CERIO Corporation

CS-2648XG

PoE CS-2000 Series - 48 Port 10/100/1000M Gigabit Web Managed Switch with 4 SFP+ 10Gigabit Ports

User Manual

Default IP / Login Information	
IP Address	192.168.2.200
User Name	root
Password	default

FCC Warning

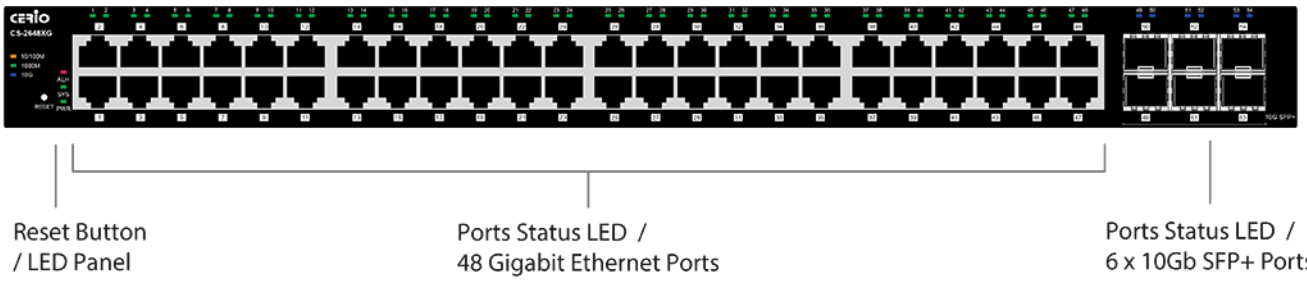
This device has been tested and found to comply with limits for a Class A digital device, pursuant to Part 2 and 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiates radio frequency energy and, if not installed and used in accordance with the user's manual, may cause interference in which case user will be required to correct the interference at his own expense.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user many be required to take adequate measures.

1. Exterior

1.1 Front Panel



1.2 Rear Panel Layout

Status LED lights for 48 Port 10/100/1000Mps with 4 SFP+ 10Gigabit Ports

Per Port: Link / Activity Status
SFP+ 10G Port: SFP+ Connection Status
Per Unit: (ALH) Overheating/Volt error Alarm
Per Unit: (PWR)
Per Unit: (SYS)

AC input (100-240V/AC, 50-60Hz) UL safety.

.

2. Software Configuration

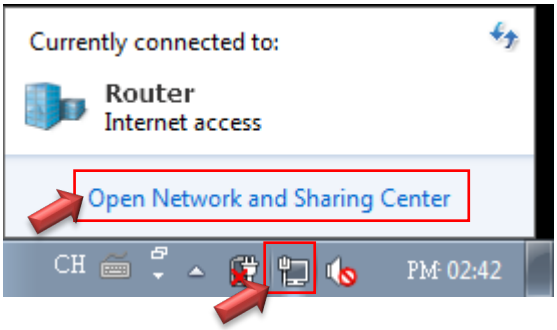
CS-2648XG supports web-based configuration. Upon the completion of hardware installation, The Switch can be configured through a PC/NB by using its web browser such as Internet Explorer 6.0 or later.

Set the IP segment of the administrator's computer to be in the same range as **CS-2648XG** for accessing the system. Do not duplicate the IP Address used here with IP Address of **CS-2648XG** or any other device within the network. ***Please refer to the following steps***

2.1 Example of Segment: (Windows OS)

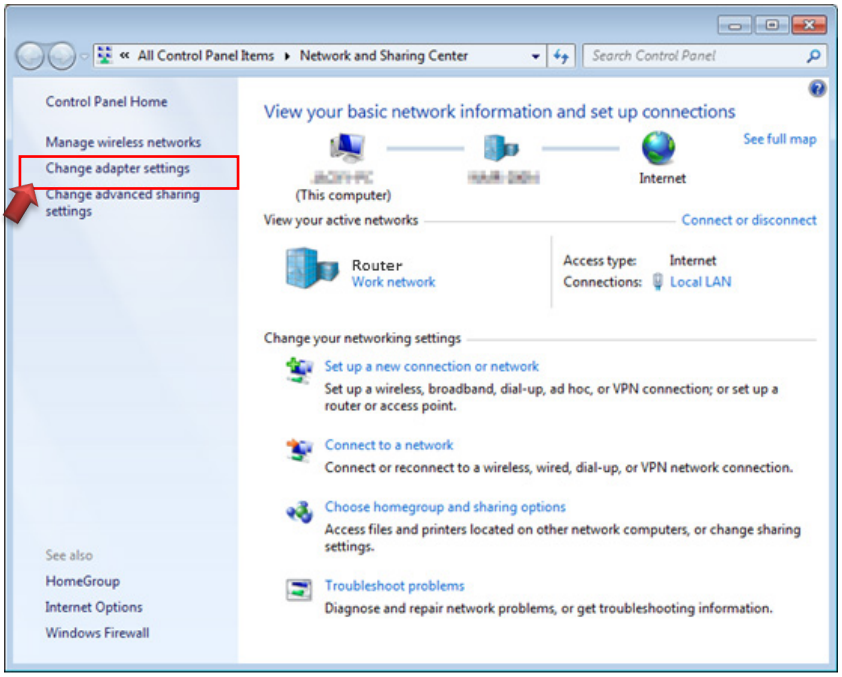
Step 1 :

Please click on the computer icon in the bottom right window, and click **"Open Network and Sharing Center"**



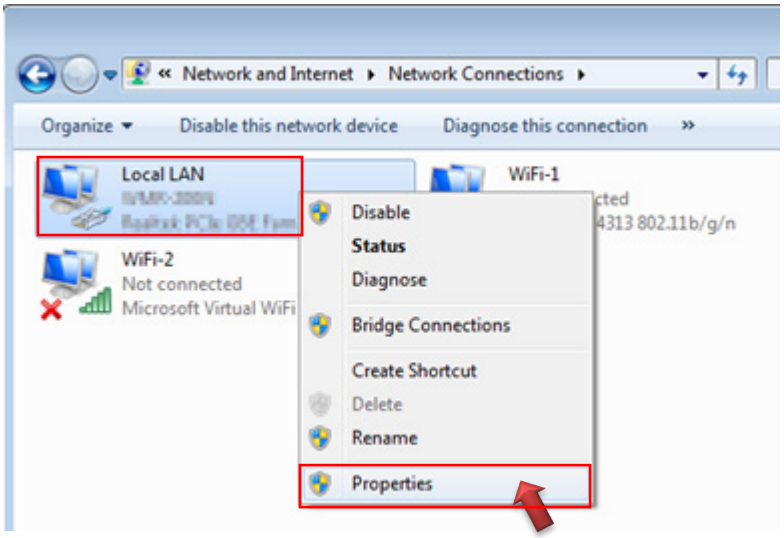
Step 2 :

In the Network and Sharing Center page, click on the left side of **"Change adapter setting"** button



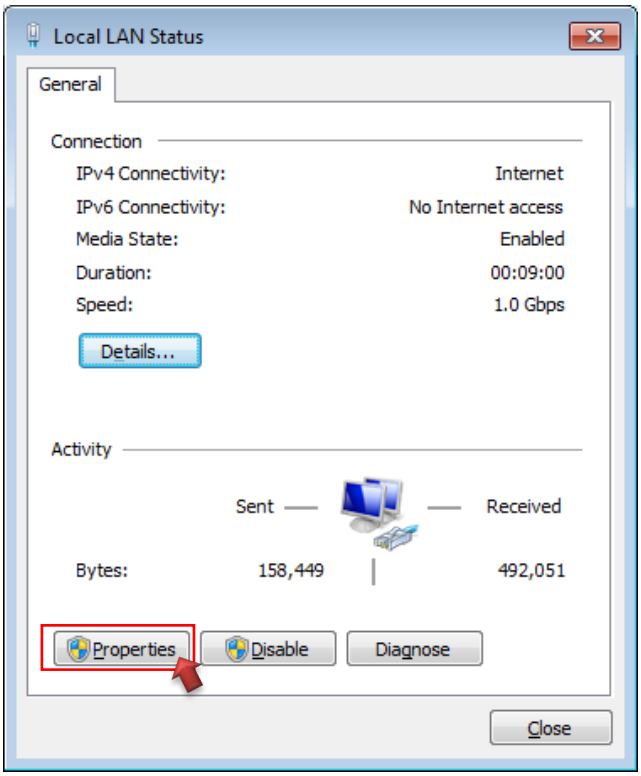
Step 3 :

