name	Transport Tag	Action
NETMAN	noAuthUser		Edit Delete

4. To add a new entry, click the **Add** button

5. Review the settings and click **Apply**,



Community Name

Security Name: None

Transport Tag

- **Community Name:** Input the community name for the new entry
- **Security Name:** Select the security type
- **Transport Tag:** Input the transport tag in the field

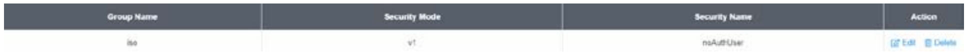
Group List

System > SNMP > Group List

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System**, click on **SNMP,** and click on **Group List**.

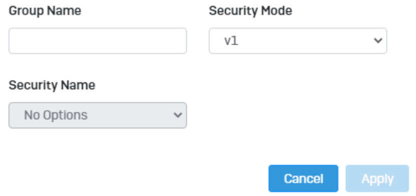
3. Select **Edit** to edit the selected group name or **Delete** to delete it.



Group Name	Security Mode	Security Name	Action
iso	v1	noAuthUser	Edit Delete

4. Click **Add** to add username to the user list.

5. Review the settings and click **Apply**,



Group Name

Security Mode: v1

Security Name: No Options

- **Group Name:** Input the desired group name
- **Security Mode:** Select the security mode for this SNMP group
- **Security Name:** Select the Security name from the drop down menu

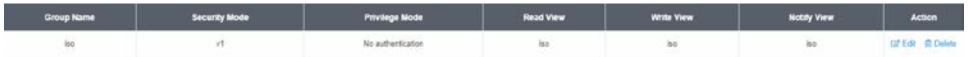
Access List

System > SNMP > Access List

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System**, click on **SNMP,** and click on **Access List**.

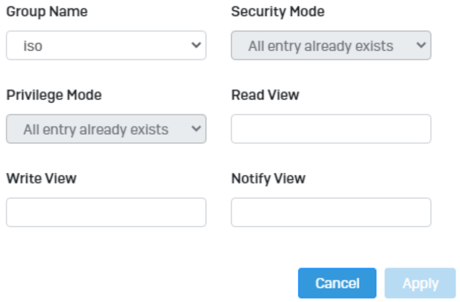
3. Select **Edit** to edit the selected group name or **Delete** to delete it.



Group Name	Security Mode	Privilege Mode	Read View	Write View	Notify View	Action
iso	v1	No authentication	iso	iso	iso	Edit Delete

4. Click **Add** to add username to the user list.

5. Review the settings and click **Apply**,



Group Name: iso

Security Mode: All entry already exists

Privilege Mode: All entry already exists

Read View

Write View

Notify View

- **Group Name:** Select from the list of group names in the drop down menu
- **Security Mode:** Select from the drop down menu the level of security
- **Read View:** Input the items that are readable for this group
- **Write View:** Input the items that can be modified by this group

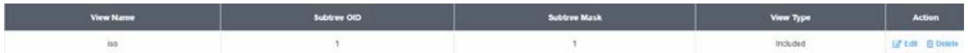
View List

System > SNMP > View List

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System**, click on **SNMP,** and click on **View List**.

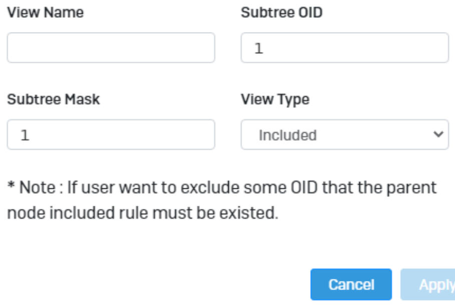
3. Select **Edit** to edit the selected group name or **Delete** to delete it.



View Name	Subtree OID	Subtree Mask	View Type	Action
iso	1	1	Included	Edit Delete

4. Click **Add** to add username to the user list.

5. Review the settings and click **Apply**,



View Name:

Subtree OID: 1

Subtree Mask: 1

View Type: Included

* Note : If user want to exclude some OID that the parent node included rule must be existed.

- **View Name:** Input the view name
- **Subtree OID:** Input the OID to be used
- **Subtree Mask:** Input the Subtree Mask
- **View Type:** Select **Included** or **Excluded** from the drop down menu

RMON

Statistics

System > RMON > Stat List

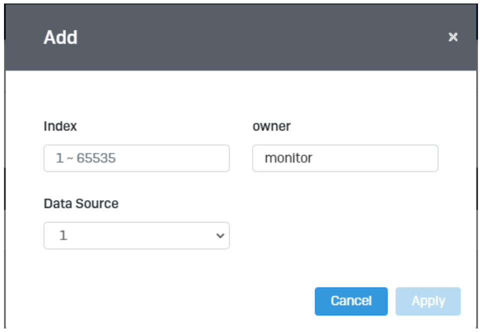
You can remotely view individual port statistics with RMON by using your SNMP NMS software and the RMON portion of the MIB tree.

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System**, click on **RMON,** and click on **Stat List**.

3. Click **Add** to add the entry to the table

4. Review the settings and click **Apply**.



Add

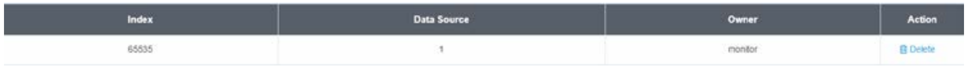
Index: 1 ~ 65535

owner: monitor

Data Source: 1

- **Index:** This parameter specifies the ID number of the new group. The range is 1 to 65535.
- **Data Source:** This parameter specifies the port where you want to monitor the statistical information of the Ethernet traffic.
- **Owner:** This parameter is used to identify the person who created an entry. It is primarily intended for switches that are managed by more than one person, and is an optional field.

In the list, you can click **Delete** to delete the entry.



Index	Data Source	Owner	Action
65535	1	monitor	Delete

- **Statistic** group— This group is used to view port statistics remotely with SNMP programs.
- **History** group— This group is used to collect histories of port statistics to identify traffic trends or patterns.
- **Event** group— This group is used with alarms to define the actions of the switch when packet statistic thresholds are crossed.
- **Alarm** group—This group is used to create alarms that trigger event log messages or SNMP traps when statistics thresholds are exceeded.

Event List

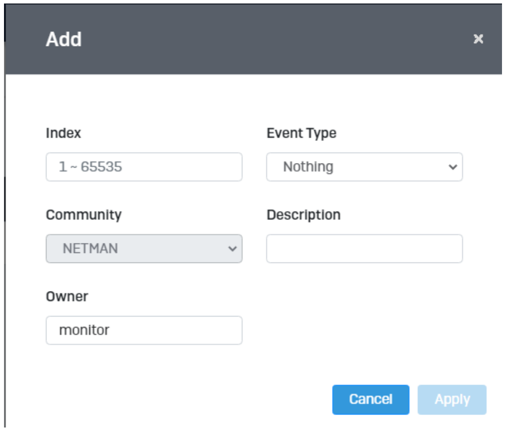
System > RMON > Event List

The RMON (Remote Monitoring) MIB is used with SNMP applications to monitor the operations of network devices. This Event group is used with alarms to define the actions of the switch when packet statistic thresholds are crossed.

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System,** click on **RMON** and click on **Event List**.

3. Click the **Add** button on the top right to enable RMON. Review and edit your settings. Click **Apply** to save settings.



Add

Index: 1 ~ 65535

Event Type: Nothing

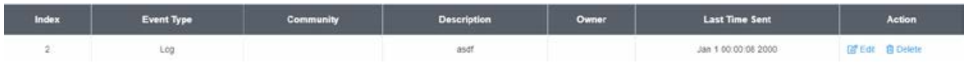
Community: NETMAN

Description:

Owner: monitor

- **Index:** This parameter specifies the ID number of the new group. The range is 1 to 65535.
- **Event:** Select the type of event that will trigger the alarm
- **Description:** Provide a name for this rule
- **Owner:** This parameter is used to identify the person who created an entry. It is primarily intended for switches that are managed by more than one person, and is an optional field

4. In the list, you can click **Edit** to modify an entry or click **Delete** or delete the entry**.**



Index	Event Type	Community	Description	Owner	Last Time Sent	Action
2	Log		asdf		Jan 1 00:00:08 2000	Edit Delete

Event Log Table

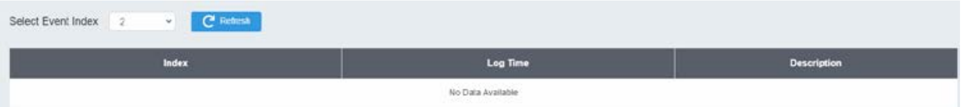
System > RMON > Event Log Table

Any RMON events that were triggered will be displayed here.

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System**, click on **RMON,** and click on **Event Log Table**.

3. Select the Event Index from the drop-down menu. Click the **Refresh** button if the page needs to be refreshed.



Select Event Index: 2

Index	Log Time	Description
	No Data Available	

Alarm List

System > RMON > Alarm List

RMON alarms are used to generate alert messages when packet activity on designated ports rises above or falls below specified threshold values. The alert messages can take the form of messages that are entered in the event log on the switch or traps that are sent to your SNMP NMS software or both.

RMON alarms consist of two thresholds. There is a rising threshold and a falling threshold. The alarm is triggered if the value of the monitored RMON statistic of the designated port exceeds the rising threshold. The response of the switch is to enter a message in the event log, send an SNMP trap, or both. The alarm is reset if the value of the monitored statistic drops below the falling threshold.

The frequency with which the switch samples the thresholds of an alarm against the actual RMON statistic is controlled by a time interval parameter. You can adjust this interval for each alarm.

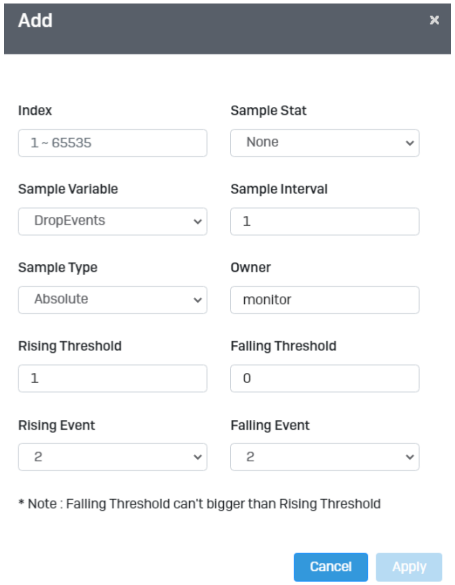
1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System**, click on **RMON,** and click on **Alarm List**.

3. Review the settings.

- **Index:** This parameter specifies the ID number of the new group. The range is 1 to 65535.
- **Sample Interval:** This parameter specifies the time (in seconds) over which the data is sampled. Its range is 1 to 2147483647 seconds.
- **Sample Variable:** This parameter specifies the RMON MIB object that the event is monitoring.
- **Sample type:** This parameter defines the type of change that has to occur to trigger the alarm on the monitored statistic. There are two choices from the pull-down menu - Delta value and Absolute value. Delta value- setting compares a threshold against the difference between the current and previous values of the statistic. Absolute value- setting compares a threshold against the current value of the statistic.
- **Owner:** This parameter is used to identify the person who created an entry. It is primarily intended for switches that are managed by more than one person, and is an optional field
- **Rising Threshold:** This parameter specifies a specific value or threshold level of the monitored statistic. When the value of the monitored statistic becomes greater than this threshold level, an alarm event is triggered. The parameter's range is 1 to 2147483647.
- **Falling Threshold:** This parameter specifies a specific value or threshold level of the monitored statistic. When the value of the monitored statistic becomes less than this threshold level, an alarm event is triggered. The parameter's range is 1 to 2147483647.
- **Rising Event:** This parameter specifies the event index for the rising threshold. Its range is 1 to 65535. This field is mandatory and must match an Event Index that you previously entered in "Events".
- **Falling Event:** This parameter specifies the event index for the falling threshold. Its range is 1 to 65535. This field is mandatory and must match an Event Index that you previously entered in "Events".

Click **Apply** to add the entry to the table.


Add

Index: 1 ~ 65535
Sample Stat: None
Sample Variable: DropEvents
Sample Interval: 1
Sample Type: Absolute
Owner: monitor
Rising Threshold: 1
Falling Threshold: 0
Rising Event: 2
Falling Event: 2

* Note : Falling Threshold can't bigger than Rising Threshold

History

System > RMON > History List

RMON histories are snapshots of port statistics. They are taken by the switch at predefined intervals and can be used to identify trends or patterns in the numbers or types of ingress packets on the ports on the switch. The snapshots can be viewed with your SNMP NMS software with the history group of the RMON portion of the MIB tree.

A history group is divided into buckets. Each bucket stores one snapshot of statistics of a port. A group can have from 1 to 50 buckets. The more buckets in a group, the more snapshots it can store.

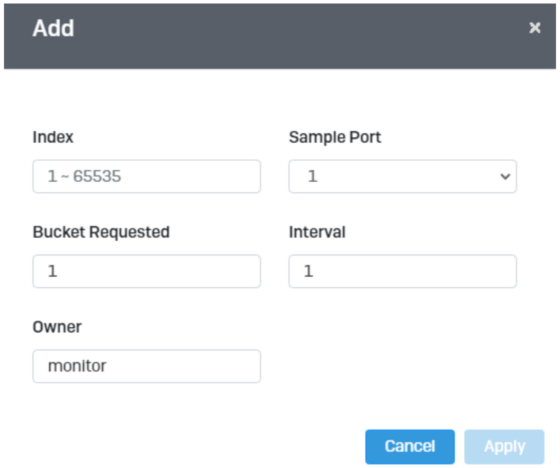
1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System**, click on **RMON,** and click on **History**.

3. Review the settings.

- **Index:** This parameter specifies the ID number of the new group. The range is 1 to 65535.
- **Sample Port:** This parameter specifies the port where you want to monitor the statistical information of the Ethernet traffic.
- **Buckets Requested:** This parameter defines the number of snapshots of the statistics for the port. Each bucket can store one snapshot of RMON statistics. Different ports can have different numbers of buckets. The range is 1 to 50 buckets.
- **Interval:** This parameter specifies how frequently the switch takes snapshots of the port's statistics. The range is 1 to 3600 seconds (1 hour). For example, if you want the switch to take one snapshot every minute on a port, you specify an interval of sixty seconds.
- **Owner:** This parameter is used to identify the person who created an entry. It is primarily intended for switches that are managed by more than one person, and is an optional field.

Click **Add** to add the entry to the table.


Add

Index: 1 ~ 65535
Sample Port: 1
Bucket Requested: 1
Interval: 1
Owner: monitor

History Log Table

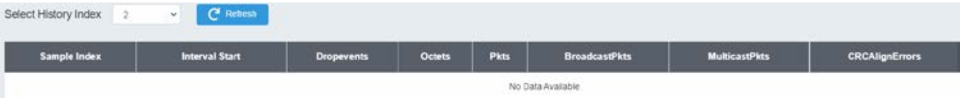
System > RMON > History Log Table

RMON History Logs are accessed from this section. RMON History logs can be filtered by RMON Index.

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System**, click on **RMON,** and click on **History Log Table.**

3. Select the History Index from the drop-down menu. Click the **Refresh** button if the page needs to be refreshed.



Select History Index: 2

Sample Index	Interval Start	Dropevents	Octets	Pkts	BroadcastPkts	MulticastPkts	CRCAlignErrors
No Data Available							

MAC Address Table

Static MAC Address

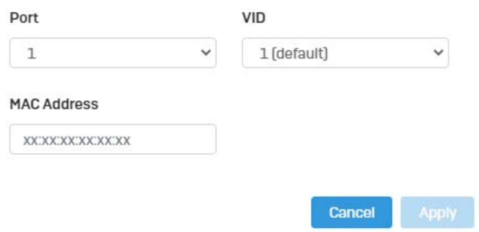
System > MAC Address Table > Static MAC Address

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System**, click on **MAC Address Table,** and click on **Static MAC Address.**

3. Click **Add** to configure a new static MAC address

4. Review the settings and click **Apply.**



Port: 1

VID: 1 (default)

MAC Address: xx:xx:xx:xx:xx:xx

- **Port:** Select the port where the MAC address will reside.
- **VID:** Select the VLAN ID where the MAC address will reside
  Note *By default, all switch ports are part of the default VLAN, VLAN ID 1*
- **MAC Address:** Enter the MAC address of he device to add

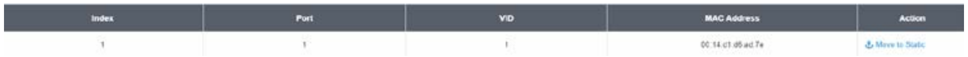
Dynamic MAC Address

System > MAC Address Table > Dynamic MAC Address

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System**, click on **MAC Address Table,** and click on **Dynamic MAC Address.**

3. The table currently displays the MAC address of devices connected to the switch. To move a MAC address to Static MAC Address, click **Move to Static**



Index	Port	VID	MAC Address	Action
1	1	1	00:14:c1:d6:ad:7e	Move to Static

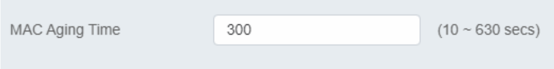
MAC Aging Time

System > MAC Address Table > MAC Aging Time

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System**, click on **MAC Address Table,** and click on **MAC Aging Time.**

3. Enter the duration in seconds for MAC Aging Table



MAC Aging Time: 300 (10 ~ 630 secs)

SFP Module Information

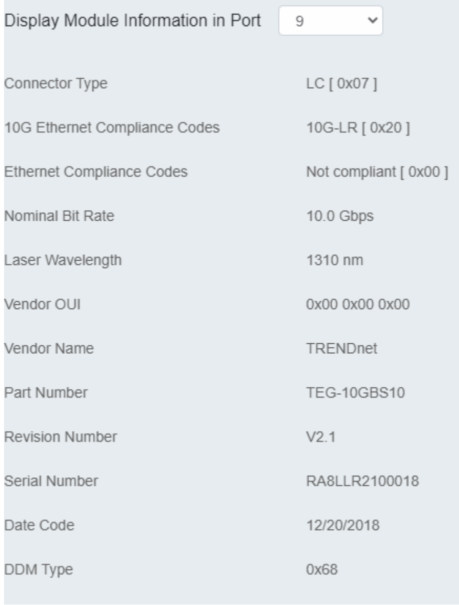
Module & **DDM**

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **System**, click on **SFP Module Information ,** and select either **Module** or **DDM.**

3. **Module** and **DDM** displays additional information of the SFP module that's connected in the SFP slots.

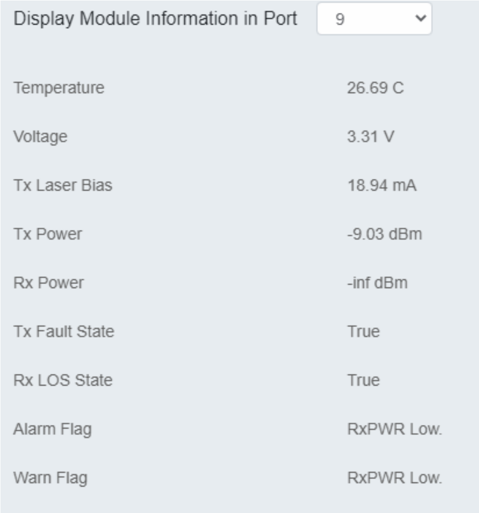
Module:



Display Module Information in Port: 9

Connector Type	LC [0x07]
10G Ethernet Compliance Codes	10G-LR [0x20]
Ethernet Compliance Codes	Not compliant [0x00]
Nominal Bit Rate	10.0 Gbps
Laser Wavelength	1310 nm
Vendor OUI	0x00 0x00 0x00
Vendor Name	TRENDnet
Part Number	TEG-10GBS10
Revision Number	V2.1
Serial Number	RA8LLR2100018
Date Code	12/20/2018
DDM Type	0x68

DDM:



Display Module Information in Port: 9

Temperature	26.69 C
Voltage	3.31 V
Tx Laser Bias	18.94 mA
Tx Power	-9.03 dBm
Rx Power	-inf dBm
Tx Fault State	True
Rx LOS State	True
Alarm Flag	RxPWR Low.
Warn Flag	RxPWR Low.

Network

Physical Interface

Configure Physical Interfaces

Network > Physical Interface

This section allows you to configure the physical port parameters such as speed, duplex, flow control, and jumbo frames. This section also reports the current link status of each port and negotiated speed/duplex. Additionally you will be able to set your BPDU ports for Spanning Tree Configuration and EAP ports for 802.1x port-based authentication configuration.

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network**, click on **Physical Interface,** and click on **Port**.

3. Review the settings. Click **Apply** to save changes.

- **Port -** Specifies the port number. The All value indicates ports 1 through 10 on the Switch. You cannot change this parameter. You can use the **All** column value in the **Port** column to apply**, Mode, Flow Control,** and **Description** settings to all ports at the same time.

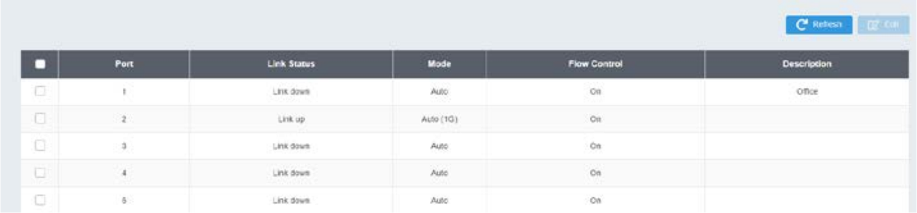
- **Link Status -** This parameter indicates the status of the link between the port and the end node connected to the port. The possible values are:
  - **Link up** -This parameter indicates a valid link exists between the port and the end node.
  - **Link down** -This parameter indicates the port and the end node have not established a valid link.

- **Mode:** This parameter indicates the speed and duplex mode settings for the port. You can use this parameter to set the speed and duplex mode of a port. The possible settings are:
  - **Auto** -This parameter indicates the port is using Auto-Negotiation to set the operating speed and duplex mode. The actual operating speed and duplex mode of the port are displayed in parentheses (for example, "10G" for 10Gbps full duplex mode) after a port establishes a link with an end node.
  - **Auto (10G)** -This parameter indicates the port is configured for 10Gbps operation in Auto-Negotiation mode.
  - **Auto (1G)** -This parameter indicates the port is configured for 1Gbps/1000Mbps operation in Auto-Negotiation mode.
  - **10G/Full** – This parameter indicates the port is configured for 10Gbps operation in full-duplex mode
  - **1G/Full** -This parameter indicates the port is configured for 1000Mbps operation in full-duplex mode.

Note: *When selecting a* ***Mode*** *setting, the following points apply:*

- *When a twisted-pair port is set to Auto-Negotiation, the end node should also be set to Auto-Negotiation to prevent a duplex mode mismatch.*
- *A switch port using Auto-Negotiation defaults to half-duplex if it detects that the end node is not using Auto-Negotiation. This can result in a mismatch if the end node is operating at a fixed duplex mode of full-duplex. To avoid this problem when connecting an end node with a fixed duplex mode of full-duplex to a switch port, disable Auto-Negotiation on the port and set the port's speed and duplex mode manually.*
- *The only valid setting for the SFP ports is Auto-Negotiation.*

- **Flow Control:** This parameter reflects the current flow control setting on the port. The switch uses a special pause packet to notify the end node to stop transmitting for a specified period of time. The possible values are:
  - **Enabled** - This parameter indicates that the port is permitted to use flow control.
  - **Disabled** - This parameter indicates that the port is not permitted to use flow control.
- **Description**: This parameter offers the ability to name the device that's connected to it



■	Port	Link Status	Mode	Flow Control	Description
□	1	Link down	Auto	On	Office
□	2	Link up	Auto (1G)	On	
□	3	Link down	Auto	On	
□	4	Link down	Auto	On	
□	5	Link down	Auto	On	

Port Isolation

Network > Physical Interface > Port Isolation

Port isolation prevents traffic from being sent between specific ports.

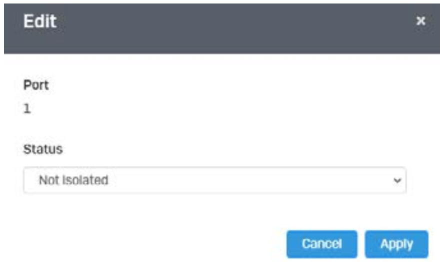
1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network**, click on **Physical Interface,** and click on **Port Isolation**.

3. Select the port you would like to be edit. You may also select all ports by selecting **All** column.

4. Select from the drop down menu to either **Isolate** or **Not Isolate** for the specified port and click **Apply** to save your settings.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*



Port
1

Status
Not Isolated

Mirroring

Network > Physical Interface > Mirror

Port mirroring allows you to monitor the ingress and egress traffic on a port by having the traffic copied to another port where a computer or device can be set up to capture the data for monitoring and troubleshooting purposes.

1. Log into your switch management page (see "Access your switch management page" on page 9).

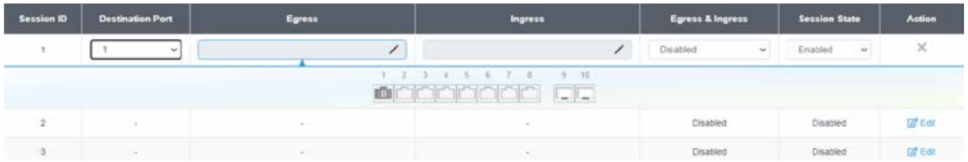
2. Click on **Network**, then click on **Physical Interface**, and click on **Mirror**.

3. Review the settings. Click **Apply** to save changes.
   - **Edit** – Click to edit the selected session ID.
   - **Session State** – Click the drop-down and list and select one of the following options:
     - **Enable** - This parameter activates the Port Mirroring feature and the rest of the configuration parameters become active on the page.
     - **Disable** - This parameter de-activates the Port Mirroring feature and the rest of the configuration parameters become inactive on the page.
   - **Destination Port** – Click the drop-down and list and select the port to send the copied ingress/egress packets/data. (*e.g. Computer or device with packet capture or data analysis program.)*

Check the port to monitor or copy inormation from. (Source)

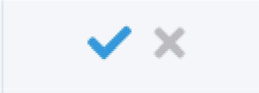
To copy data received on a specific port, select the port number(s) under the **Ingress Port** section or you could click **All** to copy data received on all ports.

To copy data transmitted on specific port, select the port number under the **Egress Port** section or you could click **All** to copy data transmitted on all ports.

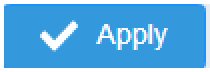


Session ID	Destination Port	Egress	Ingress	Egress & Ingress	Session State	Action
1	1			Disabled	Enabled	✕
2	-	-	-	Disabled	Disabled	Edit
3	-	-	-	Disabled	Disabled	Edit

4. At the right hand panel, click the check mark to save your settings.



5. At the top right of the screen, click **Apply**.



Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

Jumbo Frames

Network > Physical Interface > Jumbo Frames

The jumbo frame setting is applied globally on all ports and cannot be configured independently on each individual port. By default the jumbo frame setting is configured 1522 bytes.

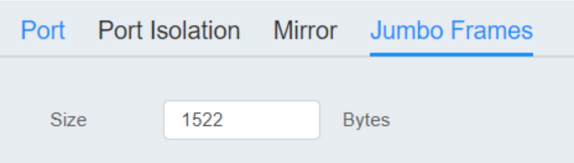
This section lets you input the size of the Jumbo Frames that can be accepted by the switch.

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network**, then click on **Physical Interface**, and click on **Jumbo Frames**.

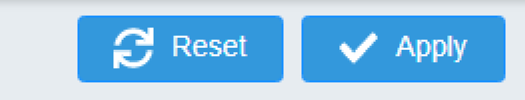
3. Enter the size of the Jumbo Frames to be accepted by the switch (in Bytes).

Note: *The value of the Jumbo Frames needs to be between 1522 and 10240 Bytes. By default the value is **1522** Bytes.*



Size 1522 Bytes

4. Click **Reset** to reset the size of the Jumbo Frames to its default value. To save your new Jumbo Frame size, click **Apply**.



Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

VLAN Settings

802.1Q VLAN

Network > VLAN Settings > 802.1Q

A VLAN is a group of ports that can be anywhere in the network, but communicate as though they were in the same area.

VLANs can be easily organized to reflect department groups (such as R&D, Marketing), usage groups (such as e-mail), or multicast groups (multimedia applications such as video conferencing), and therefore help to simplify network management by allowing users to move devices to a new VLAN without having to change any physical connections.

1. Log into your switch management page (see "Access your switch management page" on page 9).

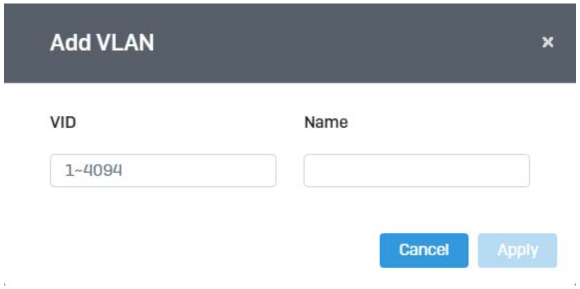
2. Click on **Network**, click on **VLAN Settings,** and click on **802.1Q**.

3. Click on **Add** to create a new VLAN.

3. Review the settings.

- **VID –** Enter the VLAN ID for the new VLAN.
- **Name** – Enter the VLAN name.

  Note: *By default, the default VLAN VID 1 is set as the Management VLAN.*
- **Cancel –** Deletes the current settings
- **Apply** – Apply the new settings



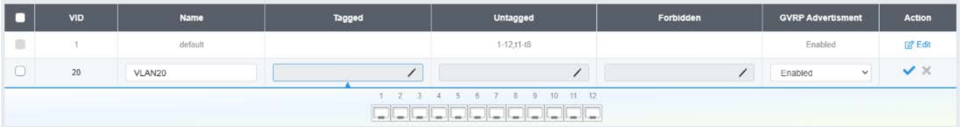
In the sections **Static Tagged, Static Untagged,** and **Not Member**, you can add the type of VLAN ports to add to the new VLAN (Tagged or Untagged) and assign ports that are not members (Forbidden) of the new VLAN.

Tagged/Untagged/Not Member VLAN Ports

On a port, the tag information within a frame is examined when it is received to determine if the frame is qualified as a member of a specific tagged VLAN. If it is, it is eligible to be switched to other member ports of the same VLAN. If it is determined that the frame's tag does not conform to the tagged VLAN, the frame is discarded.

Since these VLAN ports are VLAN aware and able to read VLAN VID tagged information on a frame and forward to the appropriate VLAN, typically tagged VLAN ports are used for uplink and downlink to other switches to carry and forward traffic for multiple VLANs across multiple switches. Tagged VLAN ports can be included as members for multiple VLANs. Computers and other edge devices are not typically connected to tagged VLAN ports unless the network interface on these device can be enabled to be VLAN aware.

Select the tagged VLAN ports to add to the new VLAN.



□	VID	Name	Tagged	Untagged	Forbidden	GVRP Advertisment	Action
□	1	default		1-12,t1-t8		Enabled	Edit
□	20	VLAN20				Enabled	✓ ✕

Untagged VLAN ports are used to connect edge devices (VLAN unaware) such as computers, laptops, and printers to a specified VLAN. It is required to modify the Port VID settings accordingly for untagged VLAN ports under Bridge > VLAN > Port Settings. (e.g. If the VID for the VLAN is 2, the PVID should also be set to 2)

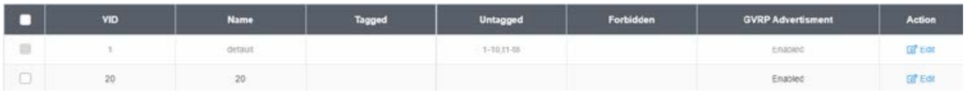
Select the untagged VLAN ports to add to the new VLAN.

Select the Forbidden ports to restrict from the new VLAN.

Click **Apply** to save the new VLAN to the table.