In **“Change adapter setting”** Page, right click on Local LAN then select **“Properties”**



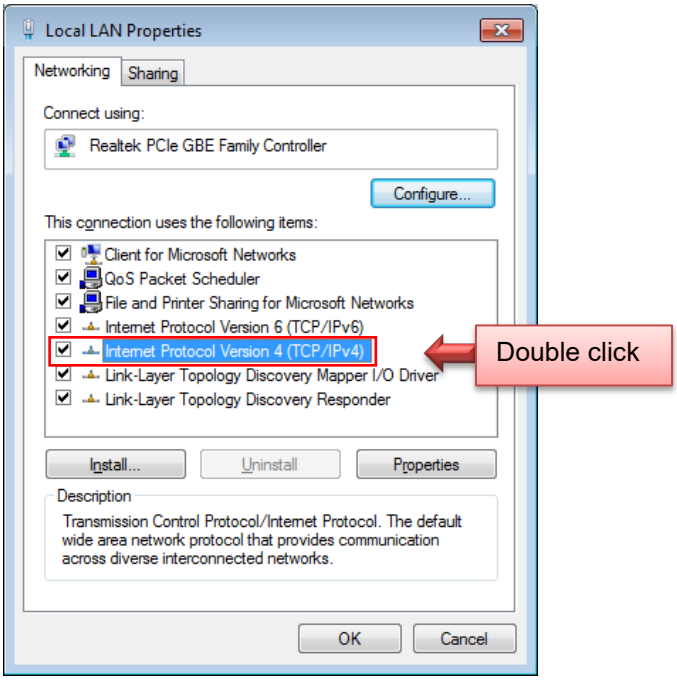
Step 4 :

In the **“Properties”** page, click the **“Properties”** button to open TCP/IP setting



Step 5 :

In Properties page for setting IP addresses, find **"Internet Protocol Version 4 (TCP/IPv4)"** and double click to open TCP/IPv4 Properties window



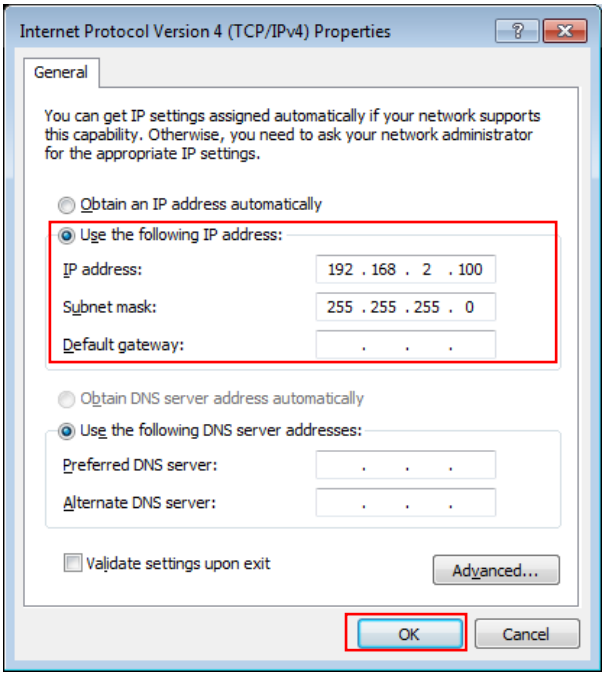
Step 6 :

Select **"Use the following IP address"**, and fix in IP Address to: 192.168.2.X

ex. The X is any number from 1 to 253

Subnet mask : 255.255.255.0

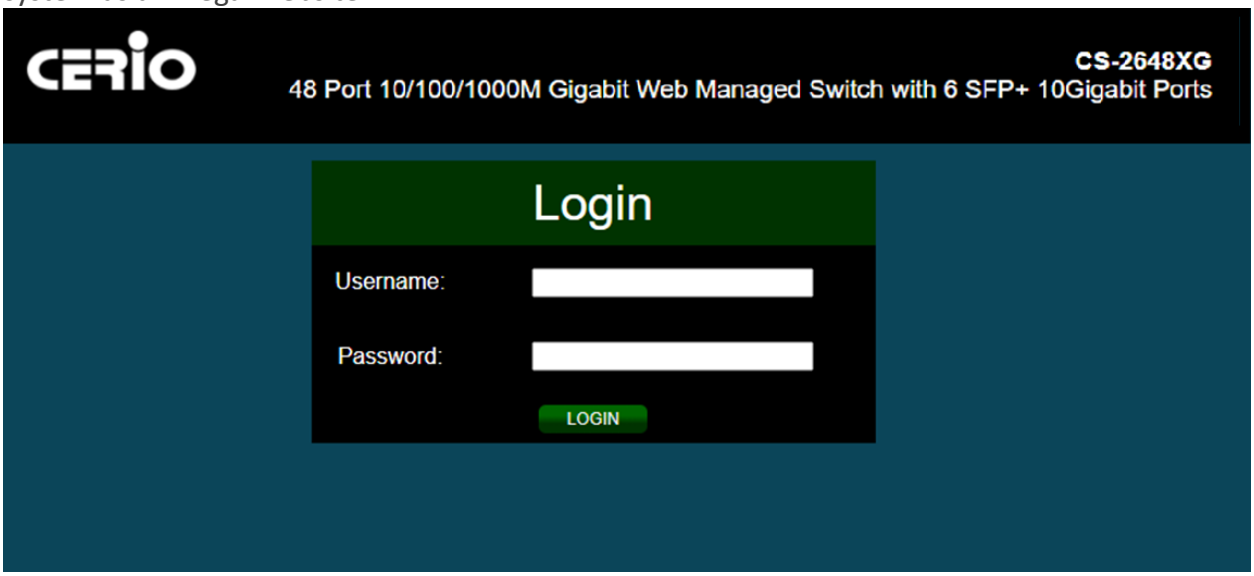
And Click **"OK"** to complete fixing the computer IP settings



Step 7 :

Open Web Browser

Without a valid certificate, users may encounter the following problem in IE7 when they try to access system's WMI (http://192.168.2.200). There will be a “Certificate Error”, because the browser treats system as an illegal website.



System login Overview page will appear after successful login.