In the list, you can click **Edit** to modify an entry

Note: *The default VLAN VID1 cannot be removed.*



☐	VID	Name	Tagged	Untagged	Forbidden	GVRP Advertisment	Action
☐	1	default		1-10,11-18		Enabled	Edit
☐	20	20				Enabled	Edit

4. At the top of the right hand panel, click **Apply**.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied*

PVID & Ingress Filter

Network > VLAN Settings > PVID & Ingress Filter

In this section, you can modify the port VID settings, acceptable frame types, and ingress filtering. Please note that when setting VLAN port members as untagged under the 802.1Q VLAN section, the port VID (PVID) setting is automatically modified in the PVID configuration setting to match that VLAN.

1. Log into your switch management page (see "Access your switch management page" on page 9).

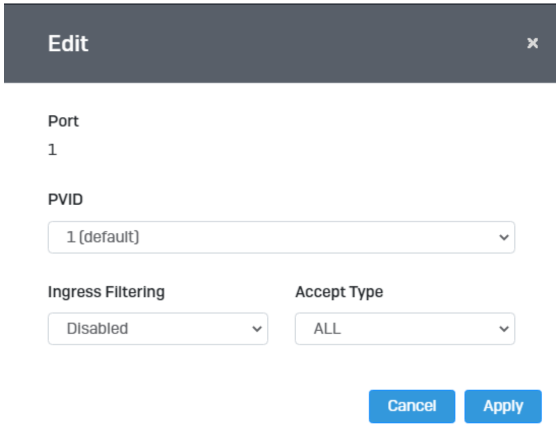
2. Click on **Network**, click on **VLAN Settings,** and click on **PVID & Ingress Filter**.

3. Select the port would like to modify and click **Edit** to modify an entry.

4. Review the settings for each port. Click **Apply** to save settings.

- **Port** – Displays the selected port
- **PVID –** Select the correct VLAN ID. ***Note:*** *Required for untagged VLAN ports.*
- **Ingress Filtering** –Click the drop-down list and select **Enabled** to enable ingress filtering or **Disabled** to disable ingress filtering.
- **Acceptable Frame Type** – Click the drop-down list and select which type of frames can be accepted.
  - **All** – The port can accept all frame types.
  - **Tagged** – The port can accept tagged frames only. Untagged frames are discarded.
  - **Untagged**– The port can accept untagged frames and frames with tagged priority information only such as 802.1p.

  Note: *Modifying settings in the row marked* ***All****, will apply the settings to all ports.*



Port: 1

PVID: 1 (default)

Ingress Filtering: Disabled

Accept Type: ALL

4. At the bottom, click **Apply** to save the changes made.

GVRP

Protocol

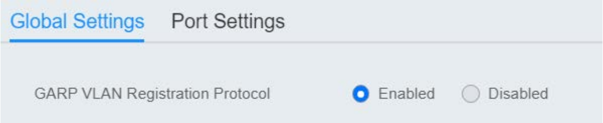
Network > GVRP > Global Settings

The GVRP VLAN Registration Protocol (GVRP) allows network devices to share VLAN information and to use the information to modify existing VLANs or create new VLANs, automatically. This makes it easier to manage VLANs that span more than one switch. Without GVRP, you have to manually configure your switches to ensure that the various parts of the VLANs can communicate with each other across the different switches. With GVRP, which is an application of the Generic Attribute Registration Protocol (GARP), this is done for you automatically.

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network**, click on **GVRP,** and click on **Global Settings**.

3. Select **Enabled** under GARP VLAN Registration Protocol to to activate GVRP or **disabled** to deactivate GVRP. Click **Apply** to save the settings.



GARP VLAN Registration Protocol ● Enabled ○ Disabled

4. At the top of the right hand panel, click **Apply**.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

Port Settings

Network > GVRP > Port Settings

This section will allow you to select which ports will have GVRP enabled or will be restricted from using GVRP.

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network**, click on **GVRP** and click on **Port Settings**.

3. Select the port to modify the settings.

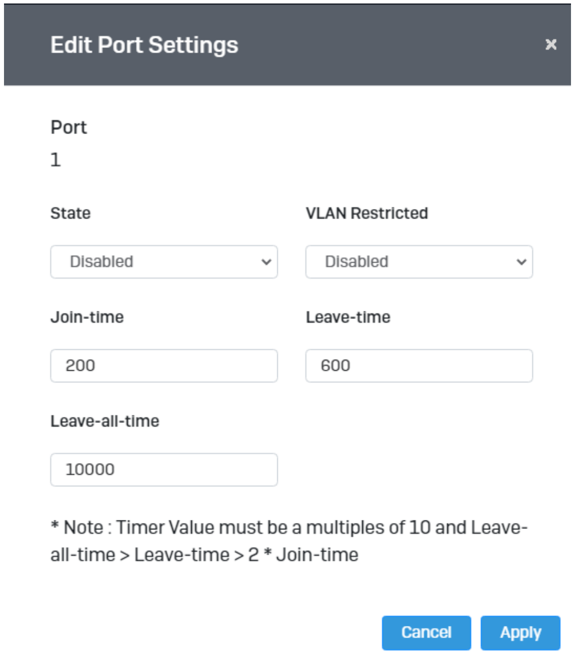
3. Review the settings for each port. Click **Apply** to save the settings.

- **Port** - This parameter displays the ports on the switch.
- **JoinTime** - This parameter is the GARP Join Timer. Its range is 10 - 4999000 milli-seconds.
- **LeaveTime** - This parameter is the GARP Leave Timer. Its range is 10 - 9999000 milli-seconds. This timer must be set in relation to the GVRP Join Timer according to the following equation:

  GARPLeaveTimer >= (GARPJoinTimer X 2) + 10

- **LeaveAllTime** - This parameter is the GARP Leave All Timer. Its range is 10 - 10000000 milli-seconds. This timer must be set in relation to the GVRP Leave Timer according to the following equation:

  GARPLeaveAllTimer > (GARPLeaveTimer + 10)


Edit Port Settings

Port
1

State: Disabled

VLAN Restricted: Disabled

Join-time: 200

Leave-time: 600

Leave-all-time: 10000

* Note : Timer Value must be a multiples of 10 and Leave-all-time > Leave-time > 2 * Join-time

4. At the bottom of the right hand panel, click **Apply**.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied*

Spanning Tree

Protocol

Network > Spanning Tree > Global Settings > STP

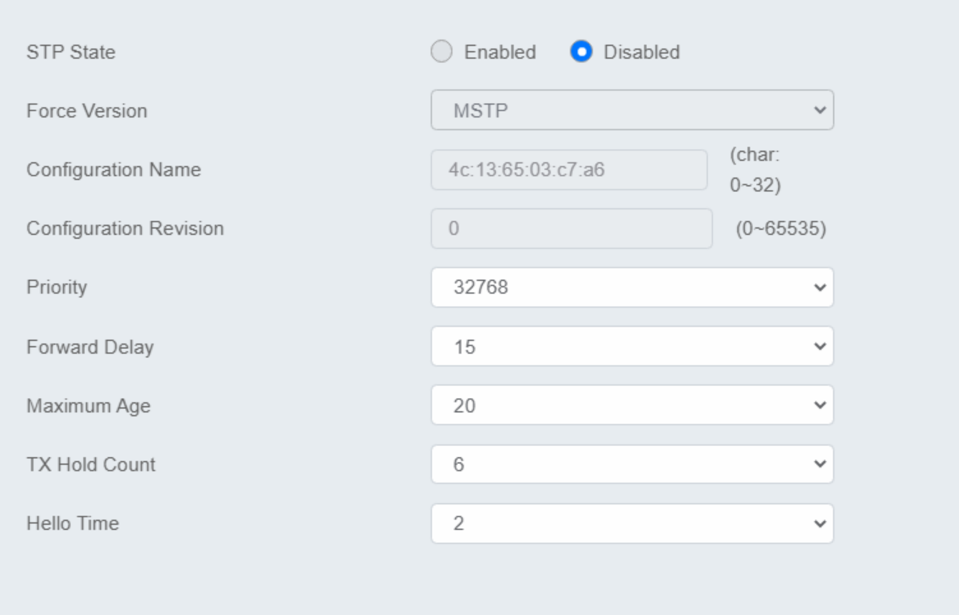
Spanning Tree Protocol (STP) provides network topology for any arrangement of bridges/switches. STP also provides a single path between end stations on a network, eliminating loops. Loops occur when alternate routes exist between hosts. Loops in an extended network can cause bridges to forward traffic indefinitely, resulting in increased traffic and reducing network efficiency.

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network**, click on **Spanning Tree,** click on **Global Settings,** and click on **STP**.

3. Review the settings. Click **Apply** to save changes.

- **STP State:** Select **Enabled** to Enable Spanning Tree Protocol, or **Disabled** to disable STP.
- **Force Version:** Select **MSTP** or **RSTP** from the drop-down menu
- **Configuration Name:** Name the current STP
- **Configuration Revision:** Assign a revision number
- **Priority:** The **Priority** has a range 0 to 61440 in increments of 4096. To make this easier for you, the Web Management Utility divides the range into increments. You specify the increment that represents the desired bridge priority value.
- **Forward Delay:** The Forward Delay defines the time that the bridge spends in the listening and learning states. Its range is 4 - 30 seconds.
- **Maximum Age:** The Maximum Age defines the amount of time a port will wait for STP/RSTP information. MSTP uses this parameter when interacting with STP/RSTP domains on the boundary ports. Its range is 6 - 40 seconds
- **TX Hold Count:** The Transmit Hold Count specifies the maximum number of BPDUs that the bridge can send per second. Its range is 1 - 10.
- **Hello Time:** The Hello Time is frequency with which the root bridge sends out a BPDU.



STP State	○ Enabled ● Disabled
Force Version	MSTP
Configuration Name	4c:13:65:03:c7:a6 (char: 0~32)
Configuration Revision	0 (0~65535)
Priority	32768
Forward Delay	15
Maximum Age	20
TX Hold Count	6
Hello Time	2

4. At the top right panel, click **Apply**.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied*

Root Bridge Information

Network > Spanning Tree > Global Settings > Root Bridge Information

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network**, click on **Spanning Tree,** click on **Global Settings,** and click on **Root Bridge Information**.

3. Displays the current settings made under STP.

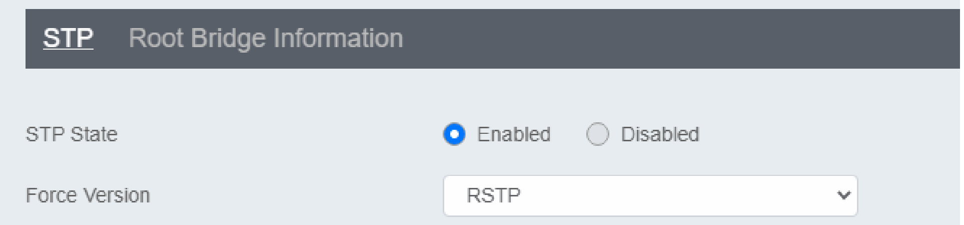
RSTP Port Settings

Network > Spanning Tree > RSTP Port Settings

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network**, click on **Spanning Tree,** click on **Global Settings,** and click on **STP**.

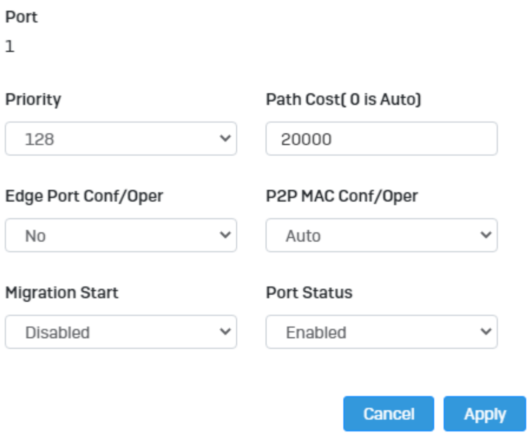
3. Select **RSTP** from the drop down menu on **Force Version**



STP State	● Enabled ○ Disabled
Force Version	RSTP

4. Click on **RSTP Port Settings** and select the port(s) to configure and click **Edit**.

5. Review the settings and click **Apply** to save your changes.



Port

1

Priority: 128

Path Cost(0 is Auto): 20000

Edge Port Conf/Oper: No

P2P MAC Conf/Oper: Auto

Migration Start: Disabled

Port Status: Enabled

- **Priority:** Indicates the port priority. If two paths have the same port cost, the bridges must select a preferred path. In some instances this can involve the use of the port priority parameter which is used as a tie breaker when two paths have the same cost. The range for port priority is 0 to 240. As with bridge priority, this range is broken into increments, in this case multiples of 16. To select a port priority for a port, you enter the desired value. Table 1 lists the values that are valid.
- **Path Cost:** This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets. The default port cost: 100Mbps port = 200000. Gigabit port = 20000.
- **Edge Port Conf/Oper:** Indicates if a port is connected to an edge device in the network topology or not. Select **Yes** designates the port is an edge port, and **No** to designate the port is not an edge port.
- **P2P MAC Conf/Oper:** P2P ports are similar to edge ports, however, they are restricted in that a P2P port must operate in full-duplex. **Auto** allows the port to have P2P status whenever possible and operate as if the P2P status were true. Selecting **Yes** indicates a P2P shared link is available. Selecting **No** means the port cannot maintain a P2P link.
- **Migration: Enabled** indicates the port is configured to accept RSTP and **Disabled** indicates the port is not configured to accept RSTP.
- **Status:** Select **Enabled** to enable the status to be shown or **Disabled** to disable this feature.

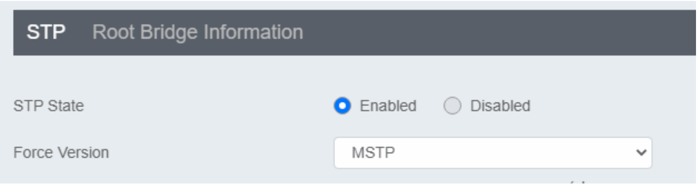
CIST Port Settings

Network > Spanning Tree > CIST Port Settings

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network**, click on **Spanning Tree,** click on **Global Settings,** and click on **STP**.

3. Select **MSTP** from the drop down menu on **Force Version**

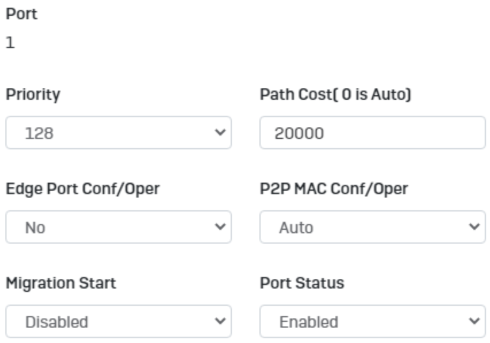


STP State: ● Enabled ○ Disabled

Force Version: MSTP

4. Click on **Cist Port Settings** and select the port(s) to configure and click **Edit**.

5. Review the settings and click **Apply** to save your changes.



Port

1

Priority: 128

Path Cost(0 is Auto): 20000

Edge Port Conf/Oper: No

P2P MAC Conf/Oper: Auto

Migration Start: Disabled

Port Status: Enabled

- **Priority:** Indicates the port priority. If two paths have the same port cost, the bridges must select a preferred path. In some instances this can involve the use of the port priority parameter which is used as a tie breaker when two paths have the same cost. The range for port priority is 0 to 240. As with bridge priority, this range is broken into increments, in this case multiples of 16. To select a port priority for a port, you enter the desired value. Table 1 lists the values that are valid.
- **Path Cost:** This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets. The default port cost: 100Mbps port = 200000. Gigabit port = 20000.
- **Edge Port Conf/Oper:** Indicates if a port is connected to an edge device in the network topology or not. Select **Yes** designates the port is an edge port, and **No** to designate the port is not an edge port.
- **P2P MAC Conf/Oper:** P2P ports are similar to edge ports, however, they are restricted in that a P2P port must operate in full-duplex. **Auto** allows the port to have P2P status whenever possible and operate as if the P2P status were true. Selecting **Yes** indicates a P2P shared link is available. Selecting **No** means the port cannot maintain a P2P link.
- **Migration: Enabled** indicates the port is configured to accept RSTP and **Disabled** indicates the port is not configured to accept RSTP.
- **Status:** Select **Enabled** to enable the status to be shown or **Disabled** to disable this feature.

MST

Network > Spanning Tree > MST Instance Settings

1. Log into your switch management page (see "Access your switch management page" on page 9).

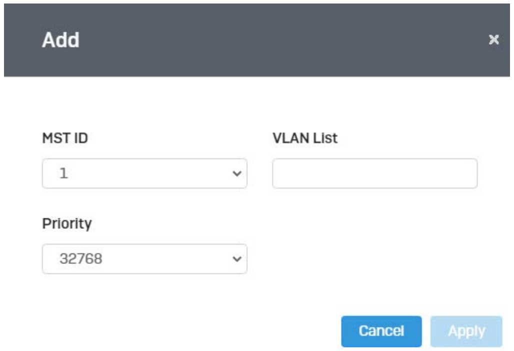
2. Click on **System**, click on **Spanning Tree**, and click on **MST Instance Settings**.

3. Click on **Add** to add a new entry.

4. Review the settings. For each section, click **Apply** to save changes.

MST Configuration Identification Settings

- **Configuration Name:** A configured name set on the switch to uniquely identify the MSTI (Multiple Spanning Tree Instance). If a configuration name is not set, this field shows the MAC address of the device running MSTP.
- ***Revision Level (0-65535): This value, together with the configuration name, and identical vlans mapped for STP instance IDs identifies the MST region configured on the switch.***



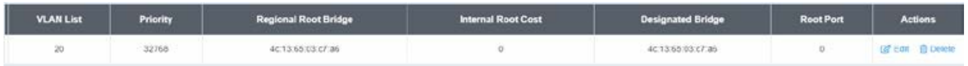
MST ID: 1

VLAN List:

Priority: 32768

MST Instance Settings

- **MSTI ID:** Displays the MST ID associated with the VID List. The possible field range is 1-4.
- **VLAN List:** Displays the VID List.
- **Priority:** Select the new priority in the Priority field from the drop down menu options. The user may set a priority value between **0-61440**.



VLAN List	Priority	Regional Root Bridge	Internal Root Cost	Designated Bridge	Root Port	Actions
20	32768	4c:13:65:03:c7:a6	0	4c:13:65:03:c7:a6	0	Edit Delete

- **MST Table:** Make changes to the table entry, and click **Edit** modify or click **Delete** to remove the ID entry.

MST Port Settings

Network > Spanning Tree > MST Port Settings

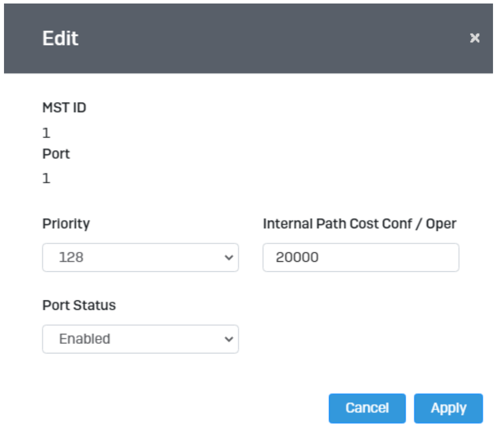
1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Network**, click on **Spanning Tree**, and click on **MST Port Settings**.

3. Review the settings. For each entry, click **Apply** to save changes.

- **Select MST Port** – Select the MST Port to configure and click the **Edit** button.

- **MST ID:** The MST ID that is associated with this port
- **MST Port Info -** The MST Port Information page provides user to configure the MSTP Interface settings.
    - **Priority** - This is the port priority used by MSTP in calculating path costs when two ports on the switch have the same port cost.
    - **Internal Path Cost (0 = Auto)** - This is the port cost used by MSTP when calculating path cost to the root bridge.
    - **Port Status**: Enable or disable the current settings configured for the selected port.



Edit

MST ID
1

Port
1

Priority: 128

Internal Path Cost Conf / Oper: 20000

Port Status: Enabled

4. Click the **Apply** button to save the settings to the **Flash.**

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

Trunk

The trunking function enables the cascading of two or more ports for a combined larger total bandwidth. Up to 8 trunk groups may be created, each supporting up to 8 ports. Add a trunking Name and select the ports to be trunked together, and click Apply to activate the selected trunking groups.

Important Note: *Do not connect the cables of a port trunk to the ports on the switch until you have configured the ports on both the switch and the end nodes. Connecting the cables prior to configuring the ports can create loops in your network topology. Loops can result in broadcast storms which can severely limited the effective bandwidth of your network.*

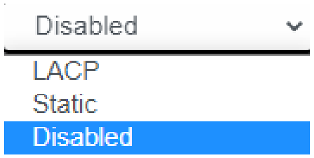
Settings

Network > Trunking

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network**, and click on **Trunking**.

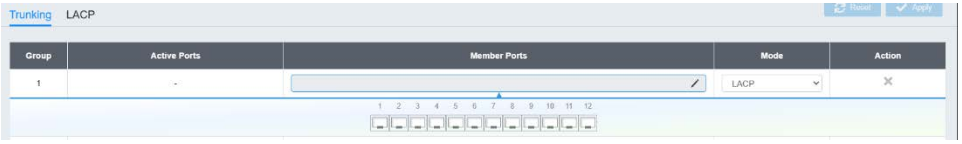
3. Review the settings. For each trunk group, click **Apply** to save changes.



Click the drop-down list and select one of the following options.

- **LACP** - The specific aggregator will broadcast and respond to LACPDU (LACP Data Unit) packets. This setting enables the dynamic LACP feature for the trunk.
- **Static** - Enables static port trunking and disables the LACP feature for the trunk. (Static link aggregation).
- **Disable** - Disables the static port trunk and disables the LACP feature for the trunk.

For each Trunk ID/Group, check the port numbers to add for each trunk group.



Group	Active Ports	Member Ports	Mode	Action
1	-		LACP	×

4. At the right hand of the group, click the check mark to apply the settings and the x button to discard the settings.

5. Select the **Apply** button on the top left of the screen to save your settings to the flash.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

LACP

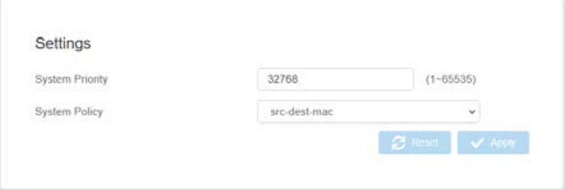
Network > Trunking > LACP

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network**, click on **Trunk**, and click on **LACP**.

3. Review the settings. Click **Apply** to save changes.

To assign a higher priority within a trunk group, input the priority value 1-65535 (65535 being the highest priority).



Settings

System Priority: 32768 (1~65535)

System Policy: src-dest-mac

4. Click **Apply** to save your settings to the flash.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

LACP Timeout

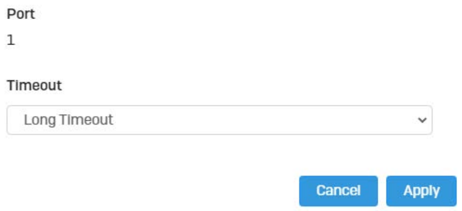
Network > Trunking > LACP

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network**, click on **Trunk**, and click on **LACP**.

3. Select the port to modify the settings and click **Edit**.

4. Select **Long Timeout** to configure the LACP timeout value to be 30 seconds, or **Short Timeout** to configure the LACP timeout value to be 1 second.



Port
1

Timeout
Long Timeout

4. Click **Apply** to save your settings to the flash.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

IGMP Snooping

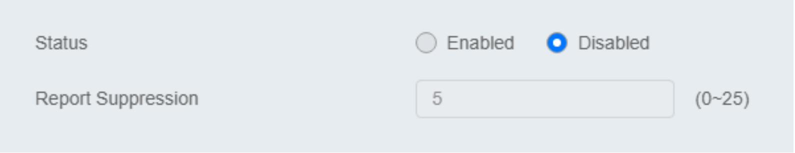
Global Settings

Network > IGMP Snooping > Global Settings

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network**, click on **IGMP Snooping**, and click on **Global Settings**.

3. Review the settings. Click **Apply** to save the settings.
   - **Status** – Select **Enabled** to enable the IGMP snooping feature or **Disabled** to disable the feature.
   - **Report Suppression** – Enter the time suppression interval between 0 – 25.



Status ○ Enabled ● Disabled

Report Suppression 5 (0~25)

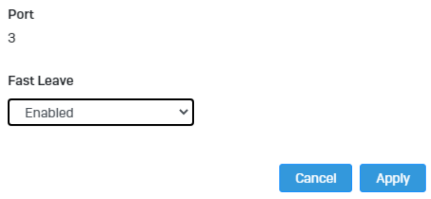
Fast Leave

Network > IGMP Snooping > Port Settings

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network**, click on **IGMP Snooping**, and click on **Port Settings**.

3. Review the settings. Click **Apply** to save the settings.
   - **Fast Leave –** Select **Enabled** to enable Fast Leave from the selected port or **Disabled** to disable the feature



Port
3

Fast Leave
Enabled

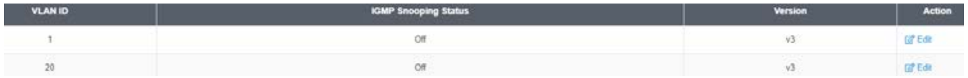
VLAN Settings

Network > IGMP Snooping > VLAN Settings

1. Log into your switch management page (see "Access your switch management page" on page 9).

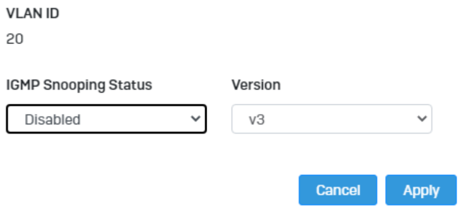
2. Click on **Network**, click on **IGMP Snooping**, and click on **VLAN Settings**.

3. Select the VLAN ID to configure



VLAN ID	IGMP Snooping Status	Version	Action
1	Off	v3	Edit
20	Off	v3	Edit

4. Review the settings. Click **Apply** to save the settings.
- **IGMP Snooping Status –** Click the drop-down list and select **Enabled** to enable the IGMP snooping or **Disabled** to disable the feature
- **Version –** Click the drop-down list and select IGMP version



VLAN ID
20

IGMP Snooping Status
Disabled

Version
v3

Querier Settings

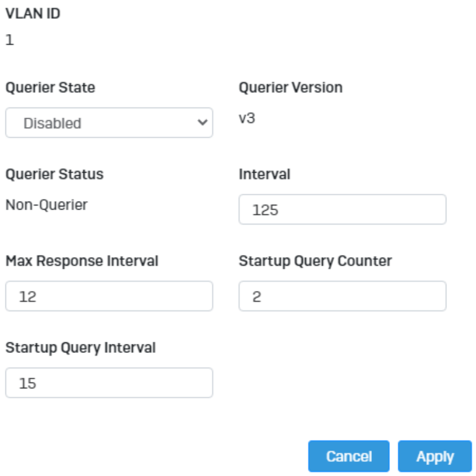
Network > IGMP Snooping > Querier Settings

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network**, click on **IGMP Snooping**, and click on **Querier Settings**.

3. Select the VLAN ID to configure

4. Review the settings. Click **Apply** to save the settings.
- **Querier State –** Click the drop-down list and select **Enabled** to enable the Querier Status or **Disabled** to disable this feature.
- **Interval** – Enter the amount of time you want your switch to send IGMP queries.
- **Max Response Interval**- Specifies the maximum time before sending a response report.
- **Startup Query Counter** – Enter the amount to start the query counter
- **Startup Query Interval** – Enter the amount of time to start the query counter



VLAN ID
1

Querier State
Disabled

Querier Version
v3

Querier Status
Non-Querier

Interval
125

Max Response Interval
12

Startup Query Counter
2

Startup Query Interval
15

Router Settings

Network > IGMP Snooping > Router Settings

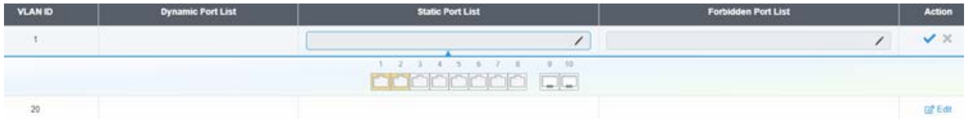
1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network**, click on **IGMP Snooping**, and click on **Router Settings**.

3. Select the VLAN ID to configure

4. Review the settings. Click **Check Mark** to save the settings.

- Click the Static Port List and select the ports you would like to statically assign
- Click the Forbidding Port List and select the ports you would like to assign to the Forbidden List



VLAN ID	Dynamic Port List	Static Port List	Forbidden Port List	Action
1				✓ ✕
20				Edit

MLD Snooping

Global Settings

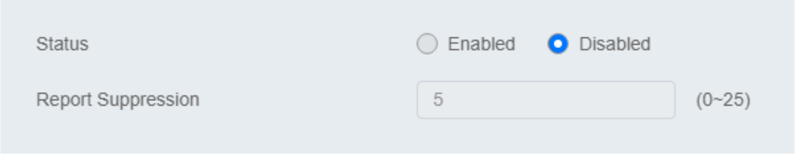
Network > MLD Snooping > Global Settings

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network**, click on **MLD Snooping**, and click on **Global Settings**.

3. Review the settings. Click **Apply** to save the settings.

- **Status** – Select **Enabled** to enable the MLD snooping feature or **Disabled** to disable the feature.
- **Report Suppression** – Enter the time suppression interval between 0 – 25.



Status ○ Enabled ● Disabled

Report Suppression 5 (0~25)

Fast Leave

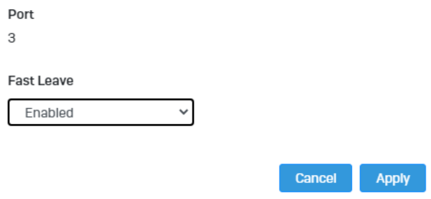
Network > MLD Snooping > Port Settings

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Network**, click on **MLD Snooping**, and click on **Port Settings**.

3. Review the settings. Click **Apply** to save the settings.

- **Fast Leave –** Select **Enabled** to enable Fast Leave from the selected port or **Disabled** to disable the feature



Port
3

Fast Leave
Enabled

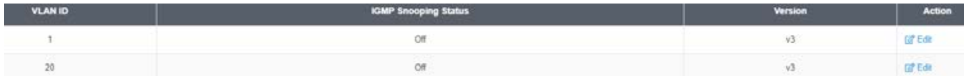
VLAN Settings

Network > IGMP Snooping > VLAN Settings

1. Log into your switch management page (see "Access your switch management page" on page 9).

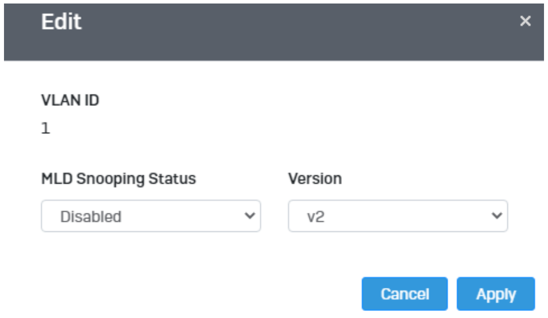
2. Click on **Network**, click on **MLD Snooping**, and click on **VLAN Settings**.

3. Select the VLAN ID to configure



VLAN ID	IGMP Snooping Status	Version	Action
1	Off	v3	Edit
20	Off	v3	Edit

4. Review the settings. Click **Apply** to save the settings.
   - **MLD Snooping Status –** Click the drop-down list and select **Enabled** to enable the IGMP snooping or **Disabled** to disable the feature
   - **Version –** Click the drop-down list and select IGMP version



Edit

VLAN ID
1

MLD Snooping Status
Disabled

Version
v2

Querier Settings

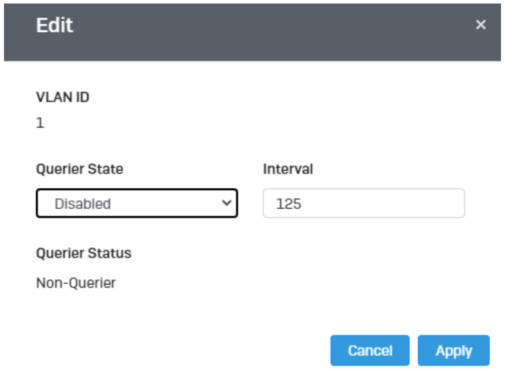
Network > MLD Snooping > Querier Settings

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network**, click on **MLD Snooping**, and click on **Querier Settings**.

3. Select the VLAN ID to configure

4. Review the settings. Click **Apply** to save the settings.
   - **Querier State –** Click the drop-down list and select **Enabled** to enable the Querier Status or **Disabled** to disable this feature.
   - **Interval** – Enter the amount of time you want your switch to send IGMP queries.



Edit

VLAN ID
1

Querier State
Disabled

Interval
125

Querier Status
Non-Querier

Router Settings

Network > MLD Snooping > Router Settings

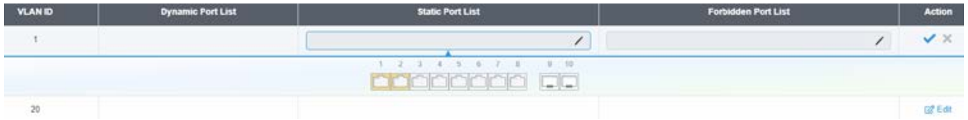
1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Network**, click on **MLD Snooping**, and click on **Router Settings**.

3. Select the VLAN ID to configure

4. Review the settings. Click **Check Mark** to save the settings.

- Click the **Static Port List** and select the ports you would like to statically assign
- Click the **Forbidding Port List** and select the ports you would like to assign to the Forbidden List



VLAN ID	Dynamic Port List	Static Port List	Forbidden Port List	Action
1				✓ ✕
20				Edit

Loopback Detection

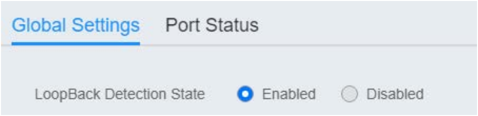
Global Settings

Network > Loopback Detection > Global Settings

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network**, click on **Loopback Detection**, and click on **Global Settings**.

3. Select **Enabled** to enable loopback detection, or **Disabled** to disable this feature



LoopBack Detection State ● Enabled ○ Disabled

4. At the top right panel, click the **Apply** button to save the changes to the Flash.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied*

Voice VLAN

This chapter contains a description of the Switch's Voice VLAN feature and the procedures to create, modify, and delete a voice VLAN configuration.

The Voice VLAN feature is specifically designed to maintain high quality, uninterrupted voice traffic through the switch. When talking on a voice over IP phone, a user expects to have no interruptions in the conversation and excellent voice quality. The Voice VLAN feature can be configured to meet these requirements.

CoS with Voice VLAN

The Voice VLAN CoS parameter maintains the voice quality between the ingress and egress ports of the switch. CoS must be enabled for the Voice VLAN CoS priority to take effect. The CoS priority level that you config is applied to voice traffic on all ports of the voice VLAN. Normally, most (non-Voice) Ethernet traffic transverses the switch through lower order egress queues. To avoid delays and interruptions in the voice data flow, the CoS priority level assigned to the voice VLAN should be mapped to a higher order queue and the scheduling algorithm should be set to Strict Priority. These settings ensure that the voice data packets are processed before other types of data so that the voice quality is maintained as the voice data passes through the switch.

Organization Unique Identifier (OUI)

Each IP phone manufacturer can be identified by one or more Organization Unique Identifiers (OUIs). An OUI is three bytes long and is usually expressed in hexadecimal format. It is imbedded into the first part of each MAC address of an Ethernet network device. You can find the OUI of an IP phone in the first three complete bytes of its MAC address.

Typically, you will find that all of the IP phones you are installing have the same OUI in common. The switch identifies a voice data packet by comparing the OUI information in the packet's source MAC address with an OUI table that you configure when you initially set up the voice VLAN. This is important when the Auto-Detection feature for a port and is a dynamic voice VLAN port.

When you are configuring the voice VLAN parameters, you must enter the complete MAC address of at least one of your IP phones. An "OUI Mask" is automatically generated and applied by the Web Management Utility software to yield the manufacturer's OUI. If the OUI of the remaining phones from that manufacturer is the same, then no other IP phone MAC addresses need to be entered into the configuration.

However, it is possible that you can find more than one OUI from the same manufacturer among the IP phones you are installing. It is also possible that your IP phones are from two or more different manufacturers in which case you will find different OUIs for each manufacturer. If you identify more than one OUI among the IP phones being installed, then one MAC address representing each individual OUI must be configured in the voice VLAN. You can enter a total of 10 OUIs.

Dynamic Auto-Detection vs Static Ports

Prior to configuring the voice VLAN, you must configure a tagged VLAN which is the basis for the voice VLAN configuration. The VLAN must be configured with one or more tagged or untagged ports that will serve as the voice VLAN uplink/downlink. By default, a tagged or untagged port is a static member of a tagged VLAN. The ports that you choose to configure as dynamic Auto-Detection ports

must be connected directly to an IP phone. When you initially define the ports of a tagged VLAN for your voice VLAN configuration, they must be configured as a "Not Member" ports. The "Not Member" ports are eligible to dynamically join the voice VLAN when voice data is detected with a predefined OUI in the source MAC address. The port will leave the voice VLAN after a specified timeout period. This port behavior is configured with the voice VLAN Auto-Detection feature.

For the Auto-Detection feature to function, your IP phone(s) must be capable of generating 802.1Q packets with imbedded VLAN ID tags. You must manually configure your IP phone(s) for the same VLAN ID as the switch's voice VLAN ID. When voice data is detected on one of the "Not Member" ports, the packets from the IP phone will contain the voice VLAN ID so they are switched within the switch's voice VLAN.

One or more ports in your voice VLAN must be configured as Static tagged or untagged members. Static VLAN members are permanent member ports of the voice VLAN and there is no dependency on the configuration of the devices connected to the ports. These ports might be connected to other voice VLAN network nodes such as other Ethernet switches, a telephone switch, or a DHCP server. The voice VLAN Auto-Detection feature cannot be enabled on Static tagged or tagged ports.

Note: *Any Static tagged members of the voice VLAN are required to have the port VLAN ID (PVID) configured to be the same as the voice VLAN ID. This insures that all untagged packets entering the port are switched within the voice VLAN as the voice data passes through the switch.*

If the IP phone(s) that you are installing cannot be configured with a VLAN ID, then the switch ports should be configured as Static tagged ports within the voice VLAN.

Note: *Link Layer Discovery Protocol for Media Endpoint Devices (LLDP- MED) is not supported on the switch. Each IP phone that is VLAN aware should be manually configured for the VLAN ID that matches your voice VLAN ID. Each of the voice VLAN ports connected to an IP phone should be configured as "Not Member" ports of the tagged VLAN.*

Global Settings

Network > Voice VLAN > Global Settings

Note: *Prior to configuring your voice VLAN, you must first configure a tagged VLAN. This VLAN will be used as a basis for your voice VLAN.*

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network**, click on **Voice VLAN,** and click on **Global Settings**.

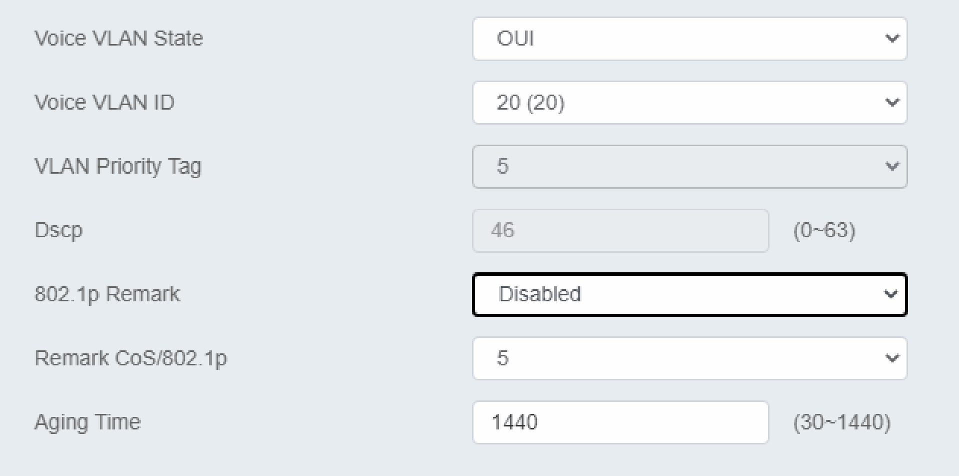
3. Review the settings.

Use the following procedure to configure voice VLAN:

- **Voice VLAN State –** Select **Disabled** to disable this feature, or **Auto** to allow this feature to be automatically enable and disable or set it to **OUI** to use pre-selected OUI VLANs
- **Voice VLAN ID** - This parameter is the tagged VLAN ID that has been configured in "Tagged VLAN Configuration". It is a pull-down menu showing the tagged VLAN IDs that have been defined.
- **VLAN Priority Tag** – This parameter sets the priority of the VLAN. The priority is configured through the pull-down menu.
- **DSCP**: Configure the DSCP for your switch. The range is from 0-63.
- **802.1p Remark –** Enable 802.1p QoS for the assigned OUI

- **Remark CoS / 802.1p** - This parameter is CoS priority level assigned to the voice data packets received on each voice VLAN port. For the **COS** priority to be effective, **802.1p Remark** must be **Enabled**.
- **Aging Time** - This parameter indicates the amount of time, in hours, after the last IP phone's OUI was received on a port, after which this port will be removed from the voice VLAN. The range is 30 to 1440.

4. Click **Apply** to save the settings.



Voice VLAN State	OUI	
Voice VLAN ID	20 (20)	
VLAN Priority Tag	5	
Dscp	46	(0~63)
802.1p Remark	Disabled	
Remark CoS/802.1p	5	
Aging Time	1440	(30~1440)

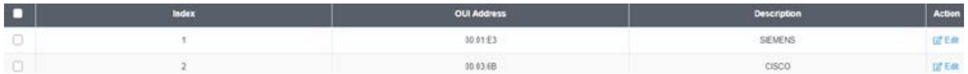
OUI Settings

Network > Voice VLAN > OUI Settings

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network**, click on **Voice VLAN,** and click on **OUI Settings**.

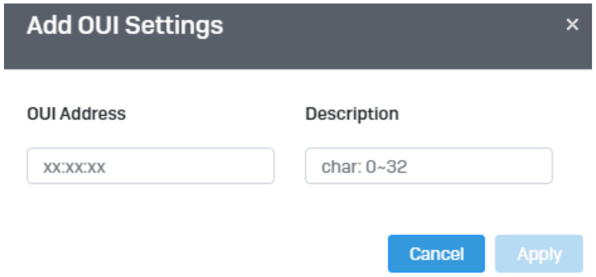
3. Select from the table to use a pre-defined OUI. To modify a pre-defined OUI, click **Edit** on the far right of the table. To delete an OUI from this table, select the OUI Index and click **Delete.**



□	Index	OUI Address	Description	Action
□	1	00:01:E3	SIEMENS	Edit
□	2	00:03:6B	CISCO	Edit

4. To add a new OUI to the table, click on **Add**.

5. Input the **OUI Address** and the name of your OUI. Click **Apply** to save it to the OUI settings table.



Add OUI Settings ×

OUI Address	Description
xx:xx:xx	char: 0~32

Port Settings

Network > Voice VLAN > Port Settings

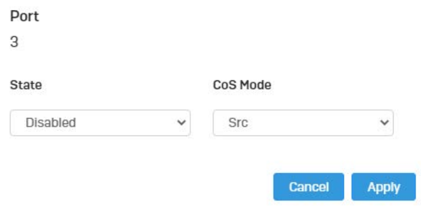
1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network**, click on **Voice VLAN,** and click on **Port Settings**.

3. Select the port and click **Edit** to configure the settings of that port.

4. Review the settings and click **Apply** to save your settings to the flash.

- **State** – Select **Enabled** to enable COS mode or **Disabled** to disable this feature.
- **CoS Mode** – Select **Src mode** or **All**



Port
3

State: Disabled
CoS Mode: Src

LLDP

Enable and configure LLDP

Link Layer Discovery Protocol (LLDP) allows Ethernet network devices, such as switches and routers, to receive and transmit device-related information to directly connected devices on the network and to store data that is learned about other devices.

Settings

Network > LLDP > Global Settings

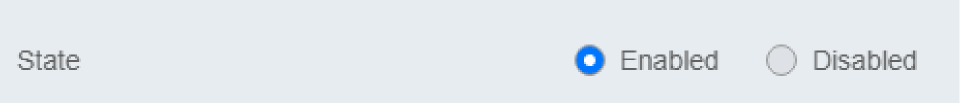
1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network**, click on **LLDP,** and click on **Settings**.

3. Review the settings.

Enabling or Disabling LLDP

- From the **LLDP** parameter, select one of the following radio button choices and click **Apply** to save the settings.
  - **Enable:** The LLDP feature is active.
  - **Disable:** The LLDP feature is inactive.



State ● Enabled ○ Disabled

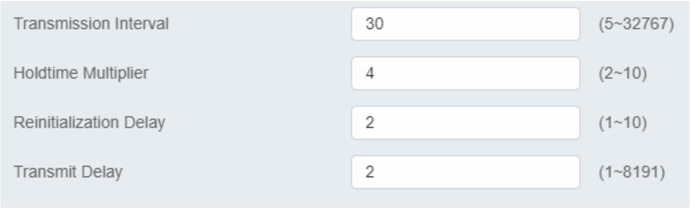
Configure the LLDP Parameter Settings

Transmission Interval: Sets the transmit interval, which is the interval between regular transmissions of LLDP advertisements. The range is from 5 to 32767 seconds.

Holdtime Multiplier: Sets the hold multiplier value. The hold time multiplier is multiplied by the transmit interval to give the Time To Live (TTL) that the switch advertises to the neighbors. The range is from 2 to 10.

Reinitialization Delay: Sets the reinitialization delay, which is the number of seconds that must elapse after LLDP is disabled on a port before it can be reinitialized. The range is from 1 to 10 seconds.

Transmit Delay: Sets the value of the transmission delay timer, which is the minimum time interval between transmissions of LLDP advertisements due to a change in LLDP local information. The range is from 1 to 8191 seconds.



Transmission Interval	30	(5~32767)
Holdtime Multiplier	4	(2~10)
Reinitialization Delay	2	(1~10)
Transmit Delay	2	(1~8191)

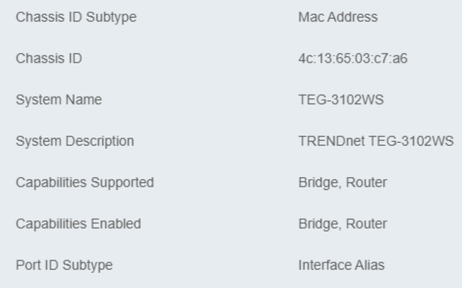
Click **Apply** to save the settings.

View LLDP System Information

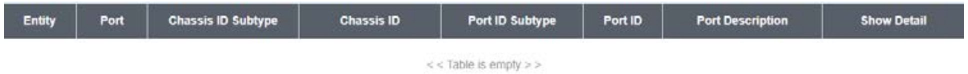
Network > LLDP > Local Device

- **Chassis ID Subtype:** This parameter describes the Chassis ID subtype which is "macAddress". You cannot change this parameter.
- **Chassis ID:** This parameter lists the MAC Address of the switch. You cannot change this parameter.
- **System Name:** This parameter lists the System Name of the switch. You can assign the system name from **System Settings.**
- **System Description:** This parameter lists the product name of the switch. You cannot change this parameter
- **Capabilities Supported:** This parameter lists the capabailities that can be supported. You cannot change this parameter.

- **Capabilities Enabled:** This parameter lists the capabilities that are enabled. You cannot change this parameter.
- **Port ID Subtype:** This parameter lists the Port ID. This parameter cannot be changed.



Chassis ID Subtype	Mac Address
Chassis ID	4c:13:65:03:c7:a6
System Name	TEG-3102WS
System Description	TRENDnet TEG-3102WS
Capabilities Supported	Bridge, Router
Capabilities Enabled	Bridge, Router
Port ID Subtype	Interface Alias



Entity	Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Port Description	Show Detail

<< Table is empty >>

Multicast Filtering

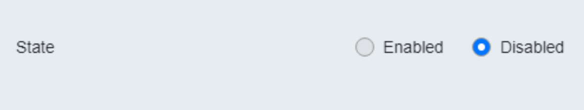
Enable Multicast Filtering

Network > Multicast Filtering

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network** and click on **Multicast Filtering**.

3. Select **Enabled** to enable this feature or **Disabled** to disable Multicast Filtering



State ○ Enabled ● Disabled

4. At the top right panel, click the **Apply** button to save the changes to the Flash.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied*

Administration

Changing login credentials

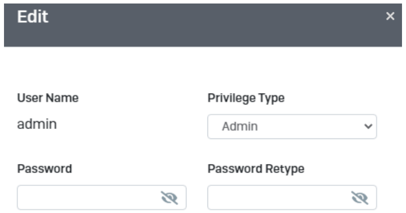
Network > Administration

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network** and click on **Administration**.

3. Click on **Add** on the top right corner to create a new username and password. To modify an existing username, click **Edit** to modify the selected login credentials

4. Review the settings below and click apply to save the changes to your flash
   - **Privilege Type**: Set the privilege for the selected username to either Admin or User.
   - **Password**: Set the password for this new username
   - **Password Retype**: Re-type your password.



Edit ×

User Name	Privilege Type
admin	Admin
Password	Password Retype

Logs

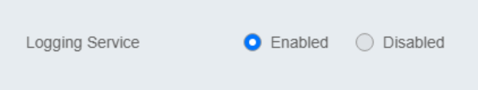
Settings

Network > Logs > Global Settings

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network,** click on **Logs,** and click on **Global Settings** .

3. Select **Enabled** to enable logs, or **Disabled** to disable this feature.


Logging Service ● Enabled ○ Disabled

Remote Logging

Network > Logs > Remote Logging

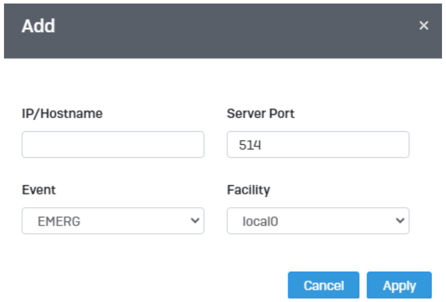
1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network,** click on **Logs,** and click on **Remote Logging** .

3. Click on **Add** on the top right corner to create a new username and password. To modify an existing username, click **Edit** to modify the selected login credentials

4. Review the settings and click **Apply** to save the changes to the Flash.

- IP/Hostname: Enter the IP address of the location you want the Log files to go to.
- **Server Port:** Enter the port number of the IP address
- **Event:** Select what type of log events will be sent to the IP Address


Add

IP/Hostname:

Server Port: 514

Event: EMERG

Facility: local0

Log Table

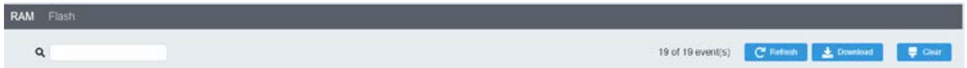
Network > Logs > Log Table

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Network,** click on **Logs,** and click on **Log Table**.

3. Review the settings below.

- **RAM:** Displays only log files that are stored on the RAM
- **Flash:** Displays only log files that were stored on the Flash
- **Refresh:** Refreshes the page
- **Download:** Download the log file. Download files can only be saved as .txt files.
- **Clear:** Erases all log files


19 of 19 event(s)

QoS (Quality of Service)

When a port on an Ethernet switch becomes oversubscribed, its egress queues contain more packets than the port can handle in a timely manner. In this situation, the port may be forced to delay the transmission of some packets, resulting in the delay of packets reaching their destinations. A port may be forced to delay transmission of packets while it handles other traffic, and, in some situations, some packets destined to be forwarded to an oversubscribed port from other switch ports may be discarded.
Minor delays are often of no consequence to a network or its performance. But there are applications, referred to as delay or time sensitive applications, which can be impacted by packet delays. Voice transmission and video conferences are two examples. If packets carrying data in either of these cases are delayed from reaching their destination, the audio or video quality may suffer.
This is where Cost of Service (CoS) is of value. It allows you to manage the flow of traffic through a switch by having the switch ports give higher priority to some packets, such as delay sensitive traffic, over other packets. This is referred to as prioritizing traffic.

Global Settings

Set QoS settings

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **QoS** and click on **Global Settings**.

3. Select **Enabled** to enable QoS and **Disabled** to disable this feature.

4. Set the scheduling method:

- **Strict Priority** - The port transmits all packets out of higher priority queues before transmitting any from the lower priority queues.
- **WRR (Weighted RoundRobin)** - The port transmits a set number of packets from each queue, in a round robin fashion, so that each has a chance to transmit traffic.

4. Select the Trust Mode:

- **DSCP –** Priority of packets is based on the ToS (Types of Service) field in the IP header
- **802.1p –** Priority of packets is based off of the PRI value.
- **802.1p – DSCP -**

CoS

Set CoS priority settings

QoS > CoS Mapping

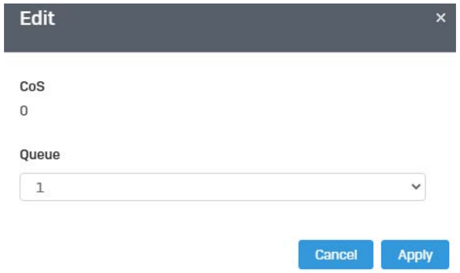
Note: *Before mapping the CoS priorities and the egress queues, you must disable the* ***Jumbo*** *frame parameter on each port. When* ***Jumbo*** *frames are enabled, COS cannot be enabled.*

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **QoS** and click on **CoS Mapping.**

3. In **QoS Status**, select the **CoS Table** (0-7) that applies to your configuration and click **Edit.**

4. Set each Queue ID (1-8) for the selected **CoS Table.** Click **Apply** to save the settings.



Edit ×

CoS
0

Queue
1

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

DSCP Mapping

Set DSCP (Differentiated Services Code Point) Class Mapping settings

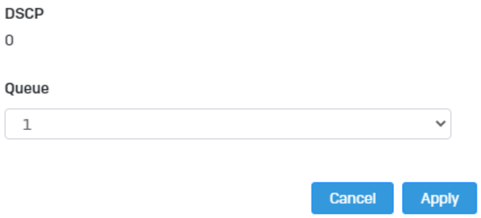
QoS > DSCP Mapping

If you choose to use the DSCP tags in your Access Control policy configuration, each DSCP value (0-63) that is relevant to your configuration needs to be mapped to one of the four egress queues (Low, Medium, High, or Highest). The default queue for all DSCP values is 0. To assign the queue mappings to the DSCP values, perform the following procedure.

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **QoS** and click on **DSCP Mapping**.

3. Select the relevant DSCP value to configure and click **Edit** to modify the Queue ID for the selected DSCP value. Click **Apply** to save the settings.



DSCP
0

Queue
1

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

Port CoS

Set Port Priority

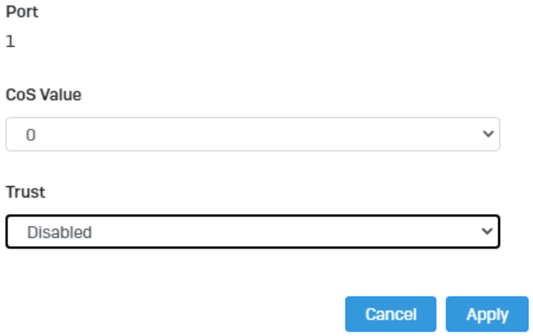
QoS > Port CoS

The Port Priority values are assigned to an untagged frame at ingress for internal processing in the switch. This procedure explains how to change the default mappings of port priorities to the User Priority. This is set at the switch level. You cannot set this at the per-port level. To change the port priority mappings, perform the following procedure.

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **QoS** and click on **Port CoS**.

3. For each port whose priority you want to change, select a priority (0-7, Ignore) in the **CoS Value**. Click **Apply** to save the settings.



Port
1

CoS Value
0

Trust
Disabled

4. At the bottom of the left hand panel, click **Apply**.

.

Bandwidth Control

Bandwidth Control

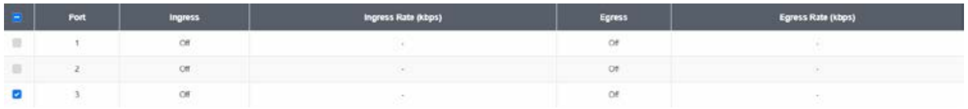
QoS > Bandwidth Control

This section allows you to configure the DLF (Destination Lookup Failure), broadcast, and multicast storm settings for each switch port.

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **QoS**, click on **Bandwidth Control**

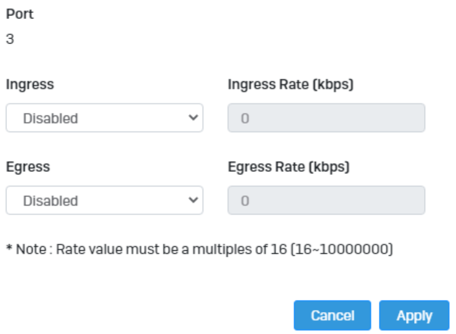
3. Select the port to modify and click the **Edit** button.



☐	Port	Ingress	Ingress Rate (kbps)	Egress	Egress Rate (kbps)
☐	1	Off	-	Off	-
☐	2	Off	-	Off	-
☑	3	Off	-	Off	-

4. Review the settings below and click **Apply** to save your settings.

- **Ingress –** Select **Enabled** to enable Ingress Rate Limiting or **Disabled** to disable this feature.
- **Ingress Rate (kbps) -** Enter the ingress rate limit value.
- **Egress –** Select **Enabled** to enable Egress Rate Limiting or **Disabled** to disable this feature.
- **Egress Rate (kbps) –** Enter the egress rate limit value.



Port
3

Ingress: Disabled
Ingress Rate (kbps): 0

Egress: Disabled
Egress Rate (kbps): 0

* Note : Rate value must be a multiples of 16 (16~10000000)

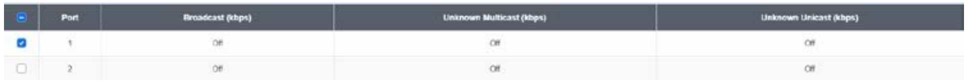
Storm Control

QoS > Storm Control

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **QoS**, click on **Storm Control**

3. Select the port to and click **Edit** to modify.

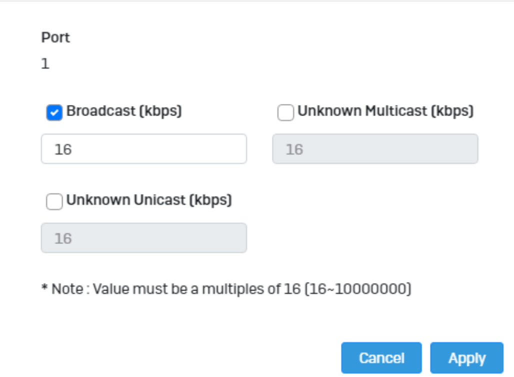


☐	Port	Broadcast (kbps)	Unknown Multicast (kbps)	Unknown Unicast (kbps)
☑	1	Off	Off	Off
☐	2	Off	Off	Off

4. Review the settings for each port. Click **Apply** to save the settings.

- **Broadcast** – Click the empty box to enable Broadcast and enter the limit value for broadcast in kbps.
- **Unknown Multicast** – Click the empty box to enable Multicast and enter the limit value for broadcast in kbps.
- **Unknown Unicast** – Click the empty box to enable Unicast and enter the limit value for broadcast in kbps.

  ***Note:** Modifying settings in the row marked **All**, will apply the settings to all ports.*



Port
1

☑ Broadcast (kbps): 16
☐ Unknown Multicast (kbps): 16
☐ Unknown Unicast (kbps): 16

* Note : Value must be a multiples of 16 (16~10000000)

Security

802.1X Authentication

Set 802.1X

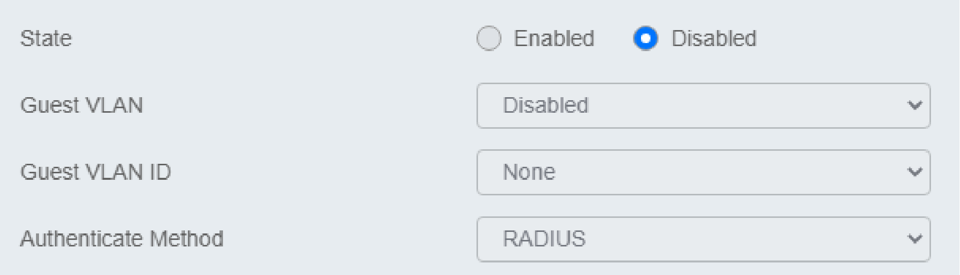
Security > 802.1X > Global Settings

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Security,** click on **802.1X,** and click on **Global Settings.**

3. Review the settings for each port. Next to each port entry, click **Apply** to save the settings.

- **State:** Click **Enabled** to enable 802.1X or **Disabled** to disable this feature.
- **Guest VLAN:** Select **Enabled** to enable 802.1X for Guest VLAN or **Disabled** to disable this feature.
- **Guest VLAN ID:** Select the VLAN ID to apply this setting to.
- **Authenticate Method:** Select **RADIUS, TACAS+** or **Local** as the authenticate method.



State ○ Enabled ● Disabled
Guest VLAN: Disabled
Guest VLAN ID: None
Authenticate Method: RADIUS

Timeout

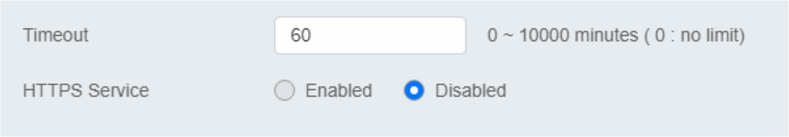
Security > Access > Web

1. Log into your switch management page (see "Access your switch management page" on page 5).

2. Click on **Security,** click on **Access,** and click on **Web.**

3. Review the settings and click **Apply** to save the settings.

- **Timeout**: Input the length of time before your switch times out. Regardless of activity/inactivity, the switch will timeout in the specific time.
  ***Note**: By default, the timeout duration is set to 30 minutes.*
- **HTTPS Service**: Select **Enabled** to enable this feature or **Disabled** to disable it.



Timeout 60 0 ~ 10000 minutes (0 : no limit)

HTTPS Service ○ Enabled ● Disabled

CLI Timeout

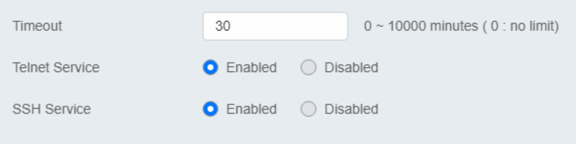
Security > Access > Web

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Security,** click on **Access,** and click on **CLI.**

3. Review the settings and click **Apply** to save the settings.

- **Timeout**: Input the length of time before your switch times out. Regardless of activity/inactivity, the switch will timeout in the specific time.
  ***Note**: By default, the timeout duration is set to 30 minutes.*
- **Telnet Service**: Select **Enabled** to enable Telnet or **Disabled** to disable this feature.
- **SSH Service**: Select **Enabled** to enable Telnet or **Disabled** to disable this feature.



Timeout 30 0 ~ 10000 minutes (0 : no limit)

Telnet Service ● Enabled ○ Disabled

SSH Service ● Enabled ○ Disabled

Port Security

Security > Port Security

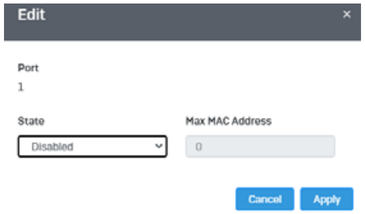
1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Security,** and click on **Port Security.**

3. Select the port to configure, and click **Edit** to configure the selected port.

4. Review the settings and click **Apply** to save your settings.

- **State**: Select **Enabled** from the drop down menu to enable this feature and **Disabled** to disable this feature.
- **Max MAC Address**: Enter the max number of MAC Addresses. The max number is 256.