2.2 System login username and password information

The **CS-2648XG** web switch default IP is 192.168.2.200
Into the management page as follows, please enter Username and password

- **Default IP Address**: 192.168.2.200
- **Default Username and Password**

Management Account	Root Account
Username	root
Password	default

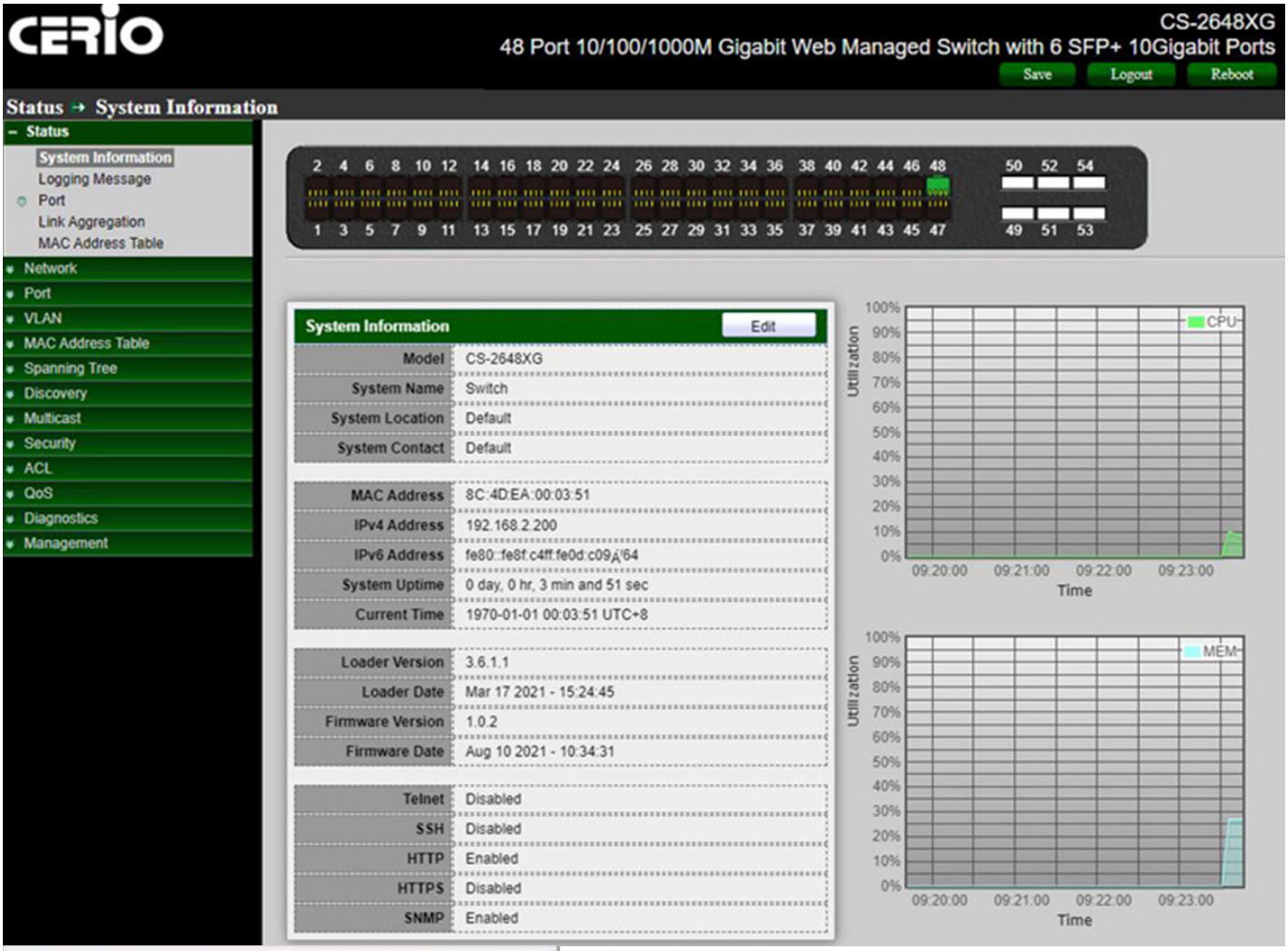
After the authentication procedure, the home page will show up. Select one of the configurations by clicking the icon.

Status

2.3 System Information

Administrator can check this page shows switch panel, CPU utilization, Memory utilization and other system current information. It also allows user to edit some system information.

Note	In the Web UI, the left column shows the configuration menu. The top row shows the switch’s current link status. Green squares indicate the port link is up, while black squares indicate the port link is down. Below the switch panel, you can find a common toolbar to provide useful functions for users. The rest of the screen area displays the configuration settings.

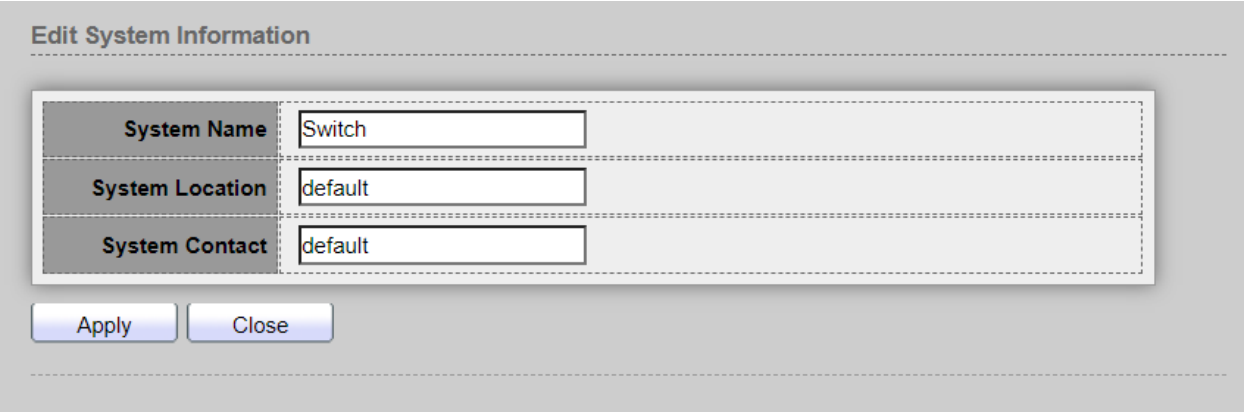


System Information
Edit
Model CS-2648XG
System Name Switch
System Location Default
System Contact Default
MAC Address 8C:4D:EA:00:03:51
IPv4 Address 192.168.2.200
IPv6 Address fe80::fe8f:c4ff:fe0d:c09Ä'64
System Uptime 0 day, 0 hr, 3 min and 51 sec
Current Time 1970-01-01 00:03:51 UTC+8
Loader Version 3.6.1.1
Loader Date Mar 17 2021 - 15:24:45
Firmware Version 1.0.2
Firmware Date Aug 10 2021 - 10:34:31
Telnet Disabled
SSH Disabled
HTTP Enabled
HTTPS Disabled
SNMP Enabled

Field	Description
Model	Model name of the switch.
System Name	System name of the switch. This name will also use as CLI prefix of each line. (“Switch>” or “Switch#”)
System Location	Location information of the switch.
System Contact	Contact information of the switch.
MAC Address	Base MAC address of the switch.
IPv4 Address	Current system IPv4 address.
IPv6 Address	Current system IPv6 address.
System OID	SNMP system object ID.
System Uptime	Total elapsed time from booting.
Current Time	Current system time.
Loader Version	Boot loader image version.
Loader Date	Boot loader image build date.
Firmware Version	Current running firmware image version.
Firmware Date	Current running firmware image build date.
Telnet	Current Telnet service enable/disable state.
SSH	Current SSH service enable/disable state.
HTTP	Current HTTP service enable/disable state.
HTTPS	Current HTTPS service enable/disable state.
SNMP	Current SNMP service enable/disable state.
Consuming Power	Current POE Power Consuming state.

Edit System Information

Administrator can click “Edit” button on the table title to edit following system information.