Port 1

State Disabled

Max MAC Address 0

Access Control: Creating MAC ACL

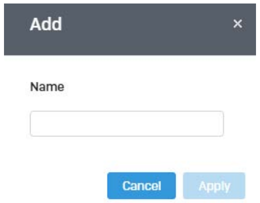
Security > Access Control > MAC ACL

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Security,** then click on **Access Control,** and click on **MAC ACL.**

3. Click the **Add** button to create a new ACL.

4. Input a name in the field and click **Apply** to save your new ACL name to the Flash.



Access Control: Configuring MAC ACL

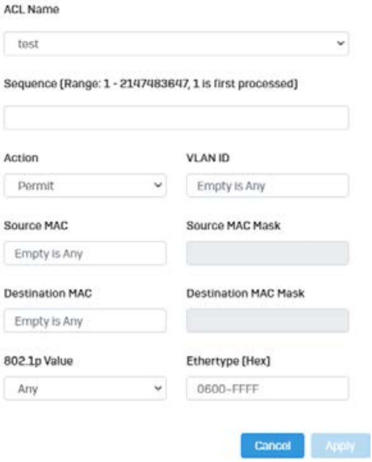
Security > Access Control > MAC ACE

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Security,** then click on **Access Control,** and click on **MAC ACE.**

3. Review the settings below and click **Apply** to save your settings.

- **ACL Name:** Select the ACL name you would like to configure.
- **Sequence:**
- **Action:** Defines the ACl action linked to the rule criteria.
  - o **Permit-** This selection allows ingress packets that conform to the specified ACL criteria.
  - o **Deny-** This selection drops ingress packets that conform to the specified ACL criteria.
- **VLAN ID:** Enter the VLAN ID to associate with this MAC ACL.
- **Source MAC**: Input the source of the MAC address
- **Destination MAC**: Input the destination MAC address
- **Source MAC Mask & Destination MAC Mask**: Enter the mask of the Source MAC and Destination MAC.
- **802.1p Value:** Select the priority to assign with 7 being the highest priority and 0 being the lowest.
- **Ethertype (Hex)-** Specifies EtherType packet filtering



ACL Name: test

Sequence (Range: 1 - 2147483647, 1 is first processed)

Action: Permit

VLAN ID: Empty is Any

Source MAC: Empty is Any

Source MAC Mask

Destination MAC: Empty is Any

Destination MAC Mask

802.1p Value: Any

Ethertype (Hex): 0600-FFFF

Access Control: Creating IPv4 ACL

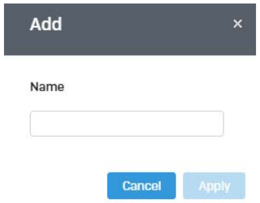
Security > Access Control > IPv4 ACL

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Security,** then click on **Access Control,** and click on **IPv4 ACL.**

3. Click the **Add** button to create a new ACL.

4. Input a name in the field and click **Apply** to save your new ACL name to the Flash.


Add ×

Name

Access Control: Configuring IPv4 ACL

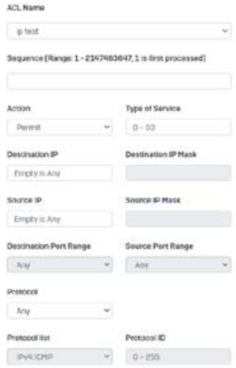
Security > Access Control > IPv4 ACE

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Security,** then click on **Access Control,** and click on **MAC ACE.**

3. Review the settings below and click **Apply** to save your settings.

- **ACL Name:** Select the ACL name you would like to configure.
- **Sequence:**
- **Action:** Defines the ACl action linked to the rule criteria.
  - **Permit-** This selection allows ingress packets that conform to the specified ACL criteria.
  - **Deny-** This selection drops ingress packets that conform to the specified ACL criteria.
- **Type of Service:** Enter a number in the **Type of Service** field within the range of 0 to 63. This field indicates the DSCP level of interest. This field is not mandatory and you may elect to leave it blank.
- **Destination IP**: Input the destination IP address
- **Source IP**: Input the source of the IP address
- **Source IP Mask & Destination IP Mask**: Enter the mask of the Source MAC and Destination MAC.
- **Protocol:** Select the protocol
  - **Select from list:** Select from a pre-defined list below under "IGMP List"
  - **Select from Protocol ID:** Input the protocol ID between the range of 0-255.
- **IGMP:** Select the from the drop down menu
  - **Select from list:** Select from a pre-defined list below under "Protocol List"
  - **Select from IGMP ID:** Input the protocol ID between the range of 0-255.


ACL Name
ip test

Sequence (Range: 1 - 2147483647, 1 is first processed)

Action
Permit

Type of Service
0 - 63

Destination IP
Empty is Any

Destination IP Mask

Source IP
Empty is Any

Source IP Mask

Destination Port Range
Any

Source Port Range
Any

Protocol
Any

Protocol list
IPv4:ICMP

Protocol ID
0 - 255

Access Control: Creating IPv6 ACL

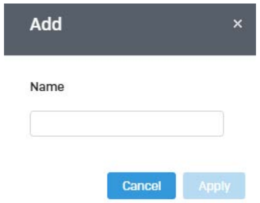
Security > Access Control > IPv6 ACL

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Security,** then click on **Access Control,** and click on **IPv6 ACL.**

3. Click the **Add** button to create a new ACL.

4. Input a name in the field and click **Apply** to save your new ACL name to the Flash.



Access Control: Configuring IPv6 ACL

Security > Access Control > IPv4 ACE

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Security,** then click on **Access Control,** and click on **IPv6 ACE.**

3. Review the settings below and click **Apply** to save your settings.

- **ACL Name:** Select the ACL name you would like to configure.
- **Sequence:**
- **Action:** Defines the ACl action linked to the rule criteria.
  - o **Permit-** This selection allows ingress packets that conform to the specified ACL criteria.
  - o **Deny-** This selection drops ingress packets that conform to the specified ACL criteria.
- **Type of Service:** Enter a number in the **Type of Service** field within the range of 0 to 63. This field indicates the DSCP level of interest. This field is not mandatory and you may elect to leave it blank.
- **Destination IP**: Input the destination IP address
- **Source IP**: Input the source of the IP address
- **Source IP Mask & Destination IP Mask**: Enter the mask of the Source MAC and Destination MAC.
- **Protocol:** Select the protocol
  - o **Select from list:** Select from a pre-defined list below under "IGMP List"
  - o **Select from Protocol ID:** Input the protocol ID between the range of 0-255.
- **IGMP:** Select the from the drop down menu
  - o **Select from list:** Select from a pre-defined list below under "Protocol List"
  - o **Select from IGMP ID:** Input the protocol ID between the range of 0-255.

Port Binding

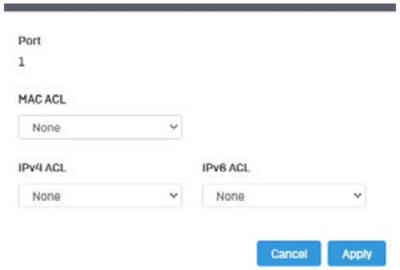
Security > Access Control > Port Binding

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Security**, click on **Access Control,** and click on **Port Binding**.

3. Select the port you would like to bind to a specific ACL and click **Edit.**

4. Select from the list of ACLs and click **Apply** to save your settings.


Port: 1

MAC ACL: None

IPv4 ACL: None

IPv6 ACL: None

Dial-in User

Create Dial-In Users (Local Authentication Method)

Security > Dial-in User

Dial-in User feature provides the local authentication server for port security when a remote (RADIUS) server is not available.

The Dial-in User (local) authentication method allows you to set up 802.1x authentication parameters internally in the Switch. In this case, the user name and password combinations are entered with an optional VLAN when they are defined. Based on these entries, the authentication process of a supplicant is done locally by the Switch Management Utility using a standard EAPOL (EAP over LAN) transaction.

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Security** and click on **Dial-In User**.

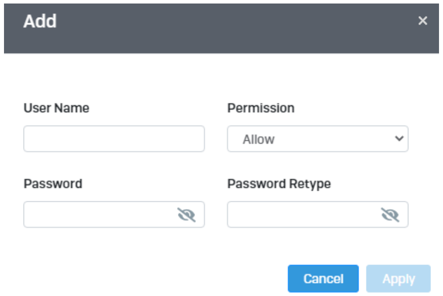
3. Click **Add** to create a dial-in user for local authentication.

4. Review the settings.

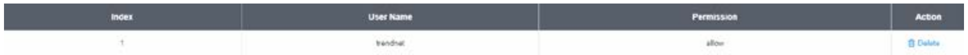
To create a dial-in user for local authentication, use the following procedure:

- In the **User Name** field, type a name for the user.
- In the **Permission** field, select **Allow** to allow this user to access or **Deny** to not grant this user access.
- In the **Password** field, type a password for the user.
- In the **Password Retype** field, re-type the password to confirm.

Click **Apply** to add the entry to the table.



In the list, you can **Delete** the entry**.**



Index	User Name	Permission	Action
1	trendnet	allow	🗑 Delete

RADIUS

Add Radius Servers (RADIUS Authentication Method)

Security > RADIUS Server

1. Log into your switch management page (see "Access your switch management page" on page 9).

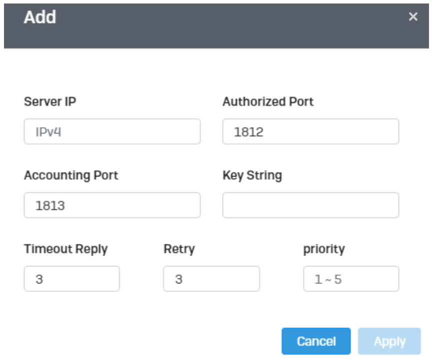
2. Click on **Security** and click on **Radius Server**.

3. Click **Add** to create a new Radius Server.

4. Review the settings.

- **Server IP**–Input the IPv4 IP address of the RADIUS server you would like to add.
- **Authorized Port (1 - 65535)** –Set the RADIUS authentic server(s) UDP port. The default port is 1812.
- **Accounting Port (1 - 65535)** –Set the RADIUS account server(s) UDP port. The default port is 1813.
- **Key String – Enter the default authentication and encryption key for RADIUS communication between the device and the RADIUS server.**
- **Timeout Reply –** Enter the max number of timeouts before it retries
- **Retry –** Enter the max number of retries before it stops trying to recover
- **Server Priority** – Enter the RADIUS Server priority (Highest: 1, Lowest: 5).

Click **Apply** to add the entry to the table.



Add ×

Server IP: IPv4

Authorized Port: 1812

Accounting Port: 1813

Key String:

Timeout Reply: 3

Retry: 3

priority: 1 ~ 5

TACACS+

Add TACACS+ Servers (TACACS+ Authentication Method)

Security > TACACS+

Terminal Access Controller Access Control System (TACACS+) provides centralized security user access validation. The system supports up-to 5 TACACS+ servers.

TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes.

The TACACS+ protocol ensures network integrity through encrypted protocol exchanges between the client and TACACS+ server. The user-assigned TACACS+ parameters are applied to newly defined TACACS+ servers. If values are not defined, the system defaults are applied to the new TACACS+ servers.

1. Log into your switch management page (see "Access your switch management page" on page 9).

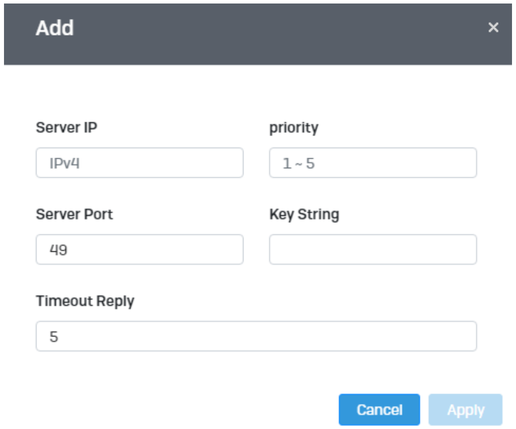
2. Click on **Security** and click on **TACACS+**.

3. Click **Add** to create a new TACAS+

4. Review the settings.

- **Server IP**– Enter the TACACS+ Server IP address.
- **Server Priority** – Enter the TACACS+ Server priority (Highest: 1, Lowest: 5).
- **Server Port** – Enter the port number via which the TACACS+ session occurs. The default port is port 49.
- **Key String** – Enter the default authentication and encryption key for TACACS+ communication between the device and the TACACS+ server.
- **Timeout** – Enter the amount of time (in seconds) the device waits for an answer from the TACACS+ server before retrying the query, or switching to the next server. Possible field values are 1-255. The default value is 5.

Click **Apply** to add the entry to the table.



Add ×

Server IP: IPv4

priority: 1 ~ 5

Server Port: 49

Key String:

Timeout Reply: 5

DHCP Snooping

Settings

DHCP Snooping > Settings

Here is a summary of the rules to observe when you configure DHCP Snooping:

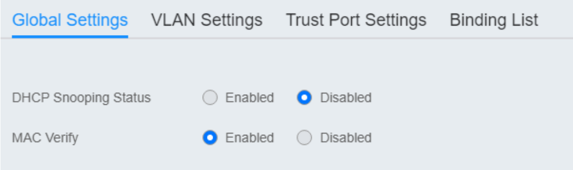
- A trusted port is connected to one of the following:
    - Directly to the legitimate trusted DHCP Server.
    - A network device relaying DHCP messages to and from a trusted server.
    - Another trusted source such as a switch with DHCP Snooping enabled.
    - Untrusted ports are connected to DHCP clients and to traffic that originates outside of the local area network.
- The VLANs to which the DHCP Snooping feature applies must be specified in the DHCP Snooping VLAN Setting configuration.
- Any static IP addresses on the network must be manually added to the Binding Database.

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Security**, click on **DHCP Snooping,** and click on **Global Settings**.

3. Review the settings..

- **DHCP Snooping Status** - Select one of the following radio button choices:
    - **Enabled** - This parameter activates the DHCP Snooping feature.
    - **Disabled** - This parameter de-activates the DHCP Snooping
- **MAC Verify -** Select one of the following choices:
    - **Enable -** The MAC address of each ingress ARP packet is validated when compared against the Binding Table entries. Invalid ARP packets are discarded.
    - **Disable** - The MAC address of each ingress ARP packet is not validated against the Binding Table. All ARP packets are forwarded through the switch without regard to the IP and MAC Address information in the packet header.



DHCP Snooping Status ○ Enabled ● Disabled

MAC Verify ● Enabled ○ Disabled

4. Click **Apply** to save the settings to the Flash.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

VLAN

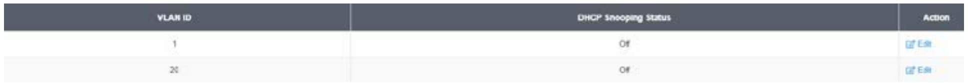
Security > DHCP Snooping > VLAN Settings

In this section, you can define an existing VLAN to apply DHCP snooping.

1. Log into your switch management page (see "Access your switch management page" on page 9).

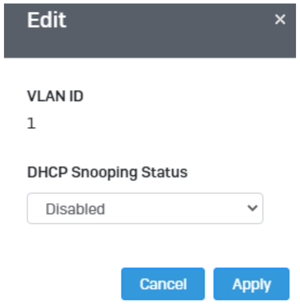
2. Click on **Security**, click on **DHCP Snooping,** and click on **VLAN Settings**.

3. Select the VLAN ID to edit. You can click **Edit** to modify an entry.



VLAN ID	DHCP Snooping Status	Action
1	Off	Edit
20	Off	Edit

4. From the drop down menu, select **Enabled** to enable DHCP Snooping, or **Disabled** to disable this feature. .



VLAN ID
1

DHCP Snooping Status
Disabled

4. Click **Apply** to save the settings to the Flash.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

Trusted Port Interfaces

Security > DHCP Snooping > Trust Port Settings

This section allows you to set trusted port interfaces where DHCP servers can be connected allows or denies DHCP server information to be received on those ports.

1. Log into your switch management page (see "Access your switch management page" on page 9).

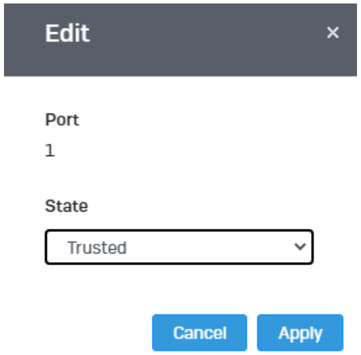
2. Click on **Security**, click on **DHCP Snooping,** and click on **Trust Port Settings**.

3. Next to each port, click on the bubble to select the port to modify and click **Edit**.

4. Review the settings:

- **Untrusted:** This parameter defines the port as untrusted for the DHCP Snooping feature.
- **Trusted:** This parameter defines the port as trusted for the DHCP Snooping feature.

Note: *You can select the row labeled* ***ALL*** *to apply settings to all ports.*



Port
1

State
Trusted

5. Click **Apply** to save the settings to the Flash.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

Denial of Service

Denial of Service (DoS)

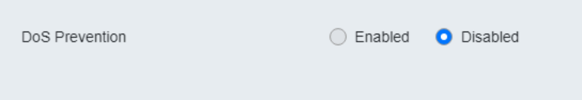
Security > DoS

The switch has built-in DoS prevention features to restrict specific type of traffic associated denial of service attacks on your network. By default, all of the DoS settings are set to Allow, which allow any type of traffic to pass through the switch. Setting one of the items to Deny will set the switch to check for traffic matching the selected item and deny any traffic matching the rule. On the other hand, setting one of rules to Deny may deny a specific type of traffic that may prevent traffic essential to running your network such as devices in load balancing configuration using virtual IP addresses (Ex. If ARP MAC SA Mismatch is set to Deny, it may cause devices in load balance configuration using shared virtual IP addresses communication issues essential for network server load balancing.) For additional security, you can set these rules to Deny as necessary.

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Security** and click on **DoS**

3. Select **Enabled** to enable DoS or **Disabled** to disable DoS.



DoS Prevention ○ Enabled ● Disabled

4. Click **Apply** to save the settings to the Flash.

Note: *This step saves all configuration changes to the NV-RAM to ensure that if the switch is rebooted or power cycled, the configuration changes will still be applied.*

Tools

Firmware Upgrade

Upgrade your switch's firmware

Tools > Firmware Upgrade

TRENDnet may periodically release firmware upgrades that may add features or fix problems associated with your TRENDnet switch model and version. To check if there is a firmware upgrade available for your device, please check your TRENDnet model and version using the link. http://www.trendnet.com/downloads/

In addition, it is also important to verify if the latest firmware version is newer than the one your switch is currently running. To identify the firmware that is currently loaded on your switch, log in to the switch, click on the System Info section or click on Tools and click on Firmware Upgrade. The firmware used by the switch is listed as Runtime Image or Image Version. If there is a newer version available, also review the release notes to check if there were any new features you may want or if any problems were fixed that you may have been experiencing.

1. If a firmware upgrade is available, download the firmware to your computer.

2. Unzip the file to a folder on your computer.

Please note the following:

- Do not interrupt the firmware upgrade process. Do not turn off the device or press the Reset button during the upgrade.
- If you are upgrade the firmware using a laptop computer, ensure that the laptop is connected to a power source or ensure that the battery is fully charged.
- Disable sleep mode on your computer as this may interrupt the firmware upgrade process.
- Do not upgrade the firmware using a wireless connection, only using a wired network connection.
- Any interruptions during the firmware upgrade process may permanently damage your switch.

Firmware Upgrade via HTTP Settings

Tools > Firmware > Firmware Upgrade

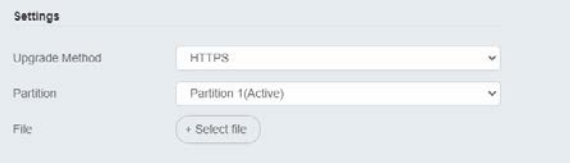
1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Tools**, click on **Firmware**, and click on **Firmware Upgrade**.

3. Select the firmware **Upgrade Method** (HTTPS or TFTP).

4. Select the **Image** you would like to upgrade to.

5. Select the location of the file by clicking **Select file.**



Settings

Upgrade Method: HTTPS

Partition: Partition 1(Active)

File: + Select file

6. Navigate to the folder on your computer where the unzipped firmware file (.*imag*) is located and select it.

5. Click **Apply**. If prompted, click **Yes** or **OK**.

Firmware Upgrade via TFTP Settings

Tools > Firmware Upgrade

Note: *Before using this method, you will require a TFTP server. There are third party TFTP server applications available for this function. If you are not familiar with the TFTP protocol, it is recommended to use the HTTP method.*

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Tools**, click on **Firmware Upgrade**.

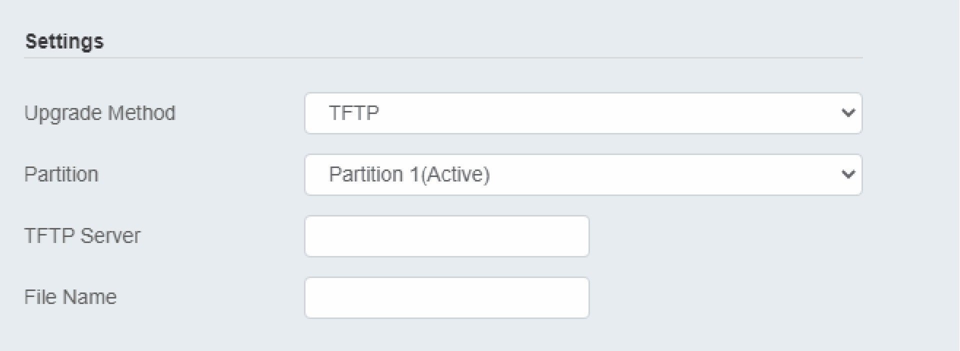
3. Make sure your TFTP server is running and note the IP address of your server and firmware file name. The TFTP server should be in the same IP subnet as the switch.

Note: *It is recommended to that the firmware file (.hex) is placed in your TFTP server root directory.*

5. Review the settings. Click **Apply** to start the firmware upgrade.

- **Upgrade Method:** Select TFTP to update the firmware via TFTP
- **Partition:** Select which image to update the firmware
- **TFTP Server:** Enter the IP address of your TFTP server.
- **File Name:** Enter the firmware filename with extension. *(.hex)*

6. Click **Apply** to start the firmware upgrade.



Settings

Upgrade Method	TFTP
Partition	Partition 1(Active)
TFTP Server	
File Name	

Dual Image

Tools > Firmware > Dual Image

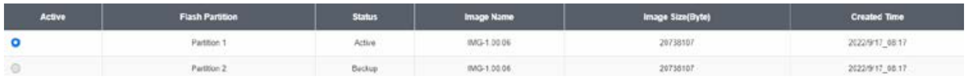
Select the image to bootup on your switch from the next power cycle.

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Tools**, click on **Firmware**, and click on **Dual Image**.

3. Review the settings. Click **Apply** to apply the changes and **Save** to save the changes.

- **Active:** Displays the current Partition Image that is running on the switch. You may select a different partition to boot up with here.
- **Flash Partition:** Name of partition
- **Status:** Displays the status of a partition. A partition that is currently running will display **Active,** while one that is in standby will display **Backup.**
- **Image Name:** Firmware name of the partition
- **Image Size:** Size of the firmware that is loaded on each partition
- **Created Time:** When the firmware was loaded onto the partition



Active	Flash Partition	Status	Image Name	Image Size(Byte)	Created Time
●	Partition 1	Active	IMG-1.00.06	20738107	2022/9/17_08:17
○	Partition 2	Backup	IMG-1.00.06	20738107	2022/9/17_08:17

Config Backup Restore

Config Backup/Restore

Tools > Firmware > Backup/Restore

You may have added many customized settings to your switch and in the case that you need to reset your switch to default, all your customized settings would be lost and would require you to manually reconfigure all of your switch settings instead of simply restoring from a backed up switch configuration file. The configuration will be backed up or restored only to the currently used image.

Backup/Restore via HTTP Settings

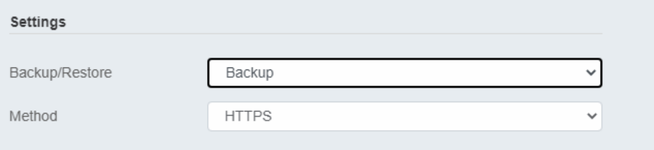
To backup your switch configuration:

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Tools**, click on **Firmware** and click on **Backup/Restore**.

3. Click **Backup** to save the configuration file (.cfg) to your local hard drive. **Startup-config** refers to the configuration that was used to startup this switch.

Note: *If prompted, choose the location on your local hard drive. If you are not prompted, the configuration file (.cfg) will be saved to your default downloads folder.*



Settings

Backup/Restore: Backup

Method: HTTPS

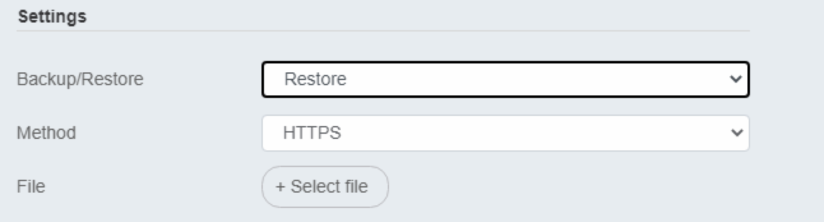
To restore your switch configuration:

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Tools**, click on **Firmware** and click on **Backup/Restore**.

3. Select **Restore** under **Backup/Restore**

Next to **Select File,** depending on your web browser, click on **Browse** or **Choose File**.



Settings

Backup/Restore: Restore

Method: HTTPS

File: + Select file

4. A separate file navigation window should open.

5. Select the switch configuration file to restore and click **Restore**. (Default File Extension: *.cfg*). Click **Apply** to restore the settings,

6. Wait for the switch to restore settings.

Backup/Restore via TFTP Settings

Note: *Before using this method, you will require a TFTP server. There are third party TFTP server applications available for this function. If you are not familiar with the TFTP protocol, it is recommended to use the HTTP method.*

To backup your switch configuration:

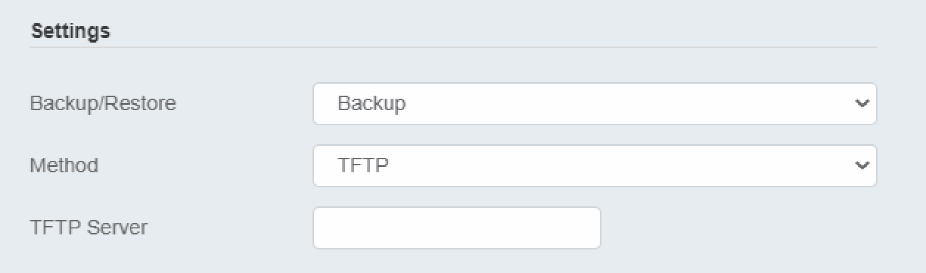
1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Tools**, click on **Firmware** and click on **Backup/Restore**.

3. Make sure your TFTP server is running and note the IP address of your server and firmware file name. The TFTP server should be in the same IP subnet as the switch.

4. Review the settings. Click **Backup** to save the configuration file (config.bin) to your local hard drive on your TFTP server root directory.

- **Backup/Restore:** Select **Backup** to backup your configurations
- **Method:** Select **TFTP** as the method of backing up your configuration
- **TFTP Server IP:** Enter the IP address of your TFTP server.



Settings

Backup/Restore: Backup

Method: TFTP

TFTP Server:

To restore your switch configuration:

1. Log into your switch management page (see "[Access your switch management page]" on page 9).

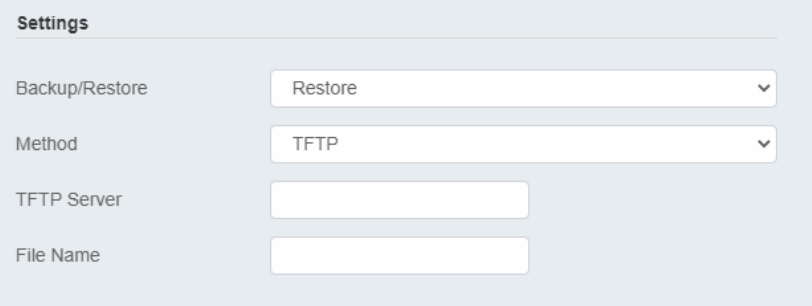
2. Click on **Tools**, click on **Firmware** and click on **Backup/Restore**.

3. Make sure your TFTP server is running and note the IP address of your server and configuration file name. The TFTP server should be in the same IP subnet as the switch.

Note: *It is recommended to put the configuration file (config.bin) is placed in your TFTP server root directory.*

4. Review the settings. Click **Restore** to restore the switch configuration file (config.bin) from your local hard drive from your TFTP server root directory.

- **Backup/Restore:** Select **Restore** to restore your configurations
- **Method:** Select **TFTP** as the method of restoring up your configuration
- **TFTP Server IP:** Enter the IP address of your TFTP server
- **TFTP Server IP:** Enter the IP address of your TFTP server.
- **Config File Name:** Enter the configuration file name to restore. (Default file extension: .cfg)



Settings

Backup/Restore: Restore

Method: TFTP

TFTP Server:

File Name:

5. Click **Apply** and wait for the switch to restore settings.

Diagnostics

Cable Diagnostics Test

Tools > Diagnostics

The switch provides a basic cable diagnostic tool in the GUI for verifying the pairs in copper cabling and estimated distance for troubleshooting purposes.

Note:

1. If the cable length displays N/A, it means that the cable length is Not Available. The may be due to the port being unable to determine the estimated cable length. If length is displayed as "N/A" it means the cable length is "Not Available". This is due to the port being unable to obtain cable length/either because its link speed is 10M or 100M, or the cables used are broken and/or of bad in quality.

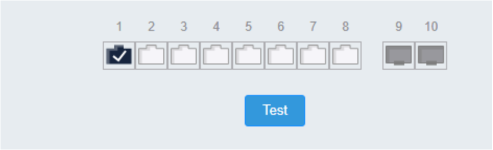
2. The deviation of "Cable Fault Distance" is +/- 2 meters. No cable may be displayed in the table when the cable is less than 2 meters in length.

3. The test also measures the cable fault and identifies the fault in length according to the distance from the switch.

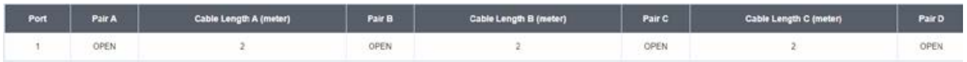
1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Tools** and click on **Cable Diagnostic**.

3. Select the **Port** from the switch to run the cable diagnostic and click **Test** to run the test.



The results will be displayed in the **Cable Diagnostic Table** below.



Port	Pair A	Cable Length A (meter)	Pair B	Cable Length B (meter)	Pair C	Cable Length C (meter)	Pair D
1	OPEN	2	OPEN	2	OPEN	2	OPEN

- **Test Results:** Displays the diagnostic results for each pair in the cable. One of the following cable status parameters is displayed:
  - **OK:** There is no problem detected with the cable.
  - **Open in Cable:** There is an open wire within the cable.
  - **Short in Cable:** Two wires are shorted together within the cable.
  - **Cross talk in Cable:** There is crosstalk detected between one pair
  - of wires and another pair within the cable.

Ping Test

Network Connectivity Test (Ping Tool)

Tools > Diagnostics > Ping Test

This chapter provides the procedure to ping a node on your network from the switch. This procedure is useful in determining whether an active link exists between the switch and another network device.

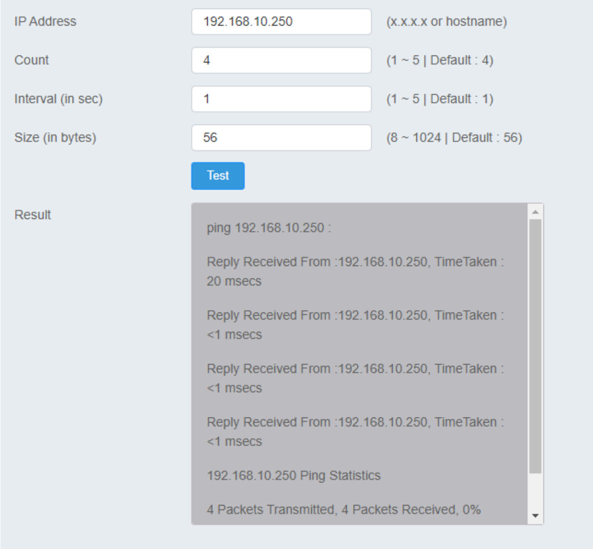
The device you are pinging must be a member of the Default VLAN and within the same local area network as your switch. In other words, the port on the switch through which the node is communicating with the switch must be an untagged or tagged member of the Default VLAN.

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Tools,** click on **Diagnostics,** and click on **Ping Test.**

3. Review the settings. Click **Start** to start the network connectivity ping test. After the ping test is activate, you can click **Show Ping Results** to check the ping test result.

- **IP Address** - The IP address of the node you want to ping in the IPv4 or IPv6 format.
- **Count** – Specifies the number of ping requests you want the switch to perform.
- **Interval –** Specifies the time between each ping request.
- **Size –** Specifies the size of the packet sent with each ping.



IP Address 192.168.10.250 (x.x.x.x or hostname)

Count 4 (1 ~ 5 | Default : 4)

Interval (in sec) 1 (1 ~ 5 | Default : 1)

Size (in bytes) 56 (8 ~ 1024 | Default : 56)

Result

```
ping 192.168.10.250 :

Reply Received From :192.168.10.250, TimeTaken :
20 msecs

Reply Received From :192.168.10.250, TimeTaken :
<1 msecs

Reply Received From :192.168.10.250, TimeTaken :
<1 msecs

Reply Received From :192.168.10.250, TimeTaken :
<1 msecs

192.168.10.250 Ping Statistics

4 Packets Transmitted, 4 Packets Received, 0%
```

IPv6 Ping Test

Network Connectivity Test (Ping Tool)

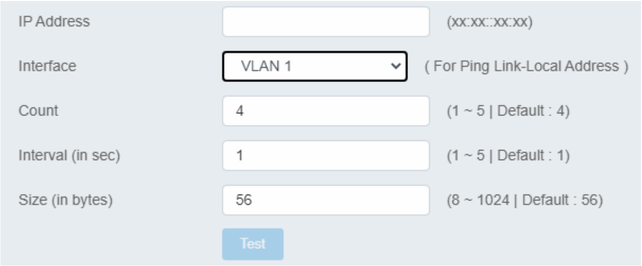
Tools > Diagnostics > IPv6 Ping Test

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Tools,** click on **Diagnostics,** and click on **IPv6 Ping Test.**

3. Review the settings. Click **Start** to start the network connectivity ping test. After the ping test is activate, you can click **Show Ping Results** to check the ping test result.

- **IP Address** - The IP address of the node you want to ping in the IPv6 format.
- **Interface** – Select the appropriate VLAN ID
- **Count** – Specifies the number of ping requests you want the switch to perform.
- **Interval –** Specifies the time between each ping request.
- **Size –** Specifies the size of the packet sent with each ping.



IP Address		(xx:xx::xx:xx)
Interface	VLAN 1	(For Ping Link-Local Address)
Count	4	(1 ~ 5 | Default : 4)
Interval (in sec)	1	(1 ~ 5 | Default : 1)
Size (in bytes)	56	(8 ~ 1024 | Default : 56)

Trace Route

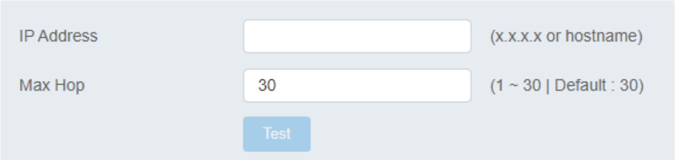
Tools > Diagnostics > Trace Route

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on **Tools,** click on **Diagnostics,** and click on **Trace Route.**

3. Review the settings. Click **Test** to start the Trace Route. After the test is completed, you can see the result below the test.

- **IP Address** - The IP address of the node you want to ping in the IPv6 format.
- **Max Hop** – Enter the maximum number of hops



IP Address		(x.x.x.x or hostname)
Max Hop	30	(1 ~ 30 | Default : 30)

Reboot

Reboot/Reset to factory defaults

Tools > Reboot

This section provides the procedures for rebooting or resetting the switch to factory default settings.

To reboot your switch:

You may want to reboot your switch if you are encountering difficulties with your switch and have attempted all other troubleshooting.

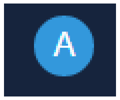
Note: *You may want to save the settings to flash before reboot the switch under Save Settings to Flash (menu) > Save Settings to Flash (button). If you have not saved your current configuration settings to flash first, the configuration changes will be lost after a reboot.*

There are two methods that can be used to reboot your switch.

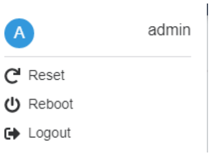
- **Hardware Method:** Using a paper clip, on the front panel of the switch, push and hold the **Reset** button between 1~5 seconds and release.
- **Software Method (Switch Management Page):**

1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on your profile in the top right corner.



3. Click **Reboot** drop-down list. Wait for the switch complete the rebooting process.



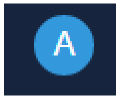
To reset your switch to factory defaults:

You may want to reset your switch to factory defaults if you are encountering difficulties with your switch and have attempted all other troubleshooting. Before you reset your switch to defaults, if possible, you should backup your switch configuration first, see "Backup/Restore" on page 88.

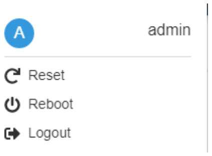
There are two methods that can be used to reset your switch to factory defaults.

- **Hardware Method:** Using a paper clip, on the front panel of the switch, push and hold the **Reset** button more than 6 seconds and release. Located on the front panel of your switch, see "Product Hardware Features" on page 2. Use this method if you are encountering difficulties with accessing your switch management page.
- **Software Method (Switch Management Page):**
- 1. Log into your switch management page (see "Access your switch management page" on page 9).

2. Click on your profile in the top right corner.



3. Click **Reset** from the drop-down list. Clicking **Reset,** will automatically reset the switch back to its factory default settings.



The switch's factory default settings are below.

Administrator User Name	admin
Administrator Password	admin
Switch IP Address	192.168.10.200
Switch Subnet Mask	255.255.255.0

Command Line Interface Reference

Access your switch command line interface

Note: *The system may be managed out-of-band through the console port. The console port is a female RJ-45 port and the included RJ-45 male to RS-232 serial DB-9 female console cable.*

1. Using the included RJ-45 to RS-232 serial DB-9 cable, connect the RJ-45 end to the switch console port and connect the RS-232 end to your computer RS-232 DB-9 male port.

m

2. On your computer, run the terminal emulation program (ex. HyperTerminal, TeraTerm, putty etc.).

3. Select the appropriate COM port used for connecting to the switch console.

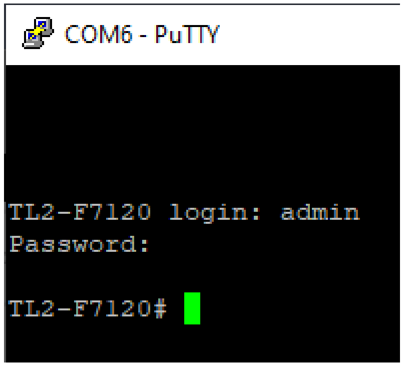
4. Use the following settings for the connection.

- Data Rate: 115200 bps
- Data Bit: 8 bits
- Parity: None
- Stop Bits: 1
- Flow Control: None
- Emulation mode: VT100

5. After you have setup all of the parameters appropriately, the terminal emulation window should display a prompt for user name and password.

Enter the user name and password. By default:

User Name: **admin**
Password: **admin**
Note: *User Name and Password are case sensitive.*



```
TL2-F7120 login: admin
Password:

TL2-F7120#
```

You can also use Telnet or SSH protocols to access the switch command line interface using IP address.

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

1 SWITCH CLI USER MANUAL

1 SYSTEM

4.1.1 help

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

4.1.2 clear screen

Command Objective	This command clears all the contents from the screen.

Syntax	clear screen
Mode	All Modes

4.1.1 end

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

4.1.2 logout

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

4.1.3 show privilege

Command Objective	Show current privilege level.
Syntax	show privilege

Mode	Privileged EXEC Mode

3 show cli

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

4.1.4 exit

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

5 configure terminal

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

4.1.6 listuser

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

4.1.7 show users

Command Objective	This command displays the information about the current user.

Syntax	show users

Mode	Privileged EXEC Mode

3 lock

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

4.1.9 show history

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

4.1.10 username

Command Objective	This command creates a user and sets the enable password for that user with the privilege level. The no form of the command deletes a user and disables the enable password for that user.
Syntax	username <user-name> [password <passwd>] [privilege <1-15>] no username < user-name >

Parameter Description	- <user-name> - Specifies the login user name to be created. - <passwd> - Specifies the password to be entered by the user to login to the system. The size password entered must be a minimum of 8 and maximum of 20 characters containing atleast one uppercase, one lowercase, one number and one special character. - privilege <1-15> - Applies restriction to the user for accessing the CLI commands. This values ranges between 1 and 15. For Example, a user ID configured with privilege level as four can access only the commands having privilege ID lesser than or equal to four.
Mode	Global Configuration Mode

4.1.1 set minimum password length

Command Objective	This command configures minimum password length. If the given password has less than the configured password length, it will not be allowed This value ranges between 8 and 20.

Syntax	set minimum password length <minimum-len>
Mode	Global Configuration Mode

4.1.2 line cli

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

4.1.3 exec-timeout

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

11 ping

Command Objective	This command sends echo messages. The Packet Internet Groper (Ping) module is built based on the ICMP echo request and ICMP echo response messages. The network administrator uses this ping on a remote device to verify its presence. Ping involves sending ICMP echo messages repeated and measuring the time between transmission and reception of message. The output displays the time taken for each packet to be transmitted, number of packets transmitted, number of packets received and packet loss percentage.
Syntax	ping [ip] {<ip_addr>|<string>} [count <integer(1-10)>] [size <integer(36-2080)>]
Parameter Description	• ip - Configures the IP address of the node to be pinged. • ipAddress - Configures the source IP address of the node to be pinged. • hostname - Configures the name of the host.

	• count - Configures the number of times the given node address is to be pinged. • size - Configures the size of the data portion of the PING PDU.
Mode	Privileged EXEC Mode

12 traceroute

Command Objective	This command traces route to the destination.
Syntax	traceroute {<ip_addr>|<string> | ipv6 <ip6_addr>} [max-ttl <short (2- 255)>]

Parameter Description	- <ip-address> - Configurest the destination IP address to which a route has to be traced. - <string> - Configurest the destination IP hostname to which a route has to be traced. - ipv6 <ip6_addr> - Configurest the destination IPv6 address to which a route has to be traced. - [max-ttl <short (2-255)>] -Configures the maximum value of the TTL field to be filled up in the IP packets used for the trace route.
Mode	Privileged EXEC Mode

4.1.13 clear counters

Command Objective	This command clears all the current interface counters from the interface unless the optional arguments type and number are specified to clear only a specific interface type (serial, Ethernet, Token Ring, and so on).

Syntax	clear counters [<interface-type> <interface-id>]
Parameter Description	• <interface-type>- Configures the specified type of interface. • <interface-id> - Configures the IP interface configuration for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1.
Mode	Privileged EXEC Mode

4.1.14 jumbo-frame

Command Objective	This command configures the maximum transmission unit frame size for all the frames transmitted and received on all the interfaces in a switch. The size of the jumbo frame size can be increased using this command. The value ranges between 1522 and 9216. The no form of this command sets the maximum transmission unit to the default value in all interfaces. 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.
Syntax	jumbo-frame <frame-size(1522-9216)>
Mode	Global Configuration Mode

4.1.15 interface range

Command Objective	This command selects the range of physical interfaces and VLAN interfaces to be configured. The no form of the command selects the range of VLAN interfaces to be removed.
Syntax	interface range ({ <interface-type> <slot/port-port>} {vlan <vlan- id(1-4094)> - <vlan-id(2-4094)>}) no interface range vlan <vlan-id(1-4094)> - <vlan-id(2-4094)>
Parameter Description	• <interface-type> - Selects the range of the specified interface. • <slot/port-port> - Selects the range of the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. • vlan <vlan-id(1-4094)> - <vlan-id(2-4094)> - Selects the range of the specified VLAN ID. This is a unique value that represents the specific VLAN created and activated. This value ranges between 1 and 4094.

Mode	Global Configuration Mode

4.1.1 configure

Command Objective	This command enters the configuration mode. Configuration from memory or network is not supported, when entered into the configuration mode using this command**.**
Syntax	configure
Mode	Privileged EXEC Mode

4.1.2 mac-address-table static unicast

Command Objective	This command configures a static unicast MAC address in the forwarding database. The no form of the command deletes a configured static Unicast MAC address from the forwarding database.
Syntax	mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id > interface ([<interface-type> <0/a-b, 0/c, ...>] [<interface-type> <0/a-b, 0/c, ...>] [port-channel <a,b,c-d>])
	no mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id >

Parameter Description	
	- <aa:aa:aa:aa:aa:aa> - Configures the static unicast destination MAC address. The received packets having the specified MAC address are processed. - vlan <vlan-id> - Configures the static unicast destination MAC address for the specified VLAN. This value ranges between 1 and 4094. ■ <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094 - interface - Configures the member ports interface type and ID. The details to be provided are: ■ <interface-type> - Configures the member ports for the specified type of interface. The interface can be: ◆ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. ◆ port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. ■ <0/a-b, 0/c, ...> - Configures the member ports for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. Port-channel ID is provided, for interface type port-channel. Use

	comma as a separator without space while configuring list of interfaces. Example: 0/1, 0/3 or 1, 3.

Mode	Global Configuration Mode

16 mac-address-table aging-time

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

Syntax	mac-address-table aging-time <10-630 seconds> no mac-address-table aging-time
Mode	Global Configuration Mode/ Switch Configuration Mode

4.1.17 set switch-name

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

18 set ip http

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

4.1.19 ip telnet service

Command Objective	This command enables the telnet service in the system. The no form of this command disables the telnet service.
Syntax	ip telnet service no ip telnet service
Mode	Global Configuration Mode

20 copy startup-config

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

Parameter 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
Mode	Privileged EXEC Mode

4.1.21 copy

Command Objective	This command copies the configuration from a remote site to flash.
Syntax	copy { tftp://ip-address/filename startup-config}

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

22 save

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

Syntax	save
Mode	Privileged EXEC Mode

4.1.23 copy logs

Command Objective	This command writes the system logs to a remote site.
Syntax	copy logs { tftp://ip-address/filename }

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

4.1.24 clock set

Command Objective	This command manages the system clock.
Syntax	clock set hh:mm:ss <day (1-31)> {january|february|march|april|may|june|july|august|september|october|november|december} <year (2000 - 2035)>

Parameter Description	- hh:mm:ss - Sets the current time. The format is hour, minutes and seconds. ■ <day (1-31)> - Sets the current day. It ranges between 1 and 31. ■ january - Sets the month as January. ■ february - Sets the month as February ■ march - Sets the month as march ■ april - Sets the month as april ■ may - Sets the month as may ■ june - Sets the month as June ■ july - Sets the month as July ■ august - Sets the month as August ■ september - Sets the month as September ■ october - Sets the month as October

	november - Sets the month as November ■ december - Sets the month as December ■ <year (2000 - 2035)> - Sets the year. It ranges between 2000 and 2035
Mode	Global Configuration Mode

4.1.25 show clock

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

4.1.26 show jumbo-frame

Command Objective	This command displays the maximum transmission unit frame size for all the frames transmitted and received on all the interfaces in a switch.
Syntax	show jumbo-frame
Mode	Privileged EXEC Mode

27 show system information

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

4.1.28 reboot

Command Objective	This command restarts the switch.
Syntax	reboot
Mode	Privileged EXEC Mode

4.1.29 restore-defaults

Command Objective	This command restore default configuration.
Syntax	restore-defaults

Mode	Privileged EXEC Mode

4.1.1 show telnet server

Command Objective	This command displays the telnet server status.
Syntax	show telnet server
Mode	Privileged EXEC Mode

4.1.2 show http server status

Command Objective	This command displays the http server status and HTTP port.
Syntax	show http server status
Mode	Privileged EXEC Mode

4.1.30 port speed - duplex

Command Objective	This command configures the speed and duplex operation.
Syntax	speed { 10 | 100 | 1000 | 10000 } duplex { full | half }

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

4.1.31 negotiation

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

32 port-isolation

Command Objective	This command set the status of the traffic to be allowed in these configured egress ports when the ingress is this interface.
Syntax	port-isolation {enable|disable}
Parameter Description	• enabled - Enables the Port Isolation rule in this ingress interface. • disabled - Disables the Port Isolation rule in this ingress interface.
Mode	Interface Configuration

4.1.33 show port-isolation status

Command Objective	This command displays the Port Isolation table.
Syntax	show port-isolation status

Mode	Privileged EXEC Mode

34 clock utc-offset

Command Objective	This command sets the system time zone with respect to UTC. The no form of command resets the system time zone to GMT.
Syntax	clock utc-offset <UTC-offset value as (+HH:MM /-HH:MM)(+00:00 to +14:00)/ (-00:00 to -12:00)> Eg: +05:30

Parameter Description	● +/- - Sets the client time zone as after or before UTC. Plus indicates forward time zone and minus indicates backward time zone. ● UTC- offset value as - Sets the UTC offset value in hours. - +00:00 to +14:00 - -00:00 to -12:00
Mode	Global Configuration Mode

4.1.35 show clock properties

Command Objective	This command displays the PTP clock properties.

Syntax	show clock properties
Mode	Privileged EXEC Mode

4.1.36 interface

Command Objective	This command allows to configure interface such as VLAN.

Syntax	interface {vlan < vlan-id > [switch <string(32)>] | port-channel <integer (1-8)> | <iftype> <ifnum>}
	no interface {vlan < vlan-id > [switch <string(32)>] | port-channel <integer (1-8)> | <iftype> <ifnum>}

Parameter **Description**	• vlan <vlan-id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094. • switch<switch-name>- Configures interface 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. This feature has been included to adhere to the Industry Standard CLI syntax. • port-channel<port-channel-id (1-8)>- Configures the port to be used by the host to configure the router. This value ranges between 1 and 8. The port channel identifier can be created or

	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 upto 1 Gigabit per second. ■ port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
Mode	Global Configuration Mode

4.1.37 ip address

Command Objective	This command sets the IP address for an interface.

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

4.1.38 ip address dhcp/bootp

Command Objective	This command sets the DHCP/BOOTP IP address for an interface.
Syntax	ip address dhcp ip address bootp no ip address
Parameter Description	• dhcp – Get IP by using DHCP protocol. • botp – Get IP by using BOOTP protocol.
Mode	Interface Configuration Mode

4.1.1 shutdown

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

4.1.2 description

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

4.1.39 show interface port-security

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

4.1.40 show interface cable-diag

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

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

41 show ip interface

Command Objective	This command displays the IP interface configuration.
Syntax	show ip interface [{[Vlan <vlan-id(1-4094)> | [<interface-type><interface-id>]
Parameter Description	• 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 upto 1 Gigabit per second.

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

Mode	Privileged EXEC Mode

4.1.42 show flow-control

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

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

4.1.43 snmp trap link-status

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

4.1.44 flowcontrol

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

45 port-security

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

4.1.46 show security-suite

Command Objective	Displays Dos information.

Syntax	show security-suite

2 ACL

47 ip access-list extend

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

4.1.48 mac access-list extend

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

4.1.49 ipv6 access-list extend

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

4.1.50 permit- ip/ospf/pim/protocol type

Command Objective	This command allows traffic for a particular protocol packet if the conditions defined in the permit statement are matched.
Syntax	permit { ip | ospf | pim | <short (1-255)>} { any| host <src-ip-address>|<src-ip-address> <mask>} { any|host <dest-ip-address>|<dest-ip-address> <mask> } ace-priority <integer (1-2147483647)> [dscp <short (0-63)>]

Parameter Description	• ip| ospf|pim|<protocol-type (1-255)> - Type of protocol for the packet. It can also be a protocol number. • any| host <src-ip-address>|<src-ip-address> <mask> - Source IP address can be ■ 'any' or ■ the dotted decimal address or ■ the IP Address of the network or the host that the packet is from and the network mask to use with the source address. • any|host <dest-ip-address>|<dest-ip-address> <mask> - Destination IP address can be ■ 'any' or ■ the dotted decimal address or ■ the IP Address of the network or the host that the packet is destined for and the network mask to use with the destination address • ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. • dscp <short (0-63)> - Differentiated services code point provides the quality of service control.
Mode	IPV4 ACL Extended Access List Configuration Mode

4.1.51 deny- ip/ospf/pim/protocol type

Command Objective	This command denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched.
Syntax	deny { ip | ospf | pim | <short (1-255)>} { any| host <src-ip-address>|<src-ip-address> <mask> } { any|host <dest-ip-address>|<dest-ip-address> <mask> } ace-priority <integer (1-2147483647)> [dscp <short (0-63)>]

Parameter Description

- ip| ospf|pim|<protocol-type (1-255)> - Type of protocol for the packet. It can also be a protocol number.
- any| host <src-ip-address>|<src-ip-address> <mask> - Source IP address can be
  - 'any' or
  - the dotted decimal address or
  - the IP Address of the network or the host that the packet is from and the network mask to use with the source address.
- any|host <dest-ip-address>|<dest-ip-address> <mask> - Destination IP address can be
  - 'any' or
  - the dotted decimal address or
  - the IP Address of the network or the host that the packet is destined for and the network mask to use with the destination address
- ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules.

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

Mode IPV4 ACL Extended Access List Configuration Mode

4.1.52 permit tcp

Command Objective	This command specifies the TCP packets to be forwarded based on the associated parameters.
Syntax	permit tcp { any| host <src-ip-address>|<src-ip-address> <mask>} [eq <short (1-65535)>] { any|host <dest-ip-address>|<dest-ip-address> <mask> } [eq <short (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 <short (0-63)>]

Parameter **Description**	• tcp - Transport Control 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. • eq <short (1-65535)> - Port Number. • 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.
- ack | non_ack - TCP ACK bit to be checked against the packet.
- rst | non_rst - TCP RST bit to be checked against the packet.
- psh | non_psh - TCP PSH bit to be checked against the packet.
- urg | non_urg - TCP URG bit to be checked against the packet.
- syn | non_syn - TCP SYN bit to be checked against the packet.
- fin | non_fin - TCP FIN bit to be checked against the packet.
- dscp <short (0-63)> - Differentiated services code point provides the quality of service control.

Mode	IPV4 ACL Extended Access List Configuration Mode

53 deny tcp

Command Objective	This command specifies the TCP packets to be rejected based on the associated parameters.
Syntax	deny tcp { any| host <src-ip-address>|<src-ip-address> <mask>} [eq <short (1-65535)>] { any|host <dest-ip-address>|<dest-ip-address> <mask> } [eq <short (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 <short (0-63)>]
Parameter	- tcp - Transport Control Protocol.

Description

- 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.
- eq <short (1-65535)> - Port Number.
- 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.
- ack | non_ack - TCP ACK bit to be checked against the packet.
- rst | non_rst - TCP RST bit to be checked against the packet.
- psh | non_psh - TCP PSH bit to be checked against the packet.
- urg | non_urg - TCP URG bit to be checked against the packet.
- syn | non_syn - TCP SYN bit to be checked against the packet.
- fin | non_fin - TCP FIN bit to be checked against the packet.
- dscp <short (0-63)> - Differentiated services code point provides the quality of service control.

Mode	IPV4 ACL Extended Access List Configuration Mode

54 permit udp

Command Objective	This command specifies the UDP packets to be forwarded based on the associated parameters.
Syntax	permit udp { any| host <src-ip-address>|<src-ip-address> <mask> } [eq <short (1-65535)>] { any|host <dest-ip-address>|<dest-ip-address> <mask> } [eq <short (1-65535)>] ace-priority <integer (1-2147483647)> [dscp <short (0-63)>]

Parameter Description

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

Mode IPV4 ACL Extended Access List Configuration Mode

55 deny udp

Command Objective	This command specifies the UDP packets to be rejected based on the associated parameters.
Syntax	deny udp { any| host <src-ip-address>|<src-ip-address> <mask> } [eq <short (1-65535)>] { any|host <dest-ip-address>|<dest-ip-address> <mask> } [eq <short (1-65535)>] ace-priority <integer (1-2147483647)> [dscp <short (0-63)>]

<table>
<tr><td><b>Parameter</b>
<b>Description</b></td><td>• udp - User Datagram 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.
• eq <short (1-65535)> - Port Number.
• 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.</td></tr>
<tr><td></td><td>• dscp &lt;short (0-63)> - Differentiated services code point provides the quality of service control.</td></tr>
<tr><td><b>Mode</b></td><td>IPV4 ACL Extended Access List Configuration Mode</td></tr>
</table>

56 permit icmp

Command Objective	This command specifies the ICMP packets to be forwarded based on the IP address and the associated parameters.
Syntax	permit icmp { any| host <src-ip-address>|<src-ip-address> <mask>} { any|host <dest-ip-address>|<dest-ip-address> <mask> } [type <short (0-255)>] [code <short (0-255)>] ace-priority <integer (1-2147483647)> [dscp <integer (0-63)>]

Parameter **Description**	• icmp - Internet Control Message Protocol. • any| host <src-ip-address>|<src-ip-address> <mask> - Source IP address can be ■ 'any' or ■ the dotted decimal address or ■ the IP Address of the network or the host that the packet is from and the network mask to use with the source address. • any|host <dest-ip-address>|<dest-ip-address> <mask> - Destination IP address can be ■ 'any' or ■ the dotted decimal address or ■ the IP Address of the network or the host that the packet is destined for and the network mask to use with the destination address

	• type <short (0-255)> - message type • code <short (0-255)> - message code • ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. • dscp <short (0-63)> - Differentiated services code point provides the quality of service control.
Mode	IPV4 ACL Extended Access List Configuration Mode

4.1.57 deny icmp

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

Syntax	deny icmp { any| host <src-ip-address>|<src-ip-address> <mask>} { any|host <dest-ip-address>|<dest-ip-address> <mask> } [type <short (0-255)>] [code <short (0-255)>] ace-priority <integer (1-2147483647)> [dscp <integer (0-63)>]
Parameter Description	• icmp - Internet Control Message Protocol. • any| host <src-ip-address>|<src-ip-address> <mask> - Source IP address can be ■ 'any' or ■ the dotted decimal address or ■ the IP Address of the network or the host that the packet is from and the network mask to use with the source address. • any|host <dest-ip-address>|<dest-ip-address> <mask> - Destination IP address can be

	■ 'any' or ■ the dotted decimal address or ■ the IP Address of the network or the host that the packet is destined for and the network mask to use with the destination address • type <short (0-255)> - message type • code <short (0-255)> - message code • ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. • dscp <short (0-63)> - Differentiated services code point provides the quality of service control.
Mode	IPV4 ACL Extended Access List Configuration Mode

58 no ace-priority

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

4.1.59 permit ipv6

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

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

4.1.60 deny ipv6

Command Objective	This command specifies IPv6 packets to be forwarded based on protocol and associated parameters.
Syntax	deny ipv6 {any | host <ip6_addr> <integer(0-128)> } { any | host <ip6_addr> <integer(0-128)> } ace-priority <integer (1-2147483647)> [dscp <short(0-63)>]
Parameter Description	• ipv6 – Ipv6 protocol. • any | host <ip6_addr> <integer(0-128)> - Source address of the host / any host. • any | host <ip6_addr> <integer(0-128)> - Destination address of the host / any host. • ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. • dscp <short (0-63)> - Differentiated services code point provides the quality of service control.

Mode	IPV6 ACL Extended Access List Configuration Mode

4.1.61 permit tcp

Command Objective	This command specifies the IPv6 TCP packets to be forwarded based on the associated parameters.
Syntax	• permit tcp {any | host <ip6_addr> <short(0-128)>}[eq <short (1-65535)>] {any | host <ip6_addr> <short(0-128)>} [eq <short (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 <short (0-63)>]

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

62 deny tcp

Command Objective	This command specifies the IPv6 TCP packets to be forwarded based on the associated parameters.
Syntax	- deny tcp {any | host <ip6_addr> <short(0-128)>}[eq <short (1-65535)>] {any | host <ip6_addr> <short(0-128)>} [eq <short (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 <short (0-63)>]

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

4.1.63 permit udp

Command Objective	This command specifies the IPv6 TCP packets to be forwarded based on the associated parameters.
Syntax	• permit udp {any | host <ip6_addr> <short(0-128)>} [eq <short (1-65535)>] {any | host <ip6_addr> <short(0-128)>} [eq <short (1-65535)>] ace-priority <integer (1-2147483647)> [dscp <short (0-63)>]

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

4.1.64 deny udp

Command Objective	This command specifies the IPv6 TCP packets to be forwarded based on the associated parameters.
Syntax	- deny udp {any | host <ip6_addr> <short(0-128)>} [eq <short (1-65535)>] {any | host <ip6_addr> <short(0-128)>} [eq <short (1-65535)>] ace-priority <integer (1-2147483647)> [dscp <short (0-63)>]
Parameter Description	- udp - User Datagram Protocol. - any | host <ip6_addr> <integer(0-128)> - Source address of the host / any host - eq <short (1-65535)> - Port Number.
	- any | host <ip6_addr> <integer(0-128)> - Destination address of the host / any host. - ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. - dscp <short (0-63)> - Differentiated services code point provides the quality of service control.
Mode	IPV6 ACL Extended Access List Configuration Mode

65 permit icmpv6

Command Objective	This command specifies the IPv6 TCP packets to be forwarded based on the associated parameters.
Syntax	- permit icmpv6 {any | host <ip6_addr> <integer(0-128)>} {any | host <ip6_addr> <integer(0-128)>} ace-priority <integer (1- 2147483647)> [type <short(0-255)>] [code <short(0-255)>][dscp <short(0-63)>]

Parameter Description	• icmpv6 - Internet Control Message 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. • type <short (0-255)> - message type • code <short (0-255)> - message code • dscp <short (0-63)> - Differentiated services code point provides the quality of service control.
Mode	IPV6 ACL Extended Access List Configuration Mode

66 deny icmpv6

Command Objective	This command specifies the IPv6 TCP packets to be forwarded based on the associated parameters.
Syntax	• deny icmpv6 {any | host <ip6_addr> <integer(0-128)>} {any | host <ip6_addr> <integer(0-128)>} ace-priority <integer (1- 2147483647)> [type <short(0-255)>] [code <short(0-255)>] [dscp <short(0-63)>]
Parameter Description	• icmpv6 - Internet Control Message 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. • type <short (0-255)> - message type • code <short (0-255)> - message code • dscp <short (0-63)> - Differentiated services code point provides the quality of service control.

Mode	IPV6 ACL Extended Access List Configuration Mode

67 no ace-priority

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

4.1.68 permit mac

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

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

4.1.69 deny mac

Command Objective	This command specifies the packets to be rejected based on the MAC address and the associated parameters.
Syntax	- deny { any | <src-mac-address > } { any | host <mac_addr> } {ace-priority <integer (1-2147483647)>} [ethertype <integer (1- 65535)>] [vlan <integer (1-4094)>] [vlan-priority <short (0-7)>]
Parameter Description	- any | host <src-mac-address > - Source MAC address to be matched with the packet - any | host <dest-mac-address > - Destination MAC address to be matched with the packet - ace-priority <integer (1-2147483647)> - The priority of the filter is used to decide which filter rule is applicable when the packet matches with more than one filter rules. - ethertype <integer (1-65535)> - Specifies the non-IP protocol type to be filtered. - vlan <integer (1-4094)> - VLAN value to match against incoming packets. - vlan-priority <short (0-7)> - VLAN priority value to match against incoming packets.