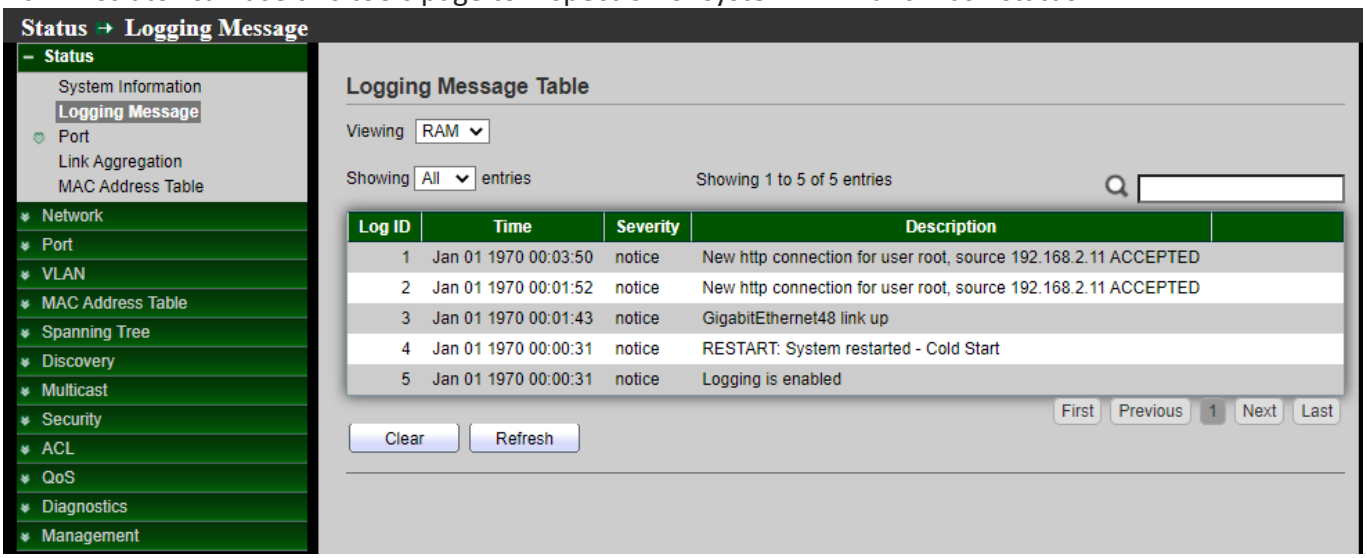


- **System Name:** System name of the switch. This name will also use as CLI prefix of each line. (“Switch>” or “Switch#”).
- **System Location:** Location Location information of the switch.
- **System Contact:** Contact information of the switch.

*Click the **“Apply”** button to save your changes or **“Close”** the button to close settings.*

2.4 Logging Message

Administrator can use this tools page to Inspection of system RAM and Flash status.



- **Viewing:** The logging view including:
  - **RAM:** Show the logging messages stored on the RAM.
  - **Flash:** Show the logging messages stored on the Flash.

Field	Description
Log ID	The log identifier.
Time	The time stamp for the logging message.
Severity	The severity for the logging message.
Description	The description of logging message.

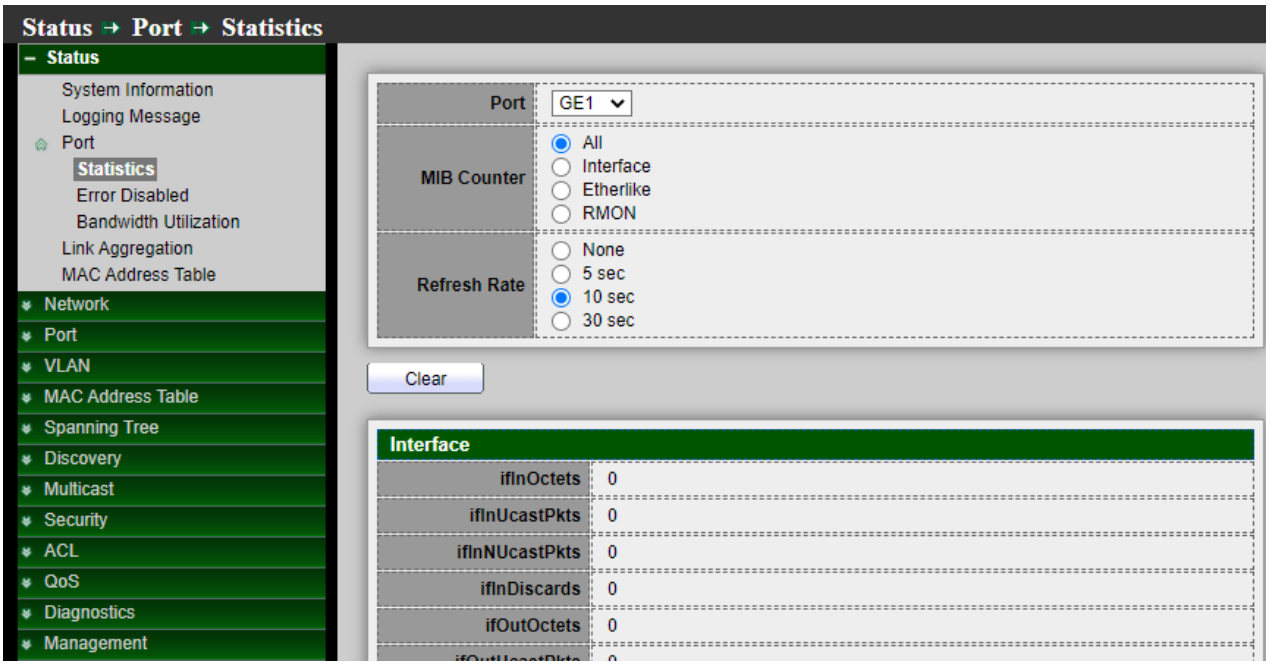
*Click the **"Clear"** button to clear this page or click the **"Refresh"** button to refresh the page .*

2.5 Port

Display detailed port summary and status information for each port.

2.5.1 Statistics

Administration can choose to view displays standard counters on network traffic form the Interfaces, Ethernet-like and RMON MIB. Interfaces and Ethernet-like counters display errors on the traffic passing through each port. RMON counters provide a total count of different frame types and sizes passing through each port. The **"Clear"** button will clear MIB counter of current selected port.



*Click the **"Clear"** button to clear this page.*

Interface	
ifInOctets	1226044
ifInUcastPkts	8677
ifInNUcastPkts	343
ifInDiscards	0
ifOutOctets	2813449
ifOutUcastPkts	5587
ifOutNUcastPkts	194
ifOutDiscards	0
ifInMulticastPkts	226
ifInBroadcastPkts	117
ifOutMulticastPkts	194
ifOutBroadcastPkts	0

Etherlike	
dot3StatsAlignmentErrors	0
dot3StatsFCSErrors	0
dot3StatsSingleCollisionFrames	0
dot3StatsMultipleCollisionFrames	0
dot3StatsDeferredTransmissions	0
dot3StatsLateCollisions	0
dot3StatsExcessiveCollisions	0
dot3StatsFrameTooLongs	0
dot3StatsSymbolErrors	0
dot3ControlInUnknownOpcodes	0
dot3InPauseFrames	0
dot3OutPauseFrames	0

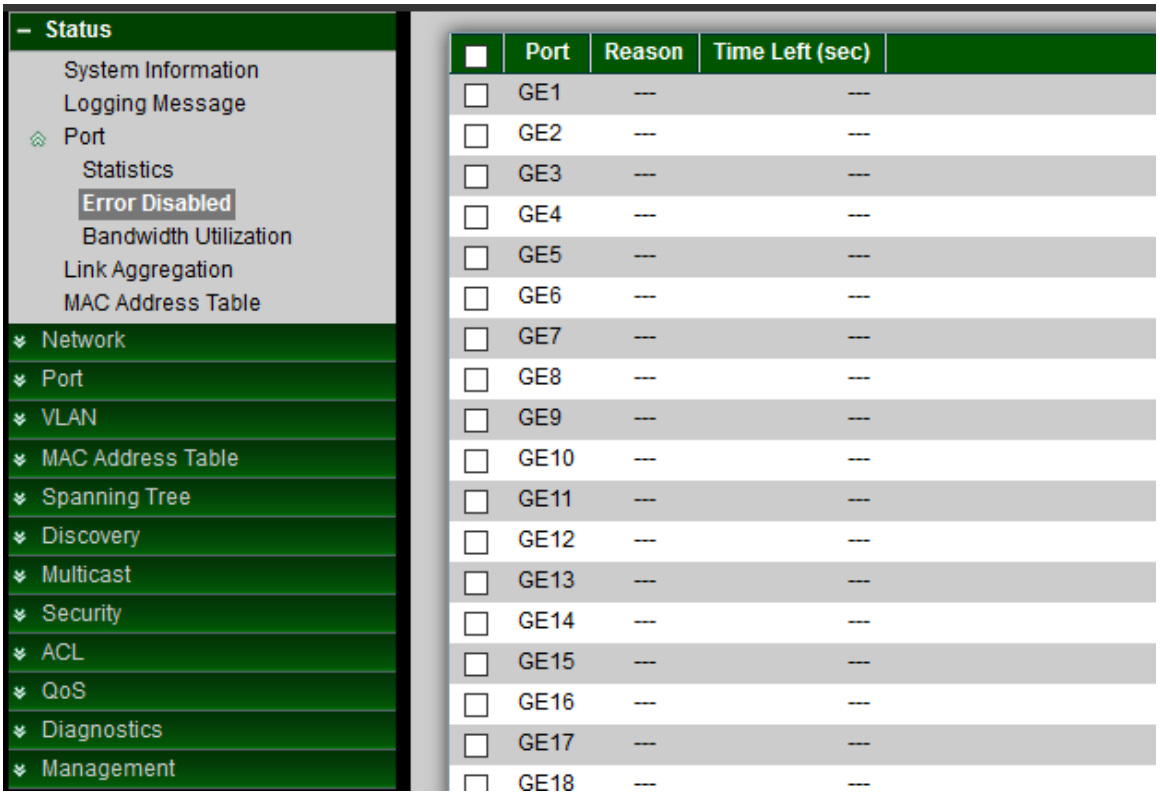
Etherlike page displays statistics per interface according to the Etherlike MIB standard definition. This function provides more detailed information regarding errors in the physical layer (Layer 1).