Mode	MAC ACL Extended Access List Configuration Mode

4.1.70 no ace-priority

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

71 ip access-group

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

4.1.72 ipv6 access-group

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

73 mac access-group

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

4.1.74 show access-lists

Command Objective	This command displays the access lists configuration.
Syntax	show access-lists [{ip | mac | ipv6 } [<string(31)>]]
Parameter Description	- ip - IP Access List - mac – MAC Access List - ipv6 – Ipv6 Access List - <string(31)> - Name of access list
Mode	Privilege EXEC Mode

3 . DHCP SERVER

75 service dhcp-server relay

Command Objective	This command enables the DHCP relay A DHCP relay agent is any host or IP router that forwards DHCP packets between clients and servers.
✏	The DHCP server relay can be config in the switch.
Syntax	service dhcp-relaydh no service dhcp-server
Mode	Global Configuration Mode

4 . DNS

4.1.76 domain name-server

Command Objective	This command configures the IP address for the domain name server. The no form of the command disables the IP address configured for the domain name server.
Syntax	domain name-server ipv4 <ucast_addr>
	no domain name-server ipv4 <ucast_addr>
Parameter Description	• ipv4 <ucast_addr> - Sets the IP address for the domain name server in IPv4 address format.
Mode	Global Configuration Mode

4.1.77 show ip dns name-server

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

5 . EEE

4.1.91 eee

Command Objective	This command enables/disables Energy Efficient Ethernet on the specified port . The no form of the command disable Energy Efficient Ethernet on the specified port.

Syntax	eee no eee
Mode	Interface Configuration Mode

4.1.92 show eee

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

6 . IGMP

4.1.93 shutdown snooping

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

4.1.94 snooping multicast-forwarding-mode

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

4.1.95 ip igmp snooping

Command Objective	This command enables IGMP snooping in the switch/ a specific VLAN. When snooping is enabled in a switch or interface, it learns the hosts intention to listen to a specific multicast address. When the switch receives any packet from the specified multicast address, it forwards the packet to the host listening for that address. Broadcasting is avoided to save bandwidth. When IGMP snooping is enabled globally, it is enabled in all the existing VLAN interfaces. The no form of the command disables IGMP snooping in the switch/a specific VLAN. When IGMP snooping is disabled globally, it is disabled in all the existing VLAN interfaces.

Syntax	Global Configuration Mode ip igmp snooping [vlan < vlan–id >] no ip igmp snooping [vlan < vlan–id >] Config-VLAN Mode
	ip igmp snooping no ip igmp snooping
Parameter Description	- <vlan –id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094.
Mode	Global Configuration Mode / Config-VLAN Mode

Example

```
switch(config)# ip igmp snooping switch

(config)# vlan 1

switch (config-vlan)# ip igmp snooping switch

(config-vlan)# exit

switch (config)# exit

switch # show ip igmp snooping globals


Snooping Configuration

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

IGMP Snooping globally enabled

IGMP Snooping is operationally enabled IGMP

Snooping Enhanced mode is disabled IGMP Snooping

Sparse mode is disabled

Transmit Query on Topology Change                globally disabled

Multicast forwarding mode is MAC based

Proxy globally disabled

Proxy reporting globally disabled
```

```
Filter is disabled

Router port purge interval is 125 seconds Port purge interval is 260 seconds  Report forward

interval is 19 seconds

Group specific query interval is 2 seconds Reports are forwarded on router ports Queries are

forwarded on non-router ports Group specific query retry count is 2 Multicast VLAN disabled

Leave config level is Vlan based

Report processing config level is on non-router ports switch #

switch # show ip igmp snooping vlan 1



Snooping VLAN Configuration for the VLAN 1 IGMP Snooping enabled

  IGMP configured version is V2 Fast leave is enabled

  Snooping switch is configured as Non-Querier Snooping switch is acting as Non-Querier Startup

  Query Count is 2

  Startup Query Interval is 15 seconds Query interval is 125 seconds

  Other Querier Present Interval is 256 seconds
```

```
Port Purge Interval is 262 seconds

Max Response Code is 120, Time is 12 seconds
```

4.1.96 ip igmp querier-timeout

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

4.1.97 ip igmp snooping vlan - immediate leave

Command Objective	This command enables fast leave processing and IGMP snooping for a specific VLAN, It enables IGMP snooping only for the specific VLAN, when IGMP snooping is globally disabled. When the fast leave feature is enabled, port information is removed from a multicast group entry immediately after fast leave message is received. The ID of the VLAN ranges between 1 and 4094. The no form of the command disables fast leave processing for a specific VLAN. This command is a standardized implementation of the existing command; ip igmp snooping fast-leave. It operates similar to the existing command.

	Fast leave configurations done in a VLAN when IGMP snooping is disabled in a VLAN, will be applied only when IGMP snooping is enabled in the VLAN.
Syntax	ip igmp snooping vlan <vlanid(1-4094)> immediate-leave no ip igmp snooping vlan <vlanid(1-4094)> immediate-leave
Mode	Global Configuration Mode

4.1.91 ip igmp snooping report-suppression interval

Command Objective	This command sets the IGMP snooping report-suppression time interval. The switch forwards IGMPv2 report message to the multicast group. A timer is started immediately after forwarding the report message and runs for set period of time. During this interval the switch does not forward another IGMPv2 report message addressed to the same multicast group to the router ports.
	The no form of the command sets the IGMP snooping report-suppression interval time to the default value.
✎	The ip igmp snooping report-suppression-interval is used only when the proxy and proxy-reporting are disabled.
Syntax	ip igmp snooping report-suppression-interval <(1 – 25) seconds> no ip igmp snooping report-suppression-interval
Mode	Global Configuration Mode

4.1.91 ip igmp snooping group-query-interval

Command Objective	This command sets the time interval after which the switch sends a group specific query to find out if there are any interested receivers in the group when it receives a leave message. If it does not receive a response from the group, the port is removed from the group membership information in the forwarding database. This value ranges between 2 and 5. The no form of the commands sets the group specific query interval time to default value.

Command Objective	This command sets the time interval after which the switch sends a group specific query to find out if there are any interested receivers in the group when it receives a leave message. If it does not receive a response from the group, the port is removed from the group membership information in the forwarding database. This value ranges between 2 and 5. The no form of the commands sets the group specific query interval time to default value.
Syntax	ip igmp snooping group-query-interval <2-5) seconds>
	no ip igmp snooping group-query-interval
Mode	Global Configuration Mode

4.1.91 ip igmp snooping querier

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

4.1.92 ip igmp snooping query-interval

Command Objective	This command sets the time period with which the general queries are sent by the IGMP snooping switch when configured as querier on a VLAN. The value range is between 60 to 600 seconds.

	The no form of the command sets the IGMP querier interval to default value.
✎	The switch must be configured as a querier for this configuration to be imposed.
Syntax	ip igmp snooping query-interval <(60 - 600) seconds> no ip igmp snooping query-interval
Mode	Config-VLAN Mode

4.1.98 show ip igmp snooping statistics

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

4.1.99 show ip igmp snooping multicast-vlan

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

7 . IP SETTING

4.1.100 ip route

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

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

4.1.101 show ip route

Command Objective	This command displays the IP routing table.

Syntax	show ip route [{ <ip_addr> [<ip_mask>] | connected | static | summary | details}]
Parameter Description	- <ip-address>- Displays the IP routing table for the specified destination IP Address. - <mask>- Displays the IP routing table for the specified prefix mask address. - connected- Displays the Directly Connected Network Routes. - static- Displays the Static Routes in the table. - summary- Displays the Summary of all routes. - details-Displays the details of all routes.
Mode	Privileged EXEC Mode

4.1.102 arp

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

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

Parameter Description	• <ip-address>- Configures the IP Address of ARP Entry. • <macaddr> - The MAC address corresponding to the IP address above. • <vlan –id>- VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094.
Mode	Global Configuration Mode

4.1.103 arp timeout

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

4.1.104 show ip arp

Command Objective	This command displays IP ARP table.
Syntax	show ip arp [{ Vlan <vlan_id> | <iftype> <ifnum> | <ipiftype> <ifnum> | <ucast_addr> | <ucast_mac> | summary | information | statistics }]

Parameter Description	• Vlan <vlan-id>- VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094. • <interface-type> - Displays specified type of interface. • <ipiftype> - Displays the IP ARP information for the specified L3 Psuedo wire interface in the system. • <ip-address> - Displays the IP Address of ARP Entry. • <mac-address> - 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.
Mode	Privileged EXEC Mode

3 . IPV6

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

4.1.105 ipv6 unicast-routing

Command Objective	This command enables unicast routing which is used for one to one communication across the ipv6 internet. An IPv6 unicast address is an identifier for a single interface, on a single node. A packet that is sent to a unicast address is delivered to the interface identified by that address.
Syntax	ipv6 unicast-routing no ipv6 unicast-routing
Mode	Interface Configuration Mode

4.1.106 ipv6 enable

Command Objective	This command enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.

Syntax	ipv6 enable no ipv6 enable
Mode	Interface Configuration Mode

4.1.107 ipv6 address - prefix and prefix length

Command Objective	This command configures IPv6 address on the interface.
Syntax	ipv6 address <prefix> <prefix Len> [unicast] no ipv6 address <prefix> <prefix Len> [unicast]

Parameter **Description**	• <prefix>-Configures the IPv6 prefix for the interface.
	• <prefix Len> - Configures the number of high-order bits in the IPv6 address. These bits are common among all hosts within a network. This value ranges between 0 and 128. • unicast- Configures the address type of the prefix as Unicast.
Mode	Interface Configuration Mode

4.1.108 ipv6 address - link local

Command Objective	This command configures the IPv6 link-local address on the interface. The link-local address is an IP address that is intended only for communications within the segment of a local network (a link) or a point-to-point connection.
Syntax	ipv6 address <prefix> link-local no ipv6 address <prefix> link-local
Parameter Description	• <prefix>-Configures the IPv6 prefix for the interface.
Mode	Interface Configuration Mode

4.1.109 show ipv6 interface

Command Objective	This command displays the IPv6 interfaces.
Syntax	show ipv6 interface [{vlan <vlan-id> [prefix]}]

Parameter Description	• <vlan –id>- VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094.
Mode	Privileged EXEC Mode

4.1.110 show ipv6 route

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

4.1.111 show ipv6 route - summary

Command Objective	This command displays the summary of IPv6 Routes.

Syntax	show ipv6 route summary
Mode	Privileged EXEC Mode

4.1.112 show ipv6 neighbors

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

4.1.113 ping ipv6

Command Objective	This command sends IPv6 echo messages along with the total number of packets to the destination.
Syntax	ping ipv6 <prefix%interface> [repeat <count>] [size <value>] [source {vlan <vlan-id> | <source_prefix>}] [timeout <value (1-100)>]

Parameter Description	• <prefix%interface>- Configures the IPv6 Destination Prefix. • repeat<count>- Configures the number of ping messages. The range varies between 0 and 10.
	• size<value> - Configures the size of the data portion of the Ping packet in the message. • source- Configures the Source Interface of the ping message. • vlan <vlan-id> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094. • <source_prefix>- Configures source prefix of the ping message. • timeout <value (1-100)>- Configures the time in seconds after which this entity times out waiting for a particular ping response. The value ranges between 1 to 100.
Mode	Privileged EXEC Mode

9 . LAG

Command Objective	This command configures the LACP priority associated with actor's system ID. This priority value ranges between 0 and 65535. The switch with the lowest LACP decides the standby and active links in the LA. The no form of the command resets the LACP priority to its default value.
Syntax	lacp system-priority <0-65535> no lacp system-priority
Mode	Global Configuration Mode

4.1.114 port-channel load-balance

Command Objective	This command configures the load balancing policy for all port channels created in the switch. The policy sets the rule for distributing the Ethernet traffic among the aggregated links to establish load balancing.
Syntax	port-channel load-balance ([src-mac][dest-mac][src-dest-mac][src-ip][dest-ip][src-dest-ip][dest-l4-port][src-l4-port])

Parameter **Description**	• src-mac - Distributes the load based on the source MAC address. The bits of the source MAC address in the packet are used to select the port in which the traffic should flow. Packets from different hosts use different ports in the channel, but packets from the same host use the same port. • dest-mac - Distributes the load based on the destination host MAC address. The bits of the destination MAC address in the packet are used to select the port in which the traffic should flow. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel • src-dest-mac - Distributes the load based on the source and destination MAC address. The bits of the source and destination MAC address in the packet are used to select the port in which the traffic should flow. • src-ip - Distributes the load based on the source IP address. The bits of the source IP address in the packet are used to select the port in which the traffic should flow. • dest-ip - Distributes the load based on the destination IP address. The bits of the destination IP address in the packet are used to select the port in which the traffic should flow. • src-dest-ip - Distributes the load based on the source and destination IP address. The bits of the source and destination IP address in the packet are used to select the port in which the traffic should flow. • dest-l4-port - Distributes the load based on the destination Layer

4 port. The bits of the destination Layer 4 port in the packet are used to select the port in which the traffic should flow.

- src-l4-port - Distributes the load based on the source Layer 4 port. The bits of the source Layer 4 port in the packet are used to select the port in which the traffic should flow.

Mode	Global Configuration Mode

4.1.115 channel-group

Command Objective	This command adds the port as a member of the specified port channel that is already created in the switch. The no form of the command deletes the aggregation of the port from all port channels.
Syntax	channel-group <channel-group-number(1-8)> Mode { on | active | passive } no channel-group

Parameter Description	• <channel-group-number(1-8)> - Adds the port as a member of the specified port channel. This is a unique value that represents the specific port-channel created. This value ranges from 1 to 8. • Mode - Configures the LACP activity for the port: - active - Starts LACP negotiation un-conditionally. - passive - Starts LACP negotiation only when LACP packet is received from peer. - on - Forces the interface to channel without LACP. This is equivalent to manual aggregation.
Mode	Interface Configuration Mode (Physical Interface Mode)

4.1.116 lacp timeout

Command Objective	This command configures the LACP timeout period within which LACPDUs should be received on a port to avoid timing out of the aggregated link. The no form of the command sets the LACP timeout period to its default value.

Syntax	lacp timeout {long | short } no lacp timeout
Parameter Description	- long - Configures the LACP timeout period as 90 seconds. The LACP PDU is sent every 30 seconds. - short - Configures the LACP timeout period as 3 seconds. The LACP PDU is sent every second.
Mode	Interface Configuration Mode (Physical Interface Mode)

4.1.117 show etherchannel

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

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

Parameter Description	- channel-group-number - Displays Etherchannel information for the specified port-channel group. This is a unique value that represents the specific port-channel created. This value ranges from 1 to 8. - detail - Displays detailed Etherchannel information. The information contain 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 groups. - port - Displays the status of protocol operate Mode and port details for each group. The port details contain port state, group to which the port belongs, port Mode, aggregation state, port- channel ID, pseudo port-channel ID, admin key, oper key, port number, port state, and LACP port-priority, wait-time, port identifier, activity and timeout. - port-channel - Displays the admin and oper status of port channel module, and port channel details. The port channel details contain port channel ID, number of member ports, ID of hot standby port, port state, status of protocol operate Mode, aggregator MAC and default port ID.

- summary - Displays the admin and oper status of port channel module, number of channel groups used, number of aggregators,

	group IDs, and port channel ID, status of protocol operate Mode and member ports for each group. - protocol - Displays the status of protocol operate Mode for each port-channel group.
Mode	Privileged EXEC Mode

10 . LBD

4.1.118 lbd

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

4.1.119 show lbd state

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

4.1.120 show lbd state

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

Mode	Privileged EXEC Mode

11 . LLDP

4.1.121 set lldp

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

no lldp transmit-interval

Mode	Global Configuration Mode

4.1.91 lldp holdtime-multiplier

Command Objective	This command sets the holdtime-multiplier value, which is the amount of time, the server should hold the LLDP. The value ranges between 2 and 10 seconds. The no form of the command sets the multiplier to the default value.

TLV (Time to Live) A value that tells the receiving agent, how long the information contained in the TLV Value field is valid.

TTL = message transmission interval * hold time multiplier.

For Example, if the value of LLDP transmission interval is 30, and the value of the LLDP hold multiplier is 4, then the value 120 is encoded in the TTL field in the LLDP header.

Syntax

```
lldp holdtime-multiplier <value(2-10)>

no lldp holdtime-multiplier
```

Mode

Global Configuration Mode

4.1.91 lldp reinitialization-delay

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

4.1.92 lldp tx-delay

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

4.1.92 lldp transmit-interval

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

show lldp

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

4.1.122 show lldp interface

Command Objective	This command displays the information about interfaces where LLDP is enabled.
Syntax	show lldp interface [<interface-type> <interface-id>] [mac-address <mac_addr>]

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

4.1.123 show lldp neighbors

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

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

Parameter Description	• chassis-id <string(255)> - Configures the chassis identifier string. This value is a string value with a maximum size of 255. • port-id <string(255)> - Configures the port number that represents the concerned aggregation port This value is a string value with a maximum size of 255. • <interface-type> - Displays information about neighbors for the specified type of interface. The interface can be: ■ gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • <interface-id> - Displays information about neighbors for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface type port-channel. For Example: 1 represents port-channel ID. • mac-address <mac_addr> - Displays information about neighbors for the specidfied destination MAC address of the LLDP agent. • detail - Displays the information obtained from all the received TLVs .
Mode	Privileged EXEC Mode

4.1.124 show lldp local

Command Objective	This command displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces.
Syntax	show lldp local {[<interface-type> <interface-id> [macaddress <mac_addr>]] | [mgmt-addr]}

Parameter Description	• <interface-type> - Displays the current switch information for the specified type of interface. The interface can be: ■ gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. • <interface-id> - Displays the current switch information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1. Only port-channel ID is provided, for interface type port-channel. For Example: 1 represents port-channel ID. • mac-address <mac_addr> - Displays information about neighbors for the specidfied destination MAC address of the LLDP agent. • mgmt-addr - All the management addresses configured in the system and Tx enabled ports.
Mode	Privileged EXEC Mode

12 . MIRROR

4.1.125 monitor session - destination

Command Objective	This command configures a destination port for a mirroring session. The no form of the command removes the destination port configuration of the mirroring session.
Syntax	monitor session <session-id (1-3)> destination { interface <interface- type> <interface-id>} [allow-ingress] no monitor session <session-id (1-3)> destination { interface <interface- type> <interface-id>}
Parameter Description	• session-id - Specifies the index of the mirroring session. This value ranges between 1 and 3. • interface - Specifies the destination port for the mirroring session. ■ <interface-type> - Interface type. This can be: GigabitEthernet or or Port Channel. ■ <interface-id> – Interface identifier. This is a combination of slot number and port number. • allow-ingress- Allow Packets Ingress to Destination Port.
Mode	Global Configuration Mode

4.1.126 monitor session - source

Command Objective	This command configures a source port / remote VLAN for a mirroring session. The no form of the command removes the source port / remote VLAN configuration of the mirroring session.
Syntax	monitor session <session-id (1-3)> { source { interface <interface-type> <interface-id> [{ rx | tx | both }] }}} no monitor session <session-id (1-3)> { source { interface <interface- type> <interface-id> [{rx|tx|both}]

Parameter Description	• session-id - Configures the session number that is used to identify a session. • interface - Configures the source interface whose traffic to be mirrored. The details to be provided are: ■ <interface-type> - Sets the type of interface. The interface can be: ◆ gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. ■ <interface-id> - Sets the interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. • rx - Mirrors received traffic • tx - Mirrors transmitted traffic • both - Specifies the traffic direction to monitor. If the traffic direction is not specified, both transmitted and received traffic is mirrored.
Mode	Global Configuration Mode

4.1.127 no monitor session

Command Objective	This command is used to remove the mirroring configuration.
Syntax	no monitor session { session-range | session-id}
Parameter Description	- session-range - Specifies the list of session for which mirroring configuration should be removed - session-id - Specifies the index of the mirroring session.
Mode	Global Configuration Mode

4.1.128 show monitor

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

13 MLD

4.1.129 ipv6 mld snooping

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

4.1.91 ipv6 mld snooping report-suppression-interval

Command Objective	This command sets the MLD snooping report-suppression interval for which MLDv1 report messages do not get forwarded onto the router ports for the same group. This value ranges is between 1 and 25. This timer is used when both proxy and proxy-reporting are disabled. This timer is started as soon as a report message for that group is forwarded out. Within this interval if another report for the same group arrives, it will not be forwarded. The no form of this command sets the MLD snooping report-suppression interval to its default value.
Syntax	ipv6 mld snooping report-suppression-interval (1-25) seconds> no ipv6 mld snooping report-suppression-interval
Mode	Global Configuration Mode

4.1.92 ipv6 mld snooping group-query-interval

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

Syntax	ipv6 mld snooping group-query-interval (2-5) seconds> no ipv6 mld snooping group-query-interval
Mode	Config-VLAN Mode

4.1.91 ipv6 mld snooping fast-leave

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

4.1.91 ipv6 mld snooping querier

Command Objective	This command configures the MLD snooping switch as a querier for a specific VLAN. The switch starts sending general queries at regular time intervals. When the router port gets operationally down and there are no router ports in the switch, the switch continues the querier functionality. The no form of this command configures the MLD snooping switch as non-querier for a specific VLAN.
✎	The configuration can be done only for the VLANs that are activated in the switch.
Syntax	ipv6 mld snooping querier <(60 - 600) seconds> no ipv6 mld snooping querier

Mode	Config-VLAN Mode

4.1.91 ipv6 mld snooping query-interval

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

Syntax	ipv6 mld snooping query-interval <(60 - 600) seconds> no ipv6 mld snooping query-interval
Mode	Config-VLAN Mode

4.1.130 ipv6 mld snooping mrouter

Command Objective	This command configures statically the router ports for a VLAN. The no form of this command deletes the statically configured router ports for a VLAN. By default the router port list is set to none.
✎	The configuration can be done only for the VLANs that are activated in the switch. The specified interface can be set as router ports for the VLAN, only if the interfaces are configured as member ports for that VLAN.

Syntax	ipv6 mld snooping mrouter <interface-type> <0/a-b, 0/c, ...> no ipv6 mld snooping mrouter <interface-type> <0/a-b, 0/c, ...>
Parameter Description	• <interface-type> - Clears all port-level spanning-tree statistics information for the specified type of interface. The interface can be: ■ gigabitethernet – A version of LAN standard architecture that supports data transfer upto 1 Gigabit per second. ■ port-channel – Logical interface that represents an aggregator which contains several ports aggregated together. • <0/a-b, 0/c, ...> - Sets the list of multicast router ports for the list of interfaces or a specific interface identifier. This value is a combination of slot number and port number separated by a slash. Port-channel ID is provided, for interface type port-channel. Use comma as a separator without space while configuring list of interfaces. Example: 0/1, 0/3 or 1, 3.
Mode	Config-VLAN Mode

4.1.131 ipv6 mld snooping blocked-router

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

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

4.1.132 show ipv6 mld snooping mrouter

Command Objective	This command displays the router ports for all the VLANs or a specific VLAN. Interface, ports (type of ports) and switch details are displayed.
Syntax	show ipv6 mld snooping mrouter [Vlan <vlan-id >] [detail] [switch <switch_name>]
Parameter 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.
Mode	Privileged EXEC Mode

4.1.133 show ipv6 mld snooping globals

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

4.1.134 show ipv6 mld snooping

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

4.1.135 show ipv6 mld snooping groups

Command Objective	This command displays the MLDS group information for all VLANs or a specific VLAN or a specific VLAN and group address. Information displayed in the output are Snooping Group information, Vlan id, Group address, Filter mode and so on.
Syntax	show ipv6 mld snooping groups [Vlan <vlan-id > [Group <Address>]] [switch <string (32)>]
Parameter Description	• < vlan-id (1-4094)> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094 • Group <Address> - Displays the Group Address of the VLAN ID • switch <switch_name> - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
Mode	Privileged EXEC Mode

4.1.136 show ipv6 mld snooping forwarding-database

Command Objective	This command displays multicast forwarding entries for all VLANs or a specific VLAN. The information displayed are VLAN, Source address, Group address and Ports.
Syntax	show ipv6 mld snooping forwarding-database [Vlan <vlan-id >] [switch <switch_name>]
Parameter **Description**	• < vlan-id (1-4094)> - VLAN ID is a unique value that represents the specific VLAN. This value ranges between 1 and 4094 • switch <switch_name> - Displays the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
Mode	Privileged EXEC Mode

4.1.137 show ipv6 mld snooping statistics

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

14 PNAC

4.1.138 dot1x system-auth-control

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

4.1.139 shutdown dot1x

Command Objective	This command shuts down dot1x feature. By shutting down the dot1x feature, the supplicant-authenticator-authentication server architecture is dissolved. The data transport and authentication are directly governed by the authentication server/server. When shutdown, all resources acquired by dot1x module are released to the system.
Syntax	shutdown dot1x
	no shutdown dot1x
Mode	Global Configuration Mode

4.1.140 dot1x clear statistics

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

4.1.141 security-suite

Command Objective	This command enables/disables DoS prevention.

Syntax	security-suite no security-suite
Mode	Global Configuration Mode

4.1.142 dot1x guest-vlan

Command Objective	This command configures Dot1x Guest VLAN ID.
Syntax	dot1x guest-vlan <short (1-4094)> no dot1x guest-vlan

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

4.1.91 dot1x default

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

4.1.92 dot1x max-req

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

4.1.91 dot1x max-start

Command Objective	This command sets the maximum number of EAPOL retries to the authenticator.The value range is 1 to 65535.

Syntax	dot1x max-start <count(1-65535)> no dot1x max-start
Mode	Interface Configuration Mode

4.1.92 dot1x reauthentication

Command Objective	This command enables periodic re-authentication from authenticator to client. The periodic re-authentication is requested to ensure if the same supplicant is accessing the protected resources. The amount of time between periodic re-authentication attempts can be configured manually.

Syntax	dot1x reauthentication no dot1x reauthentication
Mode	Interface Configuration Mode

4.1.143 dot1x timeout

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

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

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

	• held-period - Configures the number of seconds that the supplicant waits before trying to acquire the authenticator. • auth-period <value(1-65535)>- Configures the number of seconds that the supplicant waits before timing-out the authenticator
Mode	Interface Configuration Mode

4.1.144 dot1x port-control

Command Objective	This command configures the authenticator port control parameter. The dot1x exercises port based authentication to increase the security of the network. The different Modes employed to the ports offer varied access levels. The 802.1x protocol is supported on both Layer 2 static-access ports and Layer 3 routed ports.

Syntax	dot1x port-control {auto|force-authorized|force-unauthorized} no dot1x port-control
Parameter Description	- auto- Configures the 802.1x authentication process in this port. Causes the port to begin the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up or when an EAPOL-start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and

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

dot1x guest-vlan enable

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

4.1.145 show dot1x

Command Objective	This command displays dot1x information. The configured information can be viewed by running this show command. When there is any change in the configuration to ensure that the port is configured as desired, the show command is used.
Syntax	show dot1x [{ interface <interface-type> <interface-id> | statistics interface <interface-type> <interface-id> | supplicant-statistics interface <interface-type> <interface-id>|local-database | mac-info [address <aa.aa.aa.aa.aa.aa>] | mac-statistics [address <aa.aa.aa.aa.aa.aa>] | all }]

Parameter Description	• interface <interface-type> <interface-id>- Displays dot1x parameters for the switch or the specified interface. • statistics interface <interface-type> <interface-id> - Displays dot1x authenticator port statistics parameters for the switch or the specified interface. • supplicant-statistics interface<interface-type> <interface-id> - Displays dot1x supplicant statistics parameters for the switch or the specified interface. • local-database- Displays dot1x authentication server database with user name and password.
	• mac-info [address <aa.aa.aa.aa.aa.aa>] - Displays dot1x dot1x information for all MAC session or the specified MAC address. • mac-statistics [address <aa.aa.aa.aa.aa.aa>] - Displays dot1x MAC statistic for all MAC session or the specified MAC address. • all - Displays dot1x status for all interfaces.
Mode	Privileged EXEC Mode

4.1.146 show dot1x guest-vlan

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

4.1.147 dot1x re-authenticate

Command Objective	This command initiates re-authentication of all dot1x-enabled ports or the specified dot1x-enabled port. This initializes the state machines and sets up the environment for fresh authentication. Re-authentication is manually configured if periodic re-authentication is not enabled. Re-authentication is requested by the authentication server to the supplicant to furnish the identity without waiting for the configured number of seconds (re-authperiod). If no interface is specified, re-authentication is initiated on all dot1x ports.
Syntax	dot1x re-authenticate [interface <interface-type><interface-id>]
Parameter Description	• <interface type>- Configures the specified type of interface. • <interface id>- Configures the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1.
Mode	Privileged EXEC Mode

exit

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

15 . QOS

4.1.148 Storm-control

Command Objective	This command sets the storm control rate for broadcast, unknown-multicast and DLF packets. The no form of the command sets storm control rate for broadcast, unknown-multicast and DLF packets to the default value.
Syntax	storm-control { broadcast | unknown-multicast | dlf } level <rate-value> no storm-control { broadcast | unknown-multicast | dlf } level
Parameter Description	• broadcast - Broadcast packets. • unknown-multicast –Unknown multicast packets. • dlf - Unknown unicast packets. • level - Storm-control suppression level as a total number of packets per second.
Mode	Interface Configuration Mode

4.1.149 Rate-limit

Command Objective	This command enables the rate limiting on an interface.
	The no form of the command disables the rate limiting.
Syntax	rate-limit { output | input } [<integer(1-80000000)>] no rate-limit { output | input }
Parameter Description	• output – egress limitation. • input –ingress limitation. • <integer(1-80000000)> -Line rate in kbps.
Mode	Interface Configuration Mode

4.1.150 qos

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

4.1.151 qos trust

Command Objective	This command sets qos trust mode.

Syntax	qos trust {cos | dscp | cos-dscp}
Parameter **Description**	- cos – trust cos. - dscp – trust dscp. - cos-dscp – trust cos, if cos not set, trust dscp.
Mode	Global Configuration Mode

4.1.152 priority-map

Command Objective	This command sets the type of the incoming priority mapping to queue. The no form of the command sets default value.

Syntax	priority-map in-priority-type { vlanPri | ipDscp } <integer(0-63)> [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>] [<integer(0-63)>] to <integer(0-7)>
Parameter Description	• vlanPri– Vlan priority. • ipDscp– DSCP. • <integer(0-63)> –Priority value. (0-7) for vlanPri, (0-63) for ipDscp. • integer(0-7) – Queue id.
Mode	Global Configuration Mode

4.1.153 class-policy

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

4.1.154 qos interface

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

4.1.155 match policy – tcp/udp

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

Syntax	match policy { any | host <mac_addr> } { any | host <mac_addr> } [ethertype <integer (1-65535)>] [vlan <short (1-4094)>] [vlan-priority <short (0-7)>] { tcp | udp } {any | host <ip_addr>| <ip_addr> <ip_mask> } [eq <short (1-65535)>] { any | host <ip_addr> | <ip_addr> <ip_mask> } [eq <short (1-65535)>] [dscp <integer (0-63)>] [action { tos <short(0-7)> | dscp <short (0-63)>}]
Parameter **Description**	• any | host <mac_addr> - Source MAC address to be matched with the packet • any | host <mac_addr> - Destination MAC address to be matched with the packet • ethertype <integer (1-65535)> - Specifies the non-IP protocol type to be filtered. • vlan <short (1-4094)> - VLAN value to match against incoming packets. • vlan-priority <short (0-7)> - VLAN priority value to match against incoming packets. • tcp - Transport Control Protocol. • udp - User Datagram Protocol.