RMON	
etherStatsDropEvents	0
etherStatsOctets	1236728
etherStatsPkts	9117
etherStatsBroadcastPkts	117
etherStatsMulticastPkts	226
etherStatsCRCAlignErrors	0
etherStatsUnderSizePkts	0
etherStatsOverSizePkts	0
etherStatsFragments	0
etherStatsJabbers	0
etherStatsCollisions	0
etherStatsPkts64Octets	6502
etherStatsPkts65to127Octets	1080
etherStatsPkts128to255Octets	122
etherStatsPkts256to511Octets	1251
etherStatsPkts512to1023Octets	150
etherStatsPkts1024to1518Octets	12

- **Port :** Select one port to show counter statistics.
- **MIB Counter :** Select the MIB counter to show different counter type.
  - **All : All counters.**
  - **Interface : Interface related MIB counters.**
  - **Etherlike : Ethernet-like related MIB counters.**
  - **RMON : RMON related MIB counters.**
- **Refresh Rate :** Refresh the web page every period of “None , 5 sec , 10 sec , 30 sec “seconds base to get new counter of specified port.

2.5.2 Error Disabled

If administrator has set Error disabled functions then can monitor information in page.



Field	Description
Port	Interface or port number.

Reason	Port will be disabled by one of the following error reason: • BPDU Guard. • UDLD. • Self Loop. • Broadcast Flood. • Unknown Multicast Flood. • Unicast Flood. • ACL. • Port Security Violation. • DHCP rate limit. • ARP rate limit.
Time Left (sec)	The time left in second for the error recovery.

2.5.3 Bandwidth Utilization

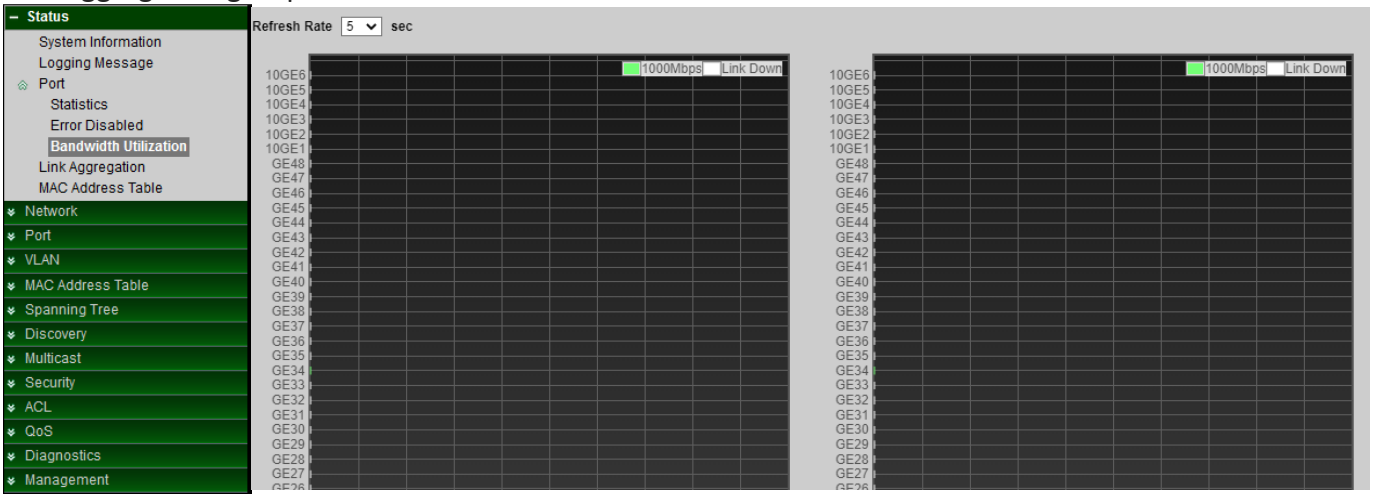
This page can display Tx / Rx Real-time bandwidth information of each port. (Instant used rate per port and this page will refresh automatically in every refresh period)

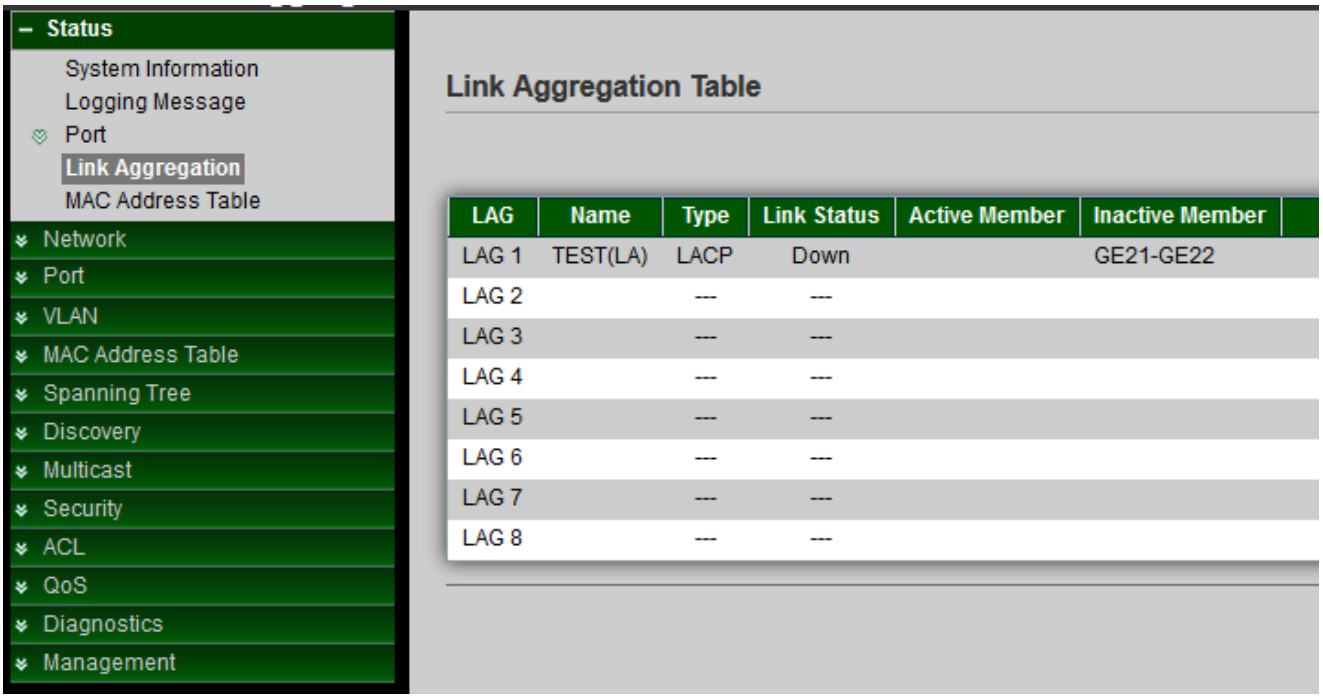
- **Refresh Rate:** Refresh the web page every period of seconds to get new bandwidth utilization Rata.
  - **2 :** Select the 2 second cycle from the drop-down menu to refresh the display page.
  - **5 :** Select the 5 second cycle from the drop-down menu to refresh the display page.

10 : Select the 10 second cycle from the drop-down menu to refresh the display page.

2.6 Link Aggregation

If administrator has set LACP function then this can display LACP information. This system have support 8 Link Aggregation group. Administrator can enable 8 LAG.

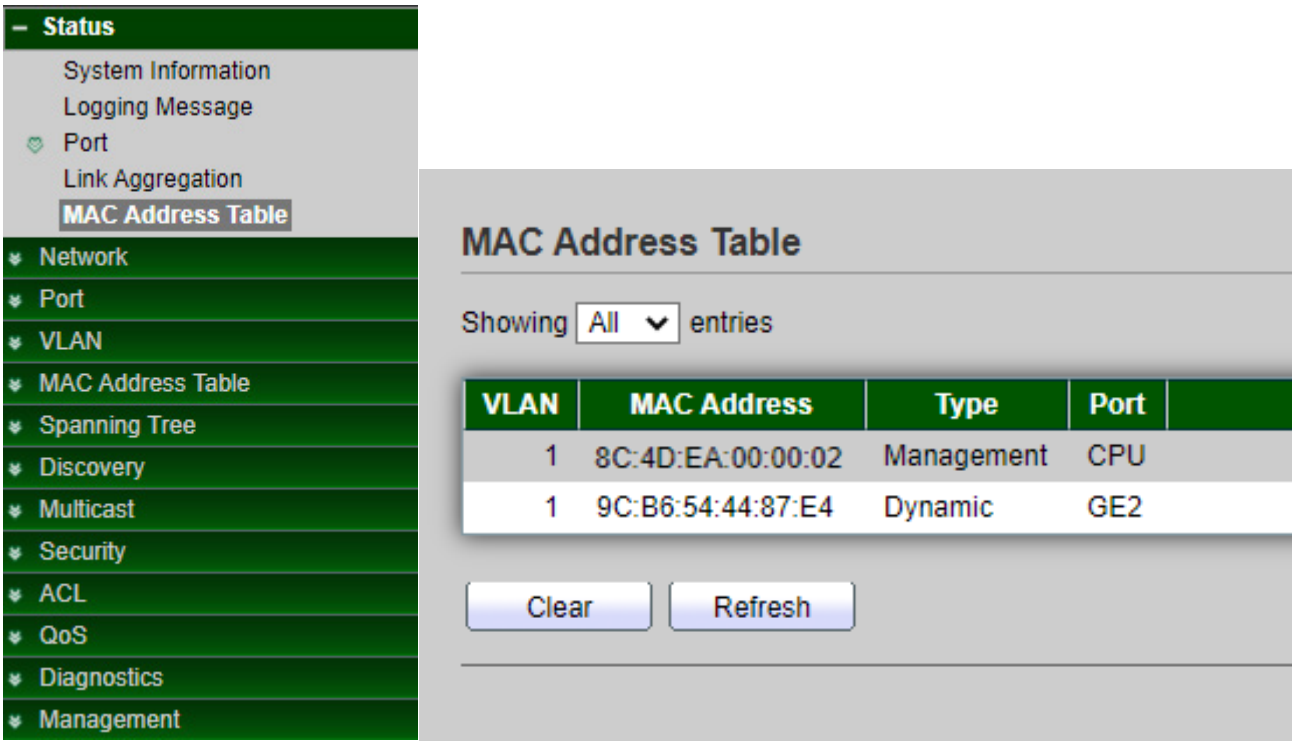




Field	Description
LAG	LAG Name.
Name	LAG port description.
Type	The type of the LAG. • **Static:** The group of ports assigned to a static LAG are always active members. • **LACP:** The group of ports assigned to dynamic LAG are candidate ports. LACP determines which candidate ports are active member ports.
Link Status	LAG port link status.
Active Member	Active member ports of the LAG.
Inactive Member	Inactive member ports of the LAG.

2.7 MAC Address Table

The MAC address table page displays all MAC address entries on the switch including static MAC address created by administrator or auto learned from hardware.
The **"Clear"** button will clear all dynamic entries and **"Refresh"** button will retrieve latest MAC address entries and show them on page.



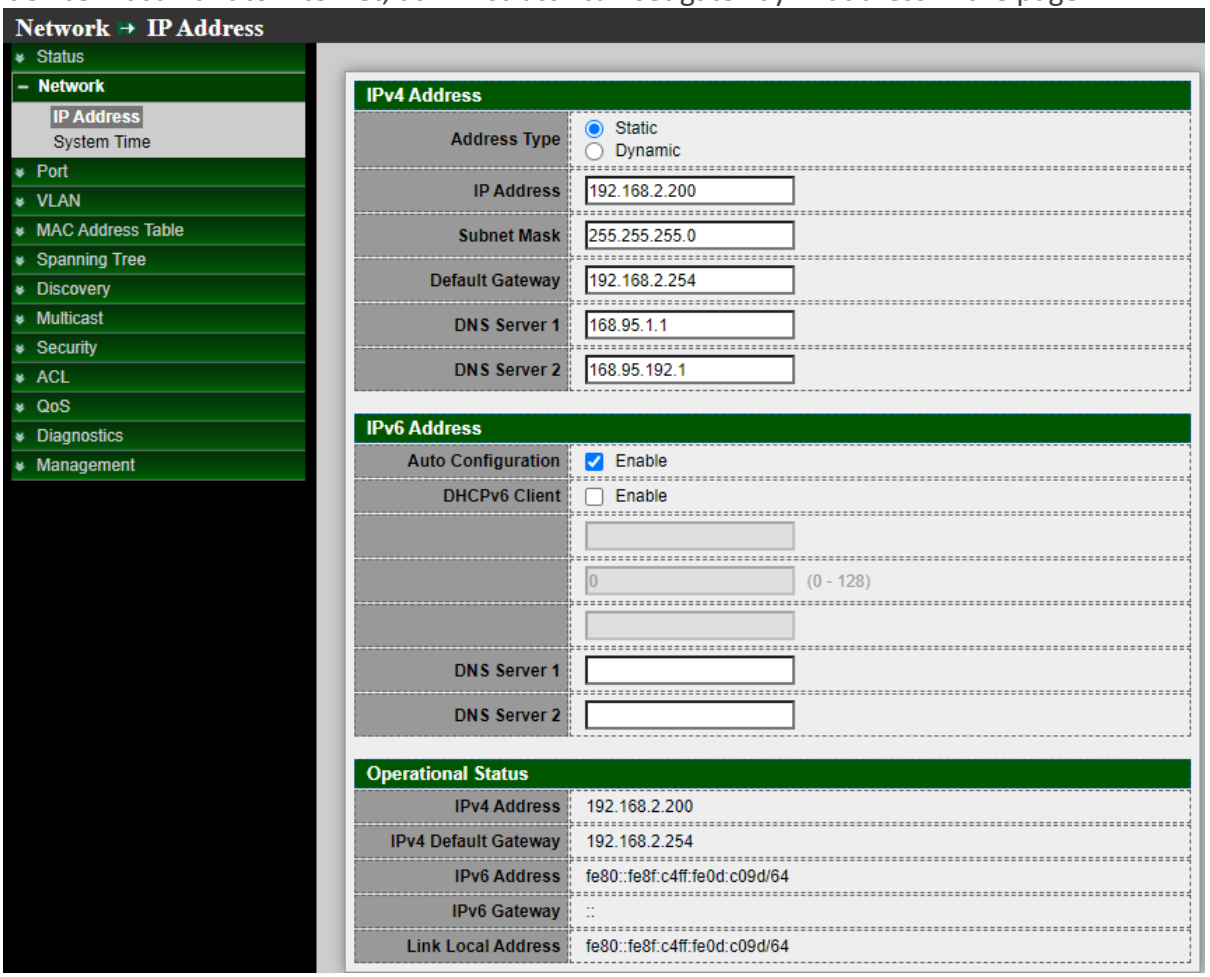
Field	Description
VLAN	VLAN ID of the mac address.
MAC Address	MAC address.
Type	The type of MAC address • **Management:** DUT's base mac address for management purpose. • **Static:** Manually configured by administrator. • **Dynamic:** Auto learned by hardware.
Port	The type of Port. • **CPU:** DUT's CPU port for management purpose. • **Other:** Normal switch port.