- any | host <ip_addr>| <ip_addr> <ip_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 <ip_addr> | <ip_addr> <ip_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 <short (0-63)> - Differentiated services code point provides the quality of service control.
- tos <short(0-7)> - set tos to value.
- dscp <short (0-63)> - set dscp to value.

Mode	Policy Map Configuration Mode

4.1.156 match policy – icmp

Command Objective	This command specifies the ICMP packets to be forwarded based on the associated parameters.
Syntax	match policy { any | host <mac_addr> } { any | host <mac_addr> } [ethertype <integer (1-65535)>] [vlan <short (1-4094)>] [vlan-priority <short (0-7)>] icmp {any | host <ip_addr>| <ip_addr> <ip_mask> } { any | host <ip_addr> | <ip_addr> <ip_mask> } [type <short(0-255)>] [code <short(0-255)>] [dscp <integer (0-63)>] [action { vpt <short(0-7)> | dscp <short (0-63)>}]

Parameter Description	• any | host <mac_addr> - Source MAC address to be matched with the packet • any | host <mac_addr> - Destination MAC address to be matched with the packet • ethertype <integer (1-65535)> - Specifies the non-IP protocol type to be filtered. • vlan <short (1-4094)> - VLAN value to match against incoming packets. • vlan-priority <short (0-7)> - VLAN priority value to match against incoming packets. • any | host <ip_addr>| <ip_addr> <ip_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 <ip_addr> | <ip_addr> <ip_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
- dscp <short (0-63)> - Differentiated services code point provides the quality of service control.
- tos <short(0-7)> - set tos to value.
- dscp <short (0-63)> - set dscp to value.

Mode	Policy Map Configuration Mode

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

Command Objective	This command specifies the ip/ospf/pim/protocol type packets to be forwarded based on the associated parameters.
Syntax	match policy { any | host <mac_addr> } { any | host <mac_addr> } [ethertype <integer (1-65535)>] [vlan <short (1-4094)>] [vlan-priority <short (0-7)>] { ip | ospf | pim | <short (1-255)>} {any | host <ip_addr>| <ip_addr> <ip_mask> } { any | host <ip_addr> | <ip_addr> <ip_mask> } [dscp <integer (0-63)>] [action { vpt <short(0-7)> | dscp <short (0-63)>}]

Parameter Description	• any | host <mac_addr> - Source MAC address to be matched with the packet • any | host <mac_addr> - Destination MAC address to be matched with the packet • ethertype <integer (1-65535)> - Specifies the non-IP protocol type to be filtered. • vlan <short (1-4094)> - VLAN value to match against incoming packets. • vlan-priority <short (0-7)> - VLAN priority value to match against incoming packets. • any | host <ip_addr>| <ip_addr> <ip_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 <ip_addr> | <ip_addr> <ip_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 <short (0-63)> - Differentiated services code point provides the quality of service control. • tos <short(0-7)> - set tos to value. • dscp <short (0-63)> - set dscp to value.
Mode	Policy Map Configuration Mode

4.1.158 no class-policy

Command Objective	This command deletes the class-policy.
Syntax	No class-policy <string(31)>
Parameter Description	• <string(31)> –Name of qos policy.
Mode	Global Configuration Mode

4.1.159 show qos global info

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

4.1.160 show priority-map

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

4.1.161 show class-policy

Command Objective	This command displays the qos policy.
Syntax	show class-policy [{<string(23)> | interface [<iftype> <ifnum>]}]
Parameter Description	• <string(31)> –Name of qos policy. • iftype - Interface type. • ifnum - Interface number.
Mode	Privileged EXEC Mode

4.1.162 show scheduler

Command Objective	This command displays the configured Scheduler.
Syntax	show scheduler
Mode	Privileged EXEC Mode

4.1.163 show qos def-user-priority

Command Objective	This command displays the configured default ingress user priority for a port.
Syntax	show qos def-user-priority [interface <iftype> <ifnum>]
Parameter	• iftype - Interface type. • ifnum - Interface number.
Description	
Mode	Privileged EXEC Mode

4.1.164 qos trust

Command Objective	This command enable/disable qos trust on port.
Syntax	qos trust {enable | disable}
Parameter Description	- enable –enable qos trust on port. - disable - disable qos trust on port.
Mode	Interface Configuration Mode

4.1.165 service-policy

Command Objective	This command enables qos policy on the interface. The no form of this command removes qos policy from the interface.
Syntax	service-policy <string(31)> in no service-policy <string(31)>
Parameter Description	• <string(31)> –Name of qos policy.
Mode	Interface Configuration Mode

16 . RADIUS

4.1.166 radius-server host

Command Objective	This command configures the RADIUS client with the parameters (host, timeout, key, retransmit).
Syntax	radius-server host {ipv4-address |ipv6-address | host-name} [auth-port <integer(1-65535)>] [acct-port <integer(1-65535)>] [timeout <1-120>] [retransmit <1-254>] [key <secret-key-string>] [primary] no radius-server host {ipv4-address |ipv6-address | host-name} [primary]
Parameter Description	• ipv4-address- Configures the IPv4 address of the RADIUS server host. • ipv6-address- Configures the IPv6 address of the RADIUS server host. • host-name - Configures the DNS (Domain Name System) name of the RADIUS server host. This feature has been included to adhere to the Industry Standard CLI syntax. This feature is currently not supported.

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

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

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

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

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

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

Mode	Global Configuration Mode

4.1.167 show radius server

Command Objective	This command displays RADIUS server Host information which contains, Index, Server address, Shared secret, Radius Server status, Response Time, Maximum Retransmission, Authentication Port and Accounting Port.
Syntax	show radius server [{<ucast_addr> | <ip6_addr> | <string>}]

Parameter Description	- <ucast_addr>- Displays the related information of the specified unicast address of the RADIUS server host. - <ip6_addr>- Displays the related information of the specified IPv6 address of the RADIUS server host. - <string>- Displays the name of the RADIUS server host. This maximum value of the string is of size 32.
Mode	Privileged EXEC Mode

4.1.168 show radius statistics

Command Objective	This command displays RADIUS Server Statistics for the data transfer between server and the client from the time of initiation.
Syntax	show radius statistics
Mode	Privileged EXEC Mode

17 RMON

4.1.169 set rmon

Command Objective	This command is used to enable or disable the RMON feature.
Syntax	set rmon {enable | disable}

Parameter Description	- enable - Enables the RMON feature in the system. On enabling, the RMON starts monitoring the networks both local and remote and provides network fault diagnosis - disable - Disables the RMON feature in the system. On disabling, the RMON's network monitoring is called off.
Mode	Global Configuration Mode

4.1.170 rmon alarm

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

Syntax	rmon alarm <short (1-65535)> stats <short (1-65535)> {etherStatsDropEvents | etherStatsOctets | etherStatsPkts |
	etherStatsBroadcastPkts | etherStatsMulticastPkts | etherStatsCRCAlignErrors | etherStatsUndersizePkts | etherStatsOversizePkts | etherStatsFragments | etherStatsJabbers | etherStatsCollisions | etherStatsPkts64Octets | etherStatsPkts65to127Octets | etherStatsPkts128to255Octets | etherStatsPkts256to511Octets | etherStatsPkts512to1023Octets | etherStatsPkts1024to1518Octets } <short (1-65535)> { absolute | delta } rising-threshold <integer (0-2147483647)> [<integer (1-65535)>] falling-threshold <integer (0-2147483647)> [<integer (1-65535)>] [owner <string (127)>] no rmon alarm <number (1-65535)>

Parameter **Description**	• <alarm-number>/ <number (1-65535)>- Displays the value of the statistic during the last sampling period. This value remains available until the current sampling period is completed. For example, if the sample type is deltaValue, this value will be the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value will be the sampled value at the end of the period. This value is compared with the rising and falling thresholds. The value ranges between 1 and 65535. • <mib-object-id (255)>- Identifies the mib object. • <sample-interval-time (1-65535)>- Identifies an entry in the alarm table. Each such entry defines a diagnostic sample at a particular level for a MIB object in the device. This value ranges between 1 and 65535 seconds. • **absolute- Compares the value of the selected variable with the thresholds at the end of the sampling interval.** • delta- Subtracts the value of the selected variable at the last sample from the current value, and the difference is compared with the thresholds at the end of the sampling interval.

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

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

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

	• <falling-event-number (1-65535)>- Raises the index of the event when the Falling threshold is reached. The event entry identified by a particular value of this index is the same as identified by the same value of the event index object. This value ranges between 1 and 65535. • owner<ownername (127)>- Sets the entity that are configured this entry.
Mode	Global Configuration Mode

4.1.171 rmon event

Command Objective	This command adds an event to the RMON event table. The added event is associated with an RMON event number.

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

4.1.172 rmon collection stats

Command Objective	This command enables RMON statistic collection on the interface/ VLAN. The no form of the command disables RMON statistic collection on the interface/ VLAN.
Syntax	rmon collection stats <index (1-65535)> [owner <ownername (127)>] no rmon collection stats <index (1-65535)>

Parameter Description	- <index (1-65535)>- Identifies an entryin the statistics table.. This value ranges between 1 and 65535. - owner <ownername (127)>- Configures the the name of the owner of the RMON group of statistics.

Mode	Interface Configuration Mode / Config VLAN Mode

4.1.173 rmon collection history

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

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

	is the bucket interval where the interface statistics details are stored. This value ranges between 1 and 65535. - interval<seconds (1-3600)>- Configures the time interval over which the data is sampled for each bucket. The value ranges between 1 and 3600. - owner<ownername (127)>- Configures the name of the owner of the RMON group of statistics.
Mode	Interface Configuration Mode / Config VLAN Mode

4.1.174 show rmon

Command Objective	This command displays the RMON statistics, alarms, events, and history configured on the interface.

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

Mode	Privileged EXEC Mode

18 SNMP

4.1.175 enable snmpagent

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

4.1.176 disable snmpagent

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

4.1.177 snmp community

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

Syntax	snmp community name <CommunityName> security <SecurityName> [transporttag <TransportTagIdentifier | none>] [contextengineid <ContextEngineID>] no snmp community name < CommunityName >
Parameter Description	• name<CommunityName> - Creates a community name which stores the community string. • security<SecurityName> - Stores the security model of the corresponding Snmp community name. string specified by the corresponding instance of snmp community name • <TransportTagIdentifier> - Specifies a set of transport endpoints from which a command responder application can accept management request. • contextengineid<ContextEngineID> - Indicates the location of the context through which the management information is accessed when using the community string specified by the corresponding instance of snmp community name
Mode	Global Configuration Mode

4.1.178 snmp group

Command Objective	This command configures SNMP group details. The no form of the command removes the SNMP group details.

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

Parameter Description	• <GroupName> - Creates a name for an SNMP group • user<UserName> - Sets an 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.
Mode	Global Configuration Mode

4.1.179 snmp access

Command Objective	This command configures the SNMP group access details. To configure an SNMP access along with the group, a group must have already been created using the snmp group command. The no form of the command removes the SNMP group access details.
Syntax	snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}} [read <ReadView | none>] [write <WriteView | none>] [notify <NotifyView | none>] no snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}}

Parameter Description	• <GroupName> - Sets the name of the group for which access is to be provided. • v1 | v2c | v3- Sets the SNMP verison. ■ 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
Mode	Global Configuration Mode

4.1.180 snmp engineid

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

4.1.181 snmp view

Command Objective	This command configures the SNMP view. The no form of the command removes the SNMP view.
Syntax	snmp view <ViewName> <OIDTree> [mask <OIDMask>] {included | excluded} no snmp view <ViewName> <OIDTree>
Parameter Description	• <ViewName> - Specifies the view name for which the view details are to be configured. This is a string value with maximum size as 32. • <OIDTree> - Specifies the sub tree value for the particular view. • mask <OIDMask> - Specifies a mask value for the particular view. • included - Allows access to the subtree • excluded - Denies access to the subtree
Mode	Global Configuration Mode

4.1.182 snmp targetaddr

Command Objective	This command configures the SNMP target address. The no form of the command removes the configured SNMP target address.
Syntax	snmp targetaddr <TargetAddressName> param <ParamName> {<IPAddress> | <IP6Address>} [timeout <Seconds(1-1500)] [retries <RetryCount(1-3)] [taglist <TagIdentifier | none>] [port <integer (1-65535)>] no snmp targetaddr <TargetAddressName>

Parameter Description	• <TargetAddressName> - Configures a unique identifier of the Target. • param<ParamName> - Configures the parameters when generating messages to be sent to transport address. • IPAddress - Configures a 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. The taglist can also be set as none using the none option. • port <integer (1-65535)> - Configures a port number through which the generated SNMP notifications are sent to the target address. The value ranges between 1 and 65535.

Mode	Global Configuration Mode

4.1.183 snmp targetparams

Command Objective	This command configures the SNMP target parameters. The no form of the command removes the SNMP target parameters.
Syntax	snmp targetparams <ParamName> user <UserName> security-model {v1 | v2c | v3 {auth | noauth | priv}} message-processing {v1 | v2c | v3} no snmp targetparams <ParamName>
Parameter Description	• <ParamName> - Sets a unique identifier of the parameter.

- User <UserName> - Sets an user for which the target parameter is to be done.
- security-model - Sets the security model
  - v1 – Sets the SNMP version as Version 1.
  - v2c – Sets the SNMP version as Version 2.
  - v3 – Sets the SNMP version as Version 3. It is the most secure model as it allows packet encryption with the priv key word
    - auth - Enables Message digest (MD5) or Secure Hash Algorithm (SHA) packet authentication
    - noauth - Sets no-authentication
    - priv - Specifies both authentication and privacy
- message-processing - Sets the message processing model
  - v1 – Sets the SNMP version as Version 1.
  - v2c – Sets the SNMP version as Version 2.
  - v3 – Sets the SNMP version as Version 3. It is the most secure model as it allows packet encryption with the priv key word

Mode	Global Configuration Mode

4.1.184 snmp user

Command Objective	This command configures the SNMP user details. The no form of the command removes the SNMP user details.
Syntax	snmp user <UserName> [auth {md5 | sha} <passwd> [priv {{{DES | AES_CFB128} <passwd> } | None}]]
	no snmp user <UserName>

Parameter Description	• <UserName> - Configures an user name 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.
Mode	Global Configuration Mode

4.1.185 snmp notify

Command Objective	This command configures the SNMP notification details. The no form of this command removes the SNMP notification details.

Syntax	snmp notify <NotifyName> tag <TagName> type {Trap | Inform} no snmp notify <NotifyName>

Parameter Description	- <NotifyName> - Configures an unique identifier associated with the entry. - tag<TagName> - Sets a notification tag, which selects the entries in the Target Address Table. - type - Sets the notification type. The list contains: ■ Trap – Allows routers to send traps to SNMP managers. Trap is a one-waymessage 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
Mode	Global Configuration Mode

4.1.186 system name

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

4.1.91 system location

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

4.1.92 system contact

Command Objective	This command sets the contact information.
Syntax	system contact <contact info>
Mode	Global Configuration Mode

4.1.93 show snmp

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

Mode	Privileged EXEC Mode

4.1.91 show snmp community

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

4.1.92 show snmp group

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

4.1.93 show snmp group access

Command Objective	This command displays the configured SNMP group access details.

Syntax	show snmp group access
Mode	Privileged EXEC Mode

4.1.91 show snmp engineid

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

4.1.92 show snmp viewtree

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

4.1.91 show snmp targetaddr

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

4.1.92 show snmp targetparam

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

4.1.93 show snmp user

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

4.1.91 show snmp notif

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

19 . SNTP

4.1.187 set sntp client

Command Objective	This command sets the listening port for SNTP client which refers to a port on a server that is waiting for a client connection. The value ranges between 1025 and 65535. The no form of this command deletes the listening port for SNTP client and sets the default value.
Syntax	set sntp client {enabled | disabled}
Parameter Description	• enabled - Enables SNTP client module and sends a request to the host for time synchronization. • disabled - Disables SNTP client module and no request is sent to the host for time synchronization.
Mode	SNTP Configuration Mode

4.1.188 set sntp client port

Command Objective	This command transmits or receives LLDP frames from the server to the LLDP module.
Syntax	set sntp client port <portno(1-65535)>
	no sntp client port
Mode	SNTP Configuration Mode

4.1.189 set sntp time-zone

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

4.1.190 set sntp client clock-summer-time

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

Parameter Description	- week-day-month – The list is given below; ■ week – First, Second, Third, Fourth or Last week of month. ■ day – Sunday, Monday, Tuesday, Wednesday, Thursday, Friday or Saturday. ■ month – /January, February, March, April, May, June, July, August, September, October, November or December. ■ hh:mm - Time in hours and minutes
Mode	SNTP Configuration Mode

4.1.191 set sntp unicast-server

Command Objective	**This command configures SNTP unicast server.** **The no form of this command deletes the sntp unicast server attributes and sets to default value**

Syntax	set sntp unicast-server {ipv4 <ucast_addr> | ipv6 <ip6_addr> | domain- name <string(64)>} [{primary | secondary}] [version {3 | 4 }] [port <integer(1025- 36564)>] no sntp unicast-server {ipv4 <ucast_addr> | ipv6 <ip6_addr> | domain- name <string(64)> }
Parameter Description	• ipv4 <ucast_addr> - Sets the address type of the unicast server as Internet Protocol Version 4. • ipv6 <ip6_addr> - Sets the address type of the unicast server as Internet Protocol Version 6. • domain-name <string(64)> - Sets the domain name for the unicast server. This value is a string with the maximum size as 64. • primary - Sets the unicast server type as primary server. • secondary - Sets the unicast server type as secondary server. • version 3 - Sets the SNTP version as 3. • version 4 - Sets the SNTP version as 4. • port <integer(1025-36564)> - Selects the port identifier numbers in the selected server. This value ranges between 1025 and 36564.
Mode	SNTP Configuration Mode

4.1.91 show sntp clock

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

4.1.92 show sntp status

Command Objective	This command displays SNTP status.
Syntax	show sntp status
Mode	User / Privileged EXEC Mode

20 STP

4.1.192 spanning-tree

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

Syntax	spanning-tree no spanning-tree
Mode	Global Configuration Mode

4.1.193 spanning-tree mode

Command Objective	This command sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch. The current selected type of spanning tree is enabled and the existing spanning tree type is disabled in the switch.
Syntax	spanning-tree mode {mst|rst}

Parameter Description	- mst - Configures the switch to execute MSTP for preventing undesirable loops. MSTP configures spanning tree on per VLAN basis or multiple VLANs per spanning tree. The Mode cannot be set as mst, if the base bridge Mode is configured as transparent bridging. - rst - Configures the switch to execute RSTP for preventing undesirable loops. RSTP provides rapid recovery of connectivity following the failure of a bridge/bridge port or a LAN
Mode	Global Configuration Mode

4.1.194 spanning-tree timers

Command Objective	This command sets the spanning tree timers such as hello time, that are used for controlling the transmission of BPDUs during the computation of loop free topology. The no form of this command resets the spanning tree timers to its default values. The spanning tree timers are reset to its default value, even if the spanning tree Mode is changed.

✎	The values configured for the spanning tree timers should satisfy the following conditions: 2 * (forward-time - 1) >= max-age, and max-age >= 2 * (hello-time +1) The STP timers can be configured in the switch, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown. This spanning tree timer's configuration is not supported in PVRST Mode.

Syntax	spanning-tree {forward-time <seconds(4-30)> | hello-time <seconds(1- 2)> | max-age <seconds(6-40)>}
	no spanning-tree { forward-time | hello-time | max-age }

Parameter Description	• forward-time - Configures the number of seconds, a port waits before changing from the blocking state to the forwarding state. This value ranges between 4 and 30 seconds. In MSTP, this time configuration is applied for IST root (that is, MSTI 0). • hello-time - Configures the time interval (in seconds) between two successive configuration BPDUs generated by the root switch. This value should be either 1 or 2 seconds. This value is configured on per-port basis for MSTP and is configured globally for RSTP. • max-age - Configures the maximum expected arrival time (in seconds) of hello BPDUs. STP information learned from network on any port is discarded, once the configured arrival time expires. The spanning tree topology is re-computed after this time interval. This value ranges between 6 and 40 seconds. In MSTP, this time configuration is applied for IST root (that is, MSTI 0).
Mode	Global Configuration Mode

4.1.91 spanning-tree transmit hold-count

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

Parameter Description	- hold-count **-** This value specifies the maximum number ofpackets that can be sent in a given hello time interval. This value ranges between 1 and 10.
Mode	Global Configuration Mode

4.1.195 spanning-tree priority

Command Objective	**T**his command configures the priority value that is assigned to the switch. The no form of this command resets the priority to its default value. The priority value is changed to its default value even if the spanning tree Mode is changed. In RSTP, this value is used during the election of root. In MSTP, this value is used during the election of CIST root, CIST regional root and IST root.

	The priority value can be configured in the switch, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.
Syntax	spanning-tree [mst <instance-id>] priority <value(0-61440)> no spanning-tree [mst <instance-id(1-64)>] priority

Parameter Description	- mst <instance-id> - Configures the ID of MSTP instance already created in the switch. This value ranges between 1 and 64. The special value 4094 can be used only in the switch that supports PBB-TE. This special value represents PTETID that identifies VID used by ESPs. This option is applicable, only if the spanning tree Mode is set as mst. - priority <value(0-61440)> - Configures the priority value for the switch and for the MSTI, in RSTP and MSTP respectively. This value ranges between 0 and 61440. The value should be set in steps of 4096, that is, you can set the value as 0, 4096, 8192, 12288 and so on.
Mode	Global Configuration Mode

4.1.196 spanning-tree mst forward-time

Command Objective	This command configures the forward timer of the spanning tree and the no form of the command sets the forward timer to the default value. The forward timer controls the speed at which a port changes its spanning tree state from Blocking state to Forwarding state. The timer value ranges between 4 and 30 seconds.
✎	The values configured for the spanning tree forward timers should satisfy the following conditions: 2* (forward-time - 1) >= max-age, and max-age >= 2 * (hello- time +1)
	This command is a standardized implementation of the existing command; spanning-tree timers. It operates similar to the existing command. The STP forward timers can be configured in the switch, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

Syntax	spanning-tree mst forward-time <seconds(4-30)> no spanning-tree mst forward-time
Mode	Global Configuration Mode

4.1.91 spanning-tree mst max-age

Command Objective	**T**his command configures the max-age timer of the spanning tree.The max-age timer denotes the time (in seconds) after which the spanning tree protocol information learnt from the network on any port will be discarded. The timer value ranges between 6 and 40 seconds. The no form of the command sets the max-age timer to the default value.
✎	The values configured for the spanning tree forward timers should satisfy the following conditions:

	2* (forward-time - 1) >= max-age, and max-age >= 2 * (hello- time +1) This command is a standardized implementation of the existing command; spanning-tree timers. It operates similar to the existing command. The STP forward timers can be configured in the switch, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.
Syntax	spanning-tree mst max-age <seconds(6-40)> no spanning-tree mst max-age
Mode	Global Configuration Mode

4.1.91 spanning-tree mst hello-time

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

4.1.197 clear spanning-tree counters

Command Objective	This command deletes all bridge and port level spanning tree statistics information. For RSTP, the information contains number of: · Transitions to forwarding state · RSTP BPDU count received / transmitted · Config BPDU count received / transmitted · TCN BPDU count received / transmitted · Invalid BPDU count transmitted · Port protocol migration count For MSTP, the information contains number of: · Port forward transitions · Port received BPDUs · Port transmitted BPDUs · Port invalid BPDUs received · Port protocol migration count

- BPDUs sent / received for each MSTI

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

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

- 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 upto 1 Gigabit per second.
    - port-channel – Logical interface that represents an aggregator which contains several ports aggregated together.
  - <interface-id> - Clears all port-level spanning-tree statistics information for the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash. For Example: 0/1 represents that the slot number is 0 and port number is 1. Only port-channel ID

is provided, for interface type port-channel. For Example: 1 represents port-channel ID.

Mode	Global Configuration Mode

4.1.91 spanning-tree mst max-instance

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

Syntax	spanning-tree mst max-instance <short(1-64)> no spanning-tree mst max-instance
Mode	Global Configuration Mode

4.1.198 spanning-tree mst root

Command Objective	This command enables BPDU (Bridge Protocol Data Unit) transmission and reception on the interface. This command is a standardized implementation of the existing command; spanning-tree priority. It operates similar to the existing command. The no form of the command disables BPDU transmission and reception on the interface.

This command executes only if

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

Syntax

spanning-tree mst {instance-id <instance-id(1-64)>} root {primary | secondary}

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

Parameter Description

- instance-id <instance-id(1-64)> - Configures the ID of MSTP instance already created in the switch. This value ranges between 1 and 64. This option is applicable, only if the spanning tree Mode is set as mst.
- primary - Sets high enough priority (low value) for the switch so that the switch can be made as the bridge root of the spanning- tree instance. The priority value is set as 24576.
- secondary - Sets the switch as a secondary root, if the primary root fails. The priority value is set as 28672.

Mode	Global Configuration Mode

4.1.91 spanning-tree mst configuration

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

4.1.92 name

Command Objective	This command configures the name for the MST region. The name is unique and used to identify the specific MST region. Each MST region contains multiple spanning tree instances and runs special instance of spanning tree known as IST to disseminate STP topology information for other STP instances.
	The no form of this command resets the name to its default value.
Syntax	name <string(optional max Length 32)> no name
Mode	MSTP Configuration Mode

4.1.91 revision

Command Objective	This command configures the revision number for the MST region. This value ranges between 0 and 65535. The no form of this command resets the revision number to its default value.
Syntax	revision <value(0-65535)> no revision
Mode	MSTP Configuration Mode

4.1.91 instance

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

4.1.92 spanning-tree auto-edge

Command Objective	This command enables automatic detection of Edge port parameter of an interface. The no form of this command disables automatic detection of Edge port parameter of an interface. The automatic detection of Edge port parameter is disabled, even if the spanning tree Mode is changed. Once automatic detection is enabled, the Edge port parameter is automatically detected and set. The port is set as edge port, if no BPDU is received on the port. The port is set as non-edge port, if any BPDU is received.

✎	The automatic detection of Edge port parameter can be configured in the switch, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

Syntax	spanning-tree auto-edge no spanning-tree auto-edge
Mode	Interface Configuration Mode

4.1.91 spanning-tree - Properties of an interface

Command Objective	This command configures the port related spanning tree information for all kinds of STPs. This can be applied for any port, in RSTP/MSTP Mode. This command creates port in STP when Automatic Port Create feature is disabled. The no form of this command resets the port related spanning tree information to its default value. The port related spanning tree information is changed to its default value even if the spanning tree Mode is changed. This command also deletes port in STP when Automatic Port Create feature is disabled.
✎	In STP module, whenever a port is mapped to any context, the corresponding port is created irrespective of whether STP is intended to be enabled on that interface. This leads To STP scaling issues and this problem is solved by having control at STP module on the port entry creation at STP module itself.

Syntax	spanning-tree [{cost <value(0-200000000)>|disable|link-type{point-to-point|shared}|port-priority <value(0-240)>}] no spanning-tree [{cost |disable|link-type|port-priority}]

Parameter **Description**	• cost <value(0-200000000)> - Configures the port's path cost value that contributes to the path cost of paths containing this particular port. The paths' path cost is used during calculation of shortest path to reach the root. The path cost represents the distance between the root port and designated port. This value ranges between 1 and 200000000. The configured path cost is used, even if the dynamic pathcost calculation feature or LAGG speed feature is enabled. • disable - Disables the spanning tree operation on the port. The port does not take part in the execution of spanning tree operation for preventing undesirable loops in the network. ■ link-type - Configures the link status of the LAN segment attached to the port. The options available are: ◆ point-to-point – The port is treated as if it is connected to a point-to-point link. ◆ shared - The port is treated as if it is using a shared media connection. • port-priority – 128
Mode	Interface Configuration Mode

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

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

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

Parameter Description	• <instance-id(1-64)> - Configures the ID of MSTP instance already created in the switch.This value ranges between 1 to 64. • cost<value(1-200000000)> - Configures the port's path cost value that contributes to the path cost of paths containing this particular port. The paths' path cost is used during calculation of shortest path to reach the root. The path cost represents the distance between the root port and designated port. This value ranges between 1 and 200000000. The configured path cost is used, even if the dynamic pathcost calculation feature or LAGG speed feature is enabled. • port-priority<value(0-240)> - Configures the priority value assigned to the port. This value is used during port role selection process. This value ranges between 0 and 240. This value should be set in steps of 16, that is, you can set the value as 0, 16, 32, 48, and so on. The MSTP puts the interface with lowest number in forwarding state and blocks all other interfaces, if all interfaces have the same priority value. • disable - Disables the spanning tree operation on the port. The port does not take part in the execution of spanning tree operation for preventing undesirable loops in the network.
Mode	Interface Configuration Mode

4.1.200 show spanning-tree - Summary, Blockedports, Pathcost

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

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

4.1.201 show spanning-tree detail

Command Objective	This command displays detailed spanning tree related information of the switch and all ports enabled in the switch. The information contains status of spanning tree operation, current selected spanning Mode, current spanning tree compatibility version, bridge and root priority, bridge and root addresses, port path cost, port priority, port timers, bridge and port level spanning tree statistics information, transmit hold-count value, link-type, and status of L2GP, loop guard, BPDU receive, BPDU transmit, restricted TCN, restricted role and portfast features.

	This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.
Syntax	show spanning-tree detail [switch <context_name>]
Parameter Description	• switch <context_name> - Displays detailed spanning tree related information, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.
Mode	Privileged EXEC Mode

4.1.202 show spanning-tree active

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

✎	This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.
Syntax	show spanning-tree active [detail] [switch <context_name>]

Parameter Description	- detail - Displays detailed spanning tree related information of the switch and all ports enabled in the switch. The information contains status of spanning tree operation, current selected spanning Mode, current spanning tree compatibility version, bridge and root priority, bridge and root addresses, port path cost, port priority, port timers, bridge and port level spanning tree statistics information, transmit hold-count value, link-type, and status of L2GP, loop guard, BPDU receive, BPDU transmit, restricted TCN, restricted role and portfast features. - switch <context_name> - Displays spanning tree related information available in the switch, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.
Mode	Privileged EXEC Mode

4.1.203 show spanning-tree interface

Command Objective	This command displays the port related spanning tree information for the specified interface.
	The information contains port ID, port role, port state, port cost, port priority and link type.
✎	This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.
Syntax	show spanning-tree interface <interface-type> <interface-id> [{ cost | priority | rootcost | state | stats | detail }]
Parameter Description	• <interface-type> - Displays the port related spanning tree information for the specified type of interface. The interface can be: ■ gigabitethernet – A version of LAN standard architecture that supports data transfer upto 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 pathcost to reach the root bridge. • 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 portfast features.
Mode	Privileged EXEC Mode

4.1.204 show spanning-tree root

Command Objective	This command displays the spanning tree root information. The information contain root ID, root path cost, maximum age time, forward delay time and root port, for the RSTP. The information also contains the instance ID for MSTP.
✎	This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.
Syntax	show spanning-tree root [{ address | cost | forward-time | id | max- age | port | priority | detail }] [switch <context_name>]

Parameter Description	- address - Displays the MAC address of the root bridge. - cost - Displays the cost of the root bridge. - forward-time - Displays the forward delay time of the root bridge. - id - Displays the ID of the root bridge. - max-age - Displays the maximum age time of the root bridge. - port - Displays the ID of the root port. - priority - Displays the priority of the root bridge. - detail - Displays the root priority, root address, root cost, root port, forward delay time and maximum age time. - switch <context_name> - Displays spanning tree root information, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.
Mode	Privileged EXEC Mode

4.1.205 show spanning-tree bridge

Command Objective	This command displays the spanning tree bridge information. The information contain bridge ID, hello time, maximum age time, forward delay time and protocol enabled, for the RSTP. The information also contains the instance ID for MSTP.
✎	This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set, if the functionality is already shutdown.