*Click the **"Clear"** button to clear this page or click the **"Refresh"** button to refresh the page .*

3. Network

3.1 IP Address

Administrator can set IP address for the system. The IP address support IPv4 & IPv6 protocol, if switch device must want to internet, administrator can set gateway IP address in the page.



IPv4 Address

- **Address Type:** Administrator can select use static or Dynamic IP address in system. If administrator chooses use Dynamic type then switch IP address will be dispatched by the DHCP server.
- **IPv4 Address / subnet / Gateway / DNS1-2:** If used static IP address then administrator can modify this IP address and subnet and gateway and DNS IP address of the system.

IPv6 Address

- **IPv6 Address:** Administrator can choose use Auto Configuration or DHCP Client mode to set IPv6 address.
  If administrator disables Auto Configuration or DHCP Client mode then administrator can manual setting IPv6 address.

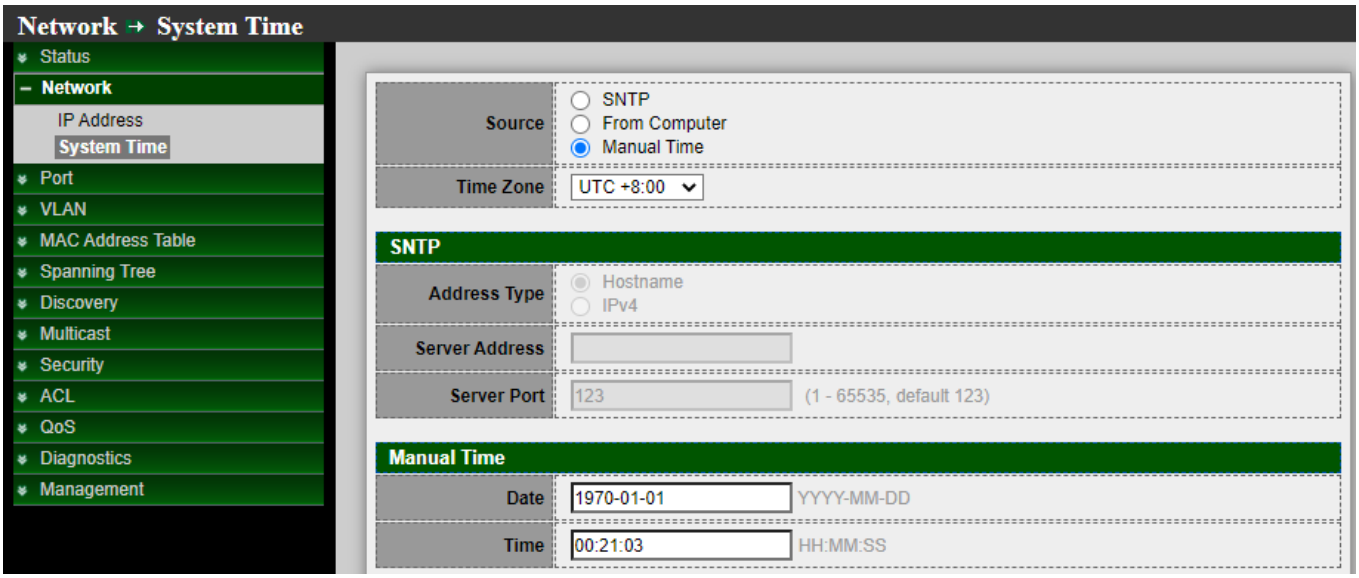
Operational Status

This information can display the current used IPv4/v6 address and gateway of the switch.

*Click the **"Apply"** button to save your changes or click the **"Clear"** button to refresh the page .*

3.2 System Time

System time can be configured via this page. Administrator can select SNTP Server or from computer to update the system time or administration can use manual setting the system time.
Note. If administrator chooses SNTP Server to synchronization update time then must confirm system gateway and DNS is correct and switch system must be able to connect to the SNTP Server.



System Time

- **Source:** Select the time source.
  - **SNTP:** Time sync from NTP server.
  - **From Computer:** Time set from browser host.
  - **Manual Time:** Time set by manually configure.
- **Time Zone:** Select a time zone difference from listing district.

SNTP

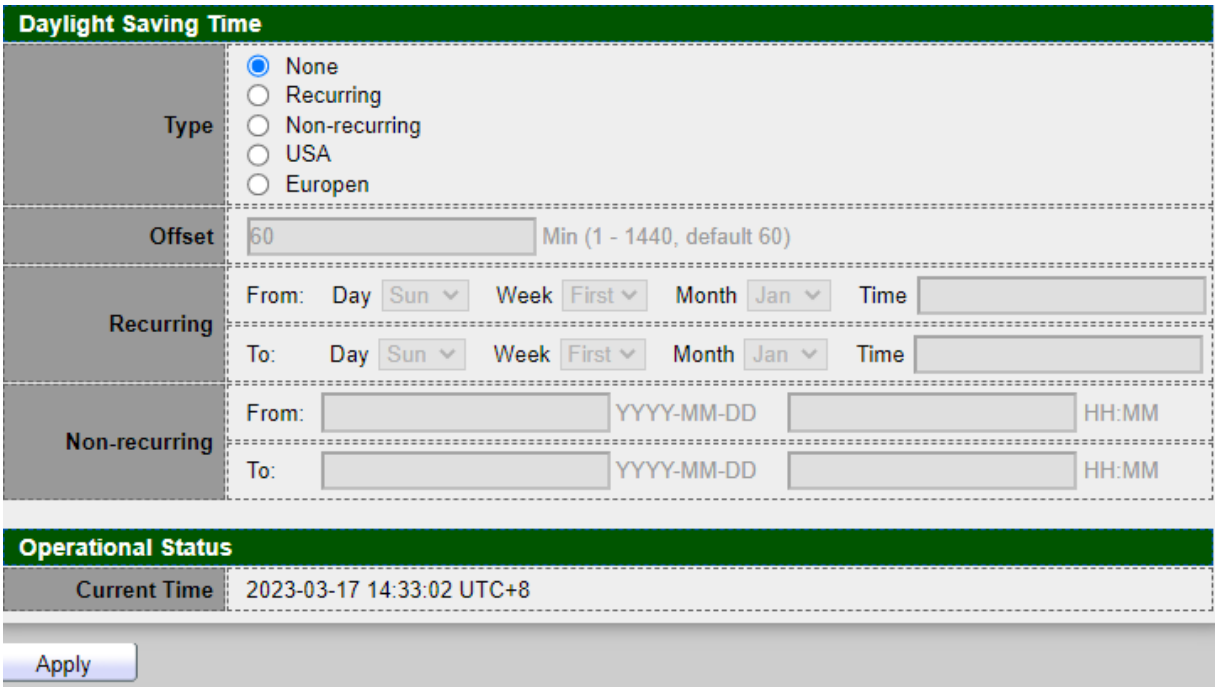
- **Address Type:** Select the address type of NTP server. This is enabled when time source is SNTP.
- **Server Address:** Input IPv4 address or hostname for NTP server. This is enabled when time Source is SNTP.
- **IPv6 Address:** Input NTP port for NTP server. Default is 123. This is enabled when time source is SNTP.