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

Parameter Description	- address - Displays the MAC address of the bridge. - forward-time - Displays the forward delay time of the bridge. - hello-time - Displays the hello time of the bridge. - id - Displays the ID of the bridge. - max-age - Displays the maximum age time of the bridge. - protocol - Displays the protocol currently enabled in the bridge. - priority - Displays the priority of the bridge. - detail - Displays the priority, address, maximum age time and forward delay time for the bridge. - switch - Displays spanning tree bridge information, for the specified context. This value represents unique name of the switch context. This value is a string with the maximum size as 32. This parameter is specific to multiple instance feature.
Mode	Privileged EXEC Mode

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

Command Objective	This command displays multiple spanning tree information for all MSTIs in the switch. The information contain MSTI ID, VLAN IDs mapped to the instance, bridge address and priority, root address and priority, IST root address, priority and path cost, forward delay, maximum age, maximum hop count, and port details of interfaces enabled in the switch. The port details contain
	interface ID, port role, port state, port cost, port priority and port link type.
✎	This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set as mst.
Syntax	show spanning-tree mst [<instance-id(1-64)>] [detail] [switch <context_name>]

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

4.1.207 show spanning-tree mst configuration

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

4.1.208 show spanning-tree mst - Port Specific Configuration

Command Objective	This command displays multiple spanning tree port specific information for the specified port. This information contain interface ID, edge port status, port link type, port hello time, BPDUs sent and received on the port, and instance related details. The instance details contain MSTI ID, MSTI role, MSTI status, MSTI cost and MSTI priority.
✎	This command can be executed successfully, only if the spanning tree functionality is not shutdown in the switch. The type of spanning tree Mode should be set as mst.
Syntax	show spanning-tree mst [<instance-id(1-64)>] interface <interface- type> <interface-id> [{ stats | hello-time | detail }]

Parameter Description	• <instance-id(1-64)> - Displays the multiple spanning tree port specific information for the specified MSTI. This value ranges between 1 to 64. • <interface-type> - Displays the port related spanning tree information for the specified type of interface. The interface can be: ■ gigabitethernet – A version of LAN standard architecture that supports data transfer upto 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 contain port priority, port cost, root address, priority and cost, IST

	address, priority and cost, bridge address, priority and cost, forward delay, maximum age, maximum hop count, and BPDUs sent and received.
Mode	Privileged EXEC Mode

21 . SSH

4.1.209 ip ssh server

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

4.1.210 show ssh-configurations

Command Objective	This command displays SSH server configurations.
Syntax	show ssh-configurations
Mode	Global Configuration Mode

22 . SSL

4.1.211 show ip http secure server status

Command Objective	This command displays SSL status and configuration information. Information such as HTTP secure server status, HTTP secure server ciphersuite are displayed.

Syntax	show ip http secure server status
Mode	Privileged EXEC Mode

4.1.212 ip http secure server

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

23 SYSLOG

4.1.213 show logging-server

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

4.1.214 show logging

Command Objective	This command displays all the logging status and configuration information.

Syntax	show logging
Mode	Privilege EXEC Mode

4.1.215 logging

Command Objective	This command enables syslog server and configures the syslog related parameters The logging process controls the distribution of logging messages to the various destinations.
Syntax	logging severity { alerts | critical | debugging | emergencies | errors | informational | notification | warnings }

Parameter Description	- 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.
Mode	Global Configuration Mode

4.1.216 logging-service

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

4.1.217 clear logs

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

4.1.218 logging server

Command Objective	This command configures a server table to log an entry in it. The no form of command deletes an entry from the server table.
Syntax	logging-server {facility {local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7}} {severity { emergencies | alerts | critical | errors | warnings | notification | informational| debugging}} {ipv4 <ucast_addr> |ipv6 <ip6_addr> | <string>} [port <integer(0-65535)>]

Parameter Description	• facility - The facility that is indicated in the message. Can be one of the following values: local0, local1, local2, local3, local4, local5, local 6, local7.. • severity - Message severity level. Messages with severity level equal to or high than the specified value are printed asynchronously. This can be configured using numerical value or using the available option. The options are: ■ 0 | emergencies - System is unusable ■ 1 | alerts - Immediate action needed. ■ 2 | critical - Critical conditions. ■ 3 | errors - Error conditions. ■ 4 | warnings - Warning conditions. ■ 5 | notification - Normal but significant conditions. ■ 6 | informational - Informational messages. ■ 7 | debugging – Debugging messages. • ipv4 <ucast_addr> - Sets the server address type as internet protocol version 4. • ipv6 <ip6_addr> - Sets the server address type as internet protocol version 6. • <string> - Configures the host name for a server to log an entry. • port<integer(0-65535)> - Sets the port number through which it sends the syslog message. The value ranges between 0 and 65535.

Mode	Global Configuration Mode

24 . VLAN

4.1.219 vlan

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

4.1.220 ports

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

	[untagged (<interface-type> <0/a-b,0/c,...> [<interface-type> <0/a- b,0/c,...>] [port-channel <a,b,c-d>] [pw <a,b,c-d>] [ac <a,b,c-d>] [all])] [forbidden <interface-type> <0/a-b,0/c,...> [<interface-type> <0/a- b,0/c,...>] [port-channel <a,b,c-d>] [pw <a,b,c-d>][ac <a,b,c-d>]] [name <vlan-name>] no ports [<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a- b,0/c,...>] [port-channel <a,b,c-d>] [pw <a,b,c-d>] [ac <a,b,c-d>] [all] [untagged ([<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a- b,0/c,...>] [port-channel <a,b,c-d>] [pw <a,b,c-d>] [ac <a,b,c-d>] [all])] [forbidden ([<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a- b,0/c,...>] [port-channel <a,b,c-d>] [pw <a,b,c-d>] [ac <a,b,c-d>] [all])] [name <vlan-name>]

Parameter **Description**	• add - Appends the new configured ports to the existing member port list of the vlan. • <interface-type> - Configures the ports that should be set as a member of the VLAN. • port-channel - 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. • pw - Configures the Pseudo wire interface as member port. When the pseudo wire interface is mapped to a specific VLAN, the interface structures are created. This value ranges between 1 and 65535. - Maximum number of8 interfaces supported in the system is 100. • ac <a,b, c-d>- Configures the specified attachment circuit interface as a member port. This value ranges between 1 and 65535. Use comma as a separator without space while configuring list of interfaces. Example: 1,3.

	• all- Deletes all configured member ports for the VLAN and sets the member ports as none. This option is available only in the no form of the command. • untagged<interface-type> <0/a-b,0/c,...>- Configures the ports that should be used for the VLAN to transmit egress packets as untagged packets. • forbidden<interface-type> <0/a-b,0/c,...>- Configures the ports that should never receive packets from the VLAN. • name<vlan-name>- Configures the unique name of the VLAN. This name is used to identify the VLAN and is an administratively assigned string with the maximum size as 32.
Mode	Config-VLAN Mode

4.1.221 exit

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

4.1.222 switchport pvid

Command Objective	This command configures the PVID on the specified port. The PVID represents the VLAN ID that is to be assigned to untagged frames or priority-tagged or C-VLAN frames received on the port. The PVID is used for port based VLAN type membership classification. This value ranges between 1 and 4094.
Syntax	switchport pvid <vlan-id>

Parameter Description	• pvid<vlan-id(1-4094)>- Configures the PVID for the provider edge port for the specified VLAN ID. This is a unique value that represents the specific VLAN. This value ranges between 1 and 4094.
Mode	Interface Configuration mode (Physical / Port channel)
Example	TL2-F7120# c t TL2-F7120(config)# interface gigabitethernet 0/13 TL2-F7120(config-if)# **switchport pvid 3** TL2-F7120(config-if)# exit TL2-F7120(config)# exit TL2-F7120# show vlan port config port gigabitethernet 0/13
	Vlan Port configuration table -------------------------------- Port Gi0/13

```
Bridge Port Type                         : Customer Bridge Port

PVID                                     : 3

Port Acceptable Frame Type               : Admit All

Port Mac Learning Status                 : Enabled

Port Ingress Filtering                   : Disabled

Port Mode                                : Hybrid

Port Gvrp Status                         : Disabled

Port Gmrp Status                         : Disabled Port Gvrp Failed Registrations      : 2

Gvrp last pdu origin                     : 00:00:00:00:00:00 Port Restricted Vlan Registration    :

Disabled

Port Restricted Group Registration       : Unknown 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

                 ------------------------------------------------------- TL2-F7120#
```

4.1.223 switchport acceptable-frame-type

Command Objective	This command is to configure the acceptable frame types for a port.

Syntax	switchport acceptable-frame-type {all | tagged | untaggedAndPrioritytagged }
Parameter Description	• all- Configures the acceptable frame type as all. All tagged, untagged and priority tagged frames received on the port are accepted and subjected to ingress filtering. • tagged- Configures the acceptable frame type as tagged. • untaggedAndPrioritytagged- Configures the acceptable frame type as untagged and priority tagged. Only the untagged or priority tagged frames received on the port are accepted and subjected to ingress filtering. The tagged frames received on the port are rejected.
Mode	Interface Configuration mode (Physical / Port channel)

Example

```
TL2-F7120# c t

TL2-F7120(config)# interface gigabitethernet 0/13

TL2-F7120(config-if)# switchport  acceptable-frame-type
untaggedAndPrioritytagged

TL2-F7120(config-if)# exit TL2-

F7120(config)# exit

TL2-F7120# show vlan port config port gigabitethernet 0/13


Vlan Port configuration table

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

Port Gi0/13

  Bridge Port Type                        : Customer Bridge Port

  PVID                                    : 3

  Port Acceptable Frame Type              : AdmitOnly Untagged and
Priority  Tagged

  Port Mac Learning Status                : Enabled

  Port Ingress Filtering                  : Disabled

  Port Mode                               : Hybrid

  Port Gvrp Status                        : Disabled
  Port Gmrp Status                              : Disabled

  Port Gvrp Failed Registrations                : 2

  Gvrp last pdu origin                          : 00:00:00:00:00:00
```

```
Port Restricted Vlan Registration          : Disabled Port Restricted Group Registration    : Unknown 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

----------------------------------------------------------- TL2-F7120#
```

4.1.224 switchport ingress-filter

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

4.1.91 show vlan

Command Objective	This command displays VLAN entry related information of all active VLANs and VLANs (that are not active) for which the port details are configured. The information contain the member ports, untagged ports, forbidden ports, VLAN name and the status of that VLAN entry.
Syntax	show vlan [brief | id <vlan-range> | summary] [switch <context_name>]

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

Mode	Privileged EXEC Mode

4.1.225 show vlan device info

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

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

4.1.226 show vlan device capabilities

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

Syntax	show vlan device capabilities [switch <context_name>]

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

4.1.227 show vlan port config

Command Objective	This command displays the VLAN related port specific information for all interfaces available in the switch / all contexts. The information contains PVID, acceptable frame type, port mode, filtering utility criteria, default priority value and status of ingress filtering feature, GVRP module, GMRP module, restricted VLAN registration feature, restricted group registration feature, MAC-based VLAN membership, subnet based VLAN membership, protocol-VLAN based membership and port protected feature.
Syntax	show vlan port config [{port < interface-type > <ifnum> | switch <string(32)>}]
Parameter Description	• <interface-type> - Displays the VLAN related port specific information for the specified interface. ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second.

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

4.1.228 show vlan statistics

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

	are activated and VLANs (that are not active) for which the port details are configured. - switch <context_name> - Displays the VLAN global information that is applicable to all VLANs, for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
Mode	Privileged EXEC Mode

4.1.229 show mac-address-table

Command Objective	This command displays all static / dynamic unicast and multicast MAC entries created in the MAC address table. These entries contain VLAN ID, unicast / multicast MAC address, unicast backbone MAC address of peer backbone edge bridge, member ports, the type of entry (that is static, learnt and so on), and total number of entries displayed.
Syntax	show mac-address-table [vlan <string(9)>] [address <mac_addr>] [{interface <interface-type> <ifnum> | switch <string(32)>}]
Parameter **Description**	• vlan <vlan-range>- Displays all static / dynamic unicast and multicast MAC entries created in the MAC address table for the specified VLANs alone. This value denotes the VLAN ID range for which the entries need to be displayed. This value is a string with the maximum size as 9. For example, the value is provided as 4000-4010 to display the entries for VLAN IDs from 4000 to4010.

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

4.1.230 show mac-address-table count

Command Objective	This command displays the total number of static / dynamic unicast and multicast MAC address entries created in the FDB table. The count is displayed for all active VLANs, VLANs (that are not active) for which the port details are configured, and VLANs for which the MAC address table entries are created.
Syntax	show mac-address-table count [vlan <vlan_id>] [switch <string(32)>]
Parameter Description	• vlan <vlan-id>- Displays the total number of static / dynamic unicast and multicast MAC address entries created for the specified VLAN ID. This value ranges between 1 and 65535.
	• switch <context_name> - Displays the VLAN global information that is applicable to all VLANs, for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
Mode	Privileged EXEC Mode

4.1.231 show mac-address-table static multicast

Command Objective

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

These entries contain VLAN ID to which multicast MAC address entry is assigned, multicast MAC address, member ports, receiver ports, forbidden ports, the status of entry (that is permanent, static and so on), and total number of entries displayed.

Syntax

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

Parameter Description

- vlan <vlan-range>- Displays all static / dynamic unicast and multicast MAC entries created in the MAC address table for the specified VLANs alone. This value denotes the VLAN ID range for which the entries need to be displayed. This value is a string with

	the maximum size as 9. For example, the value is provided as 4000-4010 to display the entries for VLAN IDs from 4000 to 4010. • address <aa:aa:aa:aa:aa:aa> - Displays all static / dynamic unicast and multicast MAC entries created in the MAC address table for the specified unicast / multicast MAC address. • <interface-type> - Displays all static multicast MAC address entries for the specified interface. ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. • switch <context_name> - Displays the VLAN global information that is applicable to all VLANs, for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
Mode	Privileged EXEC Mode

4.1.232 show mac-address-table dynamic unicast

Command Objective	This command displays all dynamically learnt unicast entries from the MAC address table. These entries contain VLAN ID for which unicast MAC address entry is learnt, unicast MAC address, ports through which the entry is learnt, the status of entry (that is permanent, static and so on), the unicast backbone MAC address of peer backbone edge bridge, and total number of entries displayed.

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

Parameter Description	- vlan <vlan-range>- Displays all static / dynamic unicast and multicast MAC entries created in the MAC address table for the specified VLANs alone. This value denotes the VLAN ID range for which the entries need to be displayed. This value is a string with the maximum size as 9. For example, the value is provided as 4000-4010 to display the entries for VLAN IDs from 4000 to 4010. - address <aa:aa:aa:aa:aa:aa> - Displays all static / dynamic unicast and multicast MAC entries created in the MAC address table for the specified unicast / multicast MAC address. - <interface-type> - Displays all static multicast MAC address entries for the specified interface. ■ gigabitethernet – A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. - switch <context_name> - Displays the VLAN global information that is applicable to all VLANs, for the specified context. This value represents unique name of the switch context. This value is a string whose maximum size is 32. This parameter is specific to multiple instance feature.
Mode	Privileged EXEC Mode

4.1.233 show mac-address-table aging-time

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

25 . VOICE-VLAN

4.1.234 voice vlan state

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

4.1.235 voice vlan id

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

4.1.236 voice vlan aging-time

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

4.1.237 voice vlan cos

Command Objective	This command specifies the OUI Voice VLAN Class of Service (CoS).
Syntax	voice vlan cos <integer(0-7)> [remark]
Parameter Description	• <integer(0-7)> – cos. • [remark] – Specifies that the L2 user priority is remarked with the CoS value.
Mode	Global Configuration Mode

4.1.238 voice vlan vpt

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

4.1.239 voice vlan dscp

Command Objective	This command specifies the LLDP-MED dscp.
Syntax	voice vlan dscp <integer(0-63)>

Parameter **Description**	• <integer(0-63)> – dscp.
Mode	Global Configuration Mode

4.1.240 voice vlan oui-table

Command Objective	This command specifies the voice vlan OUI table.
Syntax	voice vlan oui-table {add <ucast_mac> [<string(32)>] | remove <ucast_mac>}
Parameter **Description**	• add <ucast_mac> – Add voice device mac address prefix to OUI table. • [<string(32)>] - Voice device prefix description. • remove <ucast_mac> - Remove voice device mac address prefix from OUI table.

Mode	Global Configuration Mode

4.1.241 voice vlan enable

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

4.1.242 voice vlan cos mode

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

4.1.243 show voice vlan

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

Technical Specifications

Standards

- IEEE 802.1p
- IEEE 802.1Q
- IEEE 802.1s
- IEEE 802.1w
- IEEE 802.1X
- IEEE 802.1ab
- IEEE 802.1ax
- IEEE 802.3ab
- IEEE 802.3ae
- IEEE 802.3az
- IEEE 802.3x
- IEEE 802.3z

Device Interface

- 12 x SFP+ slots (1Gbps / 10Gbps)
- 1 x RJ-45 console port (out-of-band)
- LED indicators
- Reset button

Data Transfer Rate

- Gigabit Ethernet: 2000Mbps (full duplex)
- 10 Gigabit Ethernet: 20Gbps (full duplex)

Performance

- Switching capacity: 240Gbps
- RAM buffer: 2MB
- MAC address table: 32K entries
- Jumbo frames: 10KB
- Forwarding mode: store and forward
- Forwarding rate: 178.6Mpps (64-byte packet size)

Management

- CLI (Console / Telnet / SSH)
- GUI (HTTP / HTTPS)
- IPv4/IPv6
- DNS
- TFTP/HTTP firmware upgrade
- TFTP/HTTP backup and restore configuration
- SNMP v1, v2c, v3
- SNMP trap
- RMON groups 1/2/3/9
- LLDP
- ICMPv4/ICMPv6
- Trace Route IPv4/IPv6
- Virtual cable diagnostics test
- Simple Network time protocol (SNTP)
- Multi-User (Admin/User privilege)
- Dual image (Active/Backup)
- SNTP/NTP
- System Log (Local/Download/Remote Syslog)
- MAC entries (Static/Dynamic)
- ARP entries (Static/Dynamic)
- IPv6 neighbor discovery entries (Static/Dynamic)
- Port mirror (One to one, many to one)
- Digital diagnostics monitoring (DDM) for SFP modules
- Storm control: Broadcast, unknown multicast, unknown unicast (Min. limit: 16kbps)
- Port statistics counter
- Loopback detection
- CPU/Memory Utilization
- Real-time port statistics

MIB

- RMON MIB RFC 1757
- MIB II RFC 1213
- Ethernet intf MIB RFC 1643
- Bridge MIB RFC 1493

Spanning Tree

- Rapid spanning tree protocol (RSTP)
- Multiple spanning tree protocol (MSTP) Up to 16 instances

Link Aggregation

- Static link aggregation
- Dynamic LACP (Up to 8 groups, 8 ports per group)

Quality of Service (QoS)

- Class of service (CoS)
- Differentiated Services Code Point (DSCP)
- Bandwidth control per port/rate limiting
- Queue scheduling: strict priority (SP), weighted round robin (WRR)

Storm Control

- Broadcast (Min. limit: 16Kbps)
- Unknown Multicast (Min. limit: 16Kbps)
- Unknown Unicast (Min. limit: 16Kbps)

VLAN

- Management access VLAN assignment
- 802.1Q tagged VLAN
- Dynamic GVRP
- Port Isolation
- Up to 256 VLAN groups, ID range 1-4094
- Voice VLAN
- Dynamic VLAN

L3 Features

- IPv4 / IPv6 static routing
- IPv4 interfaces: Up to 4
- IPv6 interfaces: Up to 8
- Routing table entries: IPv4: 63 max. / IPv6: 21 max.
- Default route entries: 1 (IPv4 / IPv6)
- ARP table (up to 192 entries)
- DHCP IPv4 relay
- Inter-VLAN routing

Multicast

- IGMP snooping v1, v2, v3
- MLD Snooping v1, v2
- IGMP/MLD fast leave and querier
- IGMP/MLD dynamic router port, and report suppression
- Multicast filtering
- Up to 256 multicast groups

Access Control

- 802.1X authentication (Local, RADIUS IPv4, TACACS+ IPv4)
- 802.1X RADIUS/Guest VLAN assignment, MAC-based authentication
- DHCP snooping
- Port Security/MAC address learning restriction (Up to 256 entries per port)
- Denial of Service (DoS)

Power

- Input: 100 – 240V AC, 50/60 Hz, 1.5A
- Max. Consumption: 20W

Fan/Acoustics

- Quantity: 1
- Smart Fan

- Noise Level: 38.6 dBa (max.)

MTBF

- 224,641 hours

Operating Temperature

- 0° – 50° C (32° – 122° F)

Operating Humidity

- Max. 90% non-condensing

Dimensions

- 210 x 230 x 44mm (8.26 x 9.06 x 1.73 in.)
- Rack mountable 1U height
- Dual 1U rackmount kit option (ETH-F71 sold separately)

Weight

- 1.6 kg (3.5 lbs.)

Certifications

- CE
- FCC
- UL

Troubleshooting

Q: I typed http://192.168.10.200 in my Internet Browser Address Bar, but an error message says "The page cannot be displayed." How can I access the switch management page?
Answer:
1. Check your hardware settings again. See "Switch Installation" on page 8.
2. Make sure the Power and port Link/Activity and WLAN lights are lit.
3. Make sure your network adapter TCP/IP settings are set to *Use the following IP address or Static IP*(see the steps below).
4. Make sure your computer is connected to one of the Ethernet switch ports.
5. Since the switch default IP address is 192.168.10.200, make sure there are no other network devices assigned an IP address of 192.168.10.200

Windows 7/8/8.1/10

a. Go into the **Control Panel**, click **Network and Sharing Center**.

b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.

c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.

d. Then click **Use the following IP address,** and make sure to assign your network adapter an IP address in the subnet of 192.168.10.x. Click **OK**

Windows Vista

a. Go into the **Control Panel**, click **Network and Internet**.
b. Click **Manage Network Connections,** right-click the **Local Area Connection** icon and click **Properties**.
c. Click **Internet Protocol Version (TCP/IPv4)** and then click **Properties**.

d. Then click **Use the following IP address,** and make sure to assign your network adapter an IP address in the subnet of 192.168.10.x. Click **OK**

Windows XP/2000

a. Go into the **Control Panel**, double-click the **Network Connections** icon
b. Right-click the **Local Area Connection** icon and the click **Properties**.
c. Click **Internet Protocol (TCP/IP)** and click **Properties**.

d. Then click **Use the following IP address,** and make sure to assign your network adapter an IP address in the subnet of 192.168.10.x. Click **OK**

Note: *If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.*

Q: If my switch IP address is different than my network's subnet, what should I do?
Answer:
You should still configure the switch first. After all the settings are applied, go to the switch configuration page, click on System, click IPv4 Setup and change the IP address of the switch to be within your network's IP subnet. Click Apply, then click OK. Then click Save Settings to Flash (menu) and click Save Settings to Flash to save the IP settings to the NV-RAM.

Q: I changed the IP address of the switch, but I forgot it. How do I reset my switch?
Answer:
Using a paper clip, push and hold the reset button on the front of the switch and release after 15 seconds.
The default IP address of the switch is 192.168.10.200. The default user name and password is "admin".

Appendix

How to find your IP address?

Note: *Please note that although the following procedures provided to follow for your operating system on configuring your network settings can be used as general guidelines, however, it is strongly recommended that you consult your computer or operating system manufacturer directly for assistance on the proper procedure for configuring network settings.*

Command Prompt Method

Windows 2000/XP/Vista/7/8/8.1/10

1. On your keyboard, press **Windows Logo+R** keys simultaneously to bring up the Run dialog box.

2. In the dialog box, type ***cmd*** to bring up the command prompt.

3. In the command prompt, type ***ipconfig /all*** to display your IP address settings.

MAC OS X

1. Navigate to your **Applications** folder and open **Utilities**.

2. Double-click on **Terminal** to launch the command prompt.

3. In the command prompt, type ***ipconfig getifaddr <en0 or en1>*** to display the wired or wireless IP address settings.

Note: en0 *is typically the wired Ethernet and* ***en1*** *is typically the wireless Airport interface.*

Graphical Method

MAC OS 10.6/10.5

1. From the Apple menu, select **System Preferences**.
2. In System Preferences, from the **View** menu, select **Network**.
3. In the Network preference window, click a network port (e.g., Ethernet, AirPort, modem). If you are connected, you'll see your IP address settings under "Status:"

MAC OS 10.4

1. From the Apple menu, select **Location**, and then **Network Preferences**.
2. In the Network Preference window, next to "Show:", select **Network Status**. You'll see your network status and your IP address settings displayed.

Note: *If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.*

How to configure your network settings to use a static IP address?

Note: *Please note that although the following procedures provided to follow for your operating system on configuring your network settings can be used as general guidelines, however, it is strongly recommended that you consult your computer or operating system manufacturer directly for assistance on the proper procedure for configuring network settings.*

Windows 7/8/8.1/10

a. Go into the **Control Panel**, click **Network and Sharing Center**.

b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.

c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.

d. Then click **Use the following IP address,** and assign your network adapter a static IP address. Click **OK**

Windows Vista

a. Go into the **Control Panel**, click **Network and Internet**.
b. Click **Manage Network Connections,** right-click the **Local Area Connection** icon and click **Properties**.
c. Click **Internet Protocol Version (TCP/IPv4)** and then click **Properties**.

d. Then click **Use the following IP address,** and assign your network adapter a static IP address. Click **OK**

Windows XP/2000

a. Go into the **Control Panel**, double-click the **Network Connections** icon
b. Right-click the **Local Area Connection** icon and the click **Properties**.
c. Click **Internet Protocol (TCP/IP)** and click **Properties**.

d. Then click **Use the following IP address,** and assign your network adapter a static IP address. Click **OK**

MAC OS 10.4/10.5/10.6

a. From the **Apple**, drop-down list, select **System Preferences**.
b. Click the **Network** icon.
c. From the **Location** drop-down list, select **Automatic**.

d. Select and view your Ethernet connection.

In MAC OS 10.4, from the **Show** drop-down list, select **Built-in Ethernet** and select the **TCP/IP** tab.

In MAC OS 10.5/10.6, in the left column, select **Ethernet**.

e. Configure TCP/IP to use a static IP.

In MAC 10.4, from the **Configure IPv4**, drop-down list, select **Manually** and assign your network adapter a static IP address. Then click the **Apply Now** button.

In MAC 10.5/10.6, from the **Configure** drop-down list, select **Manually** and assign your network adapter a static IP address . Then click the **Apply** button.

f. Restart your computer.

Note: *If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.*

How to find your MAC address?

In Windows 2000/XP/Vista/7/8.1/.10,

Your computer MAC addresses are also displayed in this window, however, you can type ***getmac –v*** to display the MAC addresses only.

In MAC OS 10.4,

1. **Apple Menu > System Preferences > Network**
2. From the **Show** menu, select **Built-in Ethernet**.
3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.

In MAC OS 10.5/10.6,

1. **Apple Menu > System Preferences > Network**
2. Select **Ethernet** from the list on the left.
3. Click the **Advanced** button.
3. On the **Ethernet** tab, the **Ethernet ID** is your MAC Address.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth fo environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Country Code selection feature to be disabled for products marketed to the US/CANADA

RoHS

This product is RoHS compliant.

Europe – EU Declaration of Conformity

TRENDnet hereby declare that the product is in compliance with the essential requirements and other relevant provisions under our sole responsibility.

- **EN 62368-1:2014/A11:2017**
- **EN 55032:2015/A1:2020, Class A**
- **EN 55035:2017/A11:2020**
- **EN IEC 61000-3-2:2019/A1:2021**
- **EN 61000-3-3:2013/A2:2021**

Directives:

EMC Directive EN 2014/30/EC
RoHS Directive 2011/65/EU
REACH Regulation (EC) No. 1907/2006
Low Voltage Directive 2014/35/EC
Ecodesign Directive 2009/125/EC

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Limited Warranty

TRENDnet warrants only to the original purchaser of this product from a TRENDnet authorized reseller or distributor that this product will be free from defects in material and workmanship under normal use and service. This limited warranty is non-transferable and does not apply to any purchaser who bought the product from a reseller or distributor not authorized by TRENDnet, including but not limited to purchases from Internet auction sites.

Limited Warranty

TRENDnet warrants its products against defects in material and workmanship, under normal use and service. Specific warranty periods are listed on each of the respective product pages on the TRENDnet website.

- AC/DC Power Adapter, Cooling Fan, and Power Supply carry a one-year warranty.

Limited Lifetime Warranty

TRENDnet offers a limited lifetime warranty for all of its metal-enclosed network switches that have been purchased in the United States/Canada on or after 1/1/2015.

- Cooling fan and internal power supply carry a one-year warranty

To obtain an RMA, the ORIGINAL PURCHASER must show Proof of Purchase and return the unit to the address provided. The customer is responsible for any shipping-related costs that may occur. Replacement goods will be shipped back to the customer at TRENDnet's expense.

Upon receiving the RMA unit, TRENDnet may repair the unit using refurbished parts. In the event that the RMA unit needs to be replaced, TRENDnet may replace it with a refurbished product of the same or comparable model.

In the event that, after evaluation, TRENDnet cannot replace the defective product or there is no comparable model available, we will refund the depreciated value of the product.

If a product does not operate as warranted during the applicable warranty period, TRENDnet shall reserve the right, at its expense, to repair or replace the defective product or part and deliver an equivalent product or part to the customer. The repair/replacement unit's warranty continues from the original date of purchase. All products that are replaced become the property of TRENDnet. Replacement products may be new or reconditioned. TRENDnet does not issue refunds or credit. Please contact the point-of-purchase for their return policies.

TRENDnet shall not be responsible for any software, firmware, information, or memory data of customer contained in, stored on, or integrated with any products returned to TRENDnet pursuant to any warranty.

There are no user serviceable parts inside the product. Do not remove or attempt to service the product by any unauthorized service center. This warranty is voided if (i) the product has been modified or repaired by any unauthorized service center, (ii) the product was subject to accident, abuse, or improper use, or (iii) the product was subject to conditions more severe than those specified in the manual.

Warranty service may be obtained by contacting TRENDnet within the applicable warranty period and providing a copy of the dated proof of the purchase. Upon proper submission of required documentation, a Return Material Authorization (RMA) number will be issued. An RMA number is required in order to initiate warranty service support for all TRENDnet products. Products that are sent to TRENDnet for RMA service must have the RMA number marked on the outside of return packages and sent to TRENDnet prepaid, insured and packaged appropriately for safe shipment. International customers shipping from outside of the USA and Canada are responsible for any return shipping and/or customs charges, including but not limited to, duty, tax, and other fees.

Refurbished product: Refurbished products carry a 90-day warranty after date of purchase. Please retain the dated sales receipt with purchase price clearly visible as evidence of the original purchaser's date of purchase. Replacement products may be refurbished or contain refurbished materials. If TRENDnet, by its sole determination, is unable to replace the defective product, we will offer a refund for the depreciated value of the product.

WARRANTIES EXCLUSIVE: IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACE. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, OR USE OF TRENDNET'S PRODUCTS.

TRENDNET SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW, TRENDNET ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATE, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT TRENDNET'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Governing Law: This Limited Warranty shall be governed by the laws of the state of California.

Some TRENDnet products include software code written by third party developers. These codes are subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL").

Visit http://www.trendnet.com/gpl or the support section on http://www.trendnet.com and search for the desired TRENDnet product to access to the GPL Code or LGPL Code. These codes are distributed WITHOUT WARRANTY and are subject to the copyrights of the developers. TRENDnet does not provide technical support for these codes. Please visit http://www.gnu.org/licenses/gpl.txt or http://www.gnu.org/licenses/lgpl.txt for specific terms of each license.

PWP07172015v3 2023/04/05

TRENDnet®

Product Warranty Registration

Please take a moment to register your product online.
Go to TRENDnet’s website at http://www.trendnet.com/register

TRENDnet
20675 Manhattan Place
Torrance, CA 90501. USA