Manual Time

- **Date:** Input manual date. This is enabled when time source is manual.
- **Time:** Input manual time. This is enabled when time source is manual.

Daylight Saving Time

The Switch support Daylight saving time function, if administrator need enable and set the Daylight saving time function will can be enable this function.



- **Type:** Select the mode of daylight saving time.
  - **Disable:** Disable daylight saving time.
  - **Recurring:** Using recurring mode of daylight saving time.
  - **Non-Recurring:** Using non-recurring mode of daylight saving time.
  - **USA:** Using daylight saving time in the United States that starts on the second Sunday of March and ends on the first Sunday of November.
  - **European:** Using daylight saving time in the Europe that starts on the last Sunday in March and ending on the last.
- **Offset :** Specify the adjust offset of daylight saving time.
- **Recurring From:** Specify the starting time of recurring daylight saving time. This field available when selecting “Recurring” mode.
- **Recurring To:** Specify the ending time of recurring daylight saving time. This field available when selecting “Recurring” mode.
- **Non-recurring From:** Specify the starting time of non-recurring daylight saving time. This field available when selecting “Non-Recurring” mode.
- **Non recurring To:** Specify the ending time of recurring daylight saving time. This field available when selecting “Non-Recurring” mode.

Operational Status

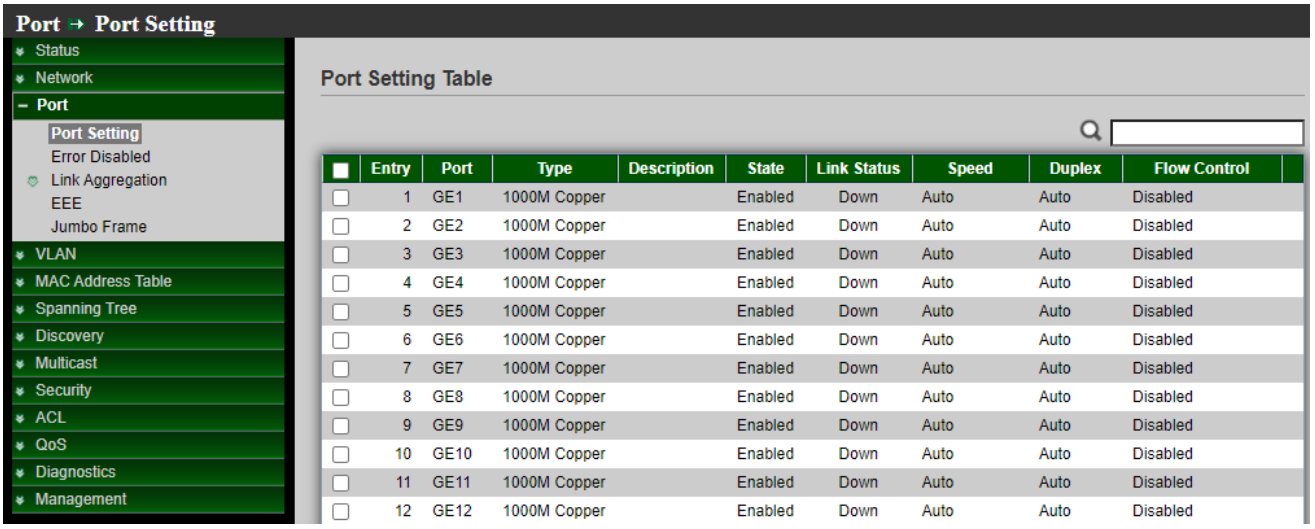
Current Time: Display the current operating time

*Click the **“Apply”** button to save your changes settings.*

4. Port

4.1 Port setting

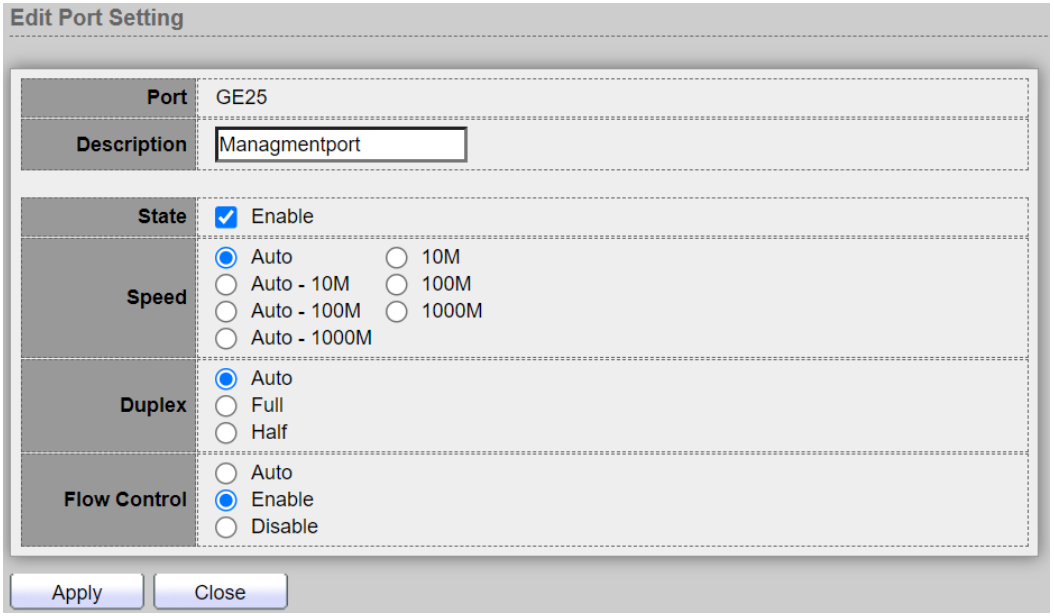
This page shows port current status and allow user to edit port configurations. Select port entry and click **"Edit"** button to edit port configurations.



Entry	Port	Type	Description	State	Link Status	Speed	Duplex	Flow Control
1	GE1	1000M Copper		Enabled	Down	Auto	Auto	Disabled
2	GE2	1000M Copper		Enabled	Down	Auto	Auto	Disabled
3	GE3	1000M Copper		Enabled	Down	Auto	Auto	Disabled
4	GE4	1000M Copper		Enabled	Down	Auto	Auto	Disabled
5	GE5	1000M Copper		Enabled	Down	Auto	Auto	Disabled
6	GE6	1000M Copper		Enabled	Down	Auto	Auto	Disabled
7	GE7	1000M Copper		Enabled	Down	Auto	Auto	Disabled
8	GE8	1000M Copper		Enabled	Down	Auto	Auto	Disabled
9	GE9	1000M Copper		Enabled	Down	Auto	Auto	Disabled
10	GE10	1000M Copper		Enabled	Down	Auto	Auto	Disabled
11	GE11	1000M Copper		Enabled	Down	Auto	Auto	Disabled
12	GE12	1000M Copper		Enabled	Down	Auto	Auto	Disabled

Field	Description
Port	Display for Port Name.
Type	Display for Port media type.
Description	Display custom port description.
State	Display for Port admin state. • **Enabled:** Enable the port. • **Disabled:** Disable the port.
Link Status	Current port link status. • **Up:** Port is link up. • **Down:** Port is link down.
Speed	Current port speed configuration and link speed status.
Duplex	Current port duplex configuration and link duplex status.
Flow Control	Current port flow control configuration and link flow control status.

Administrator can set speed / Duplex / Flow Control by each port.
Please select port number in checkbox and click apply button to set speed / Duplex / Flow Control of each port.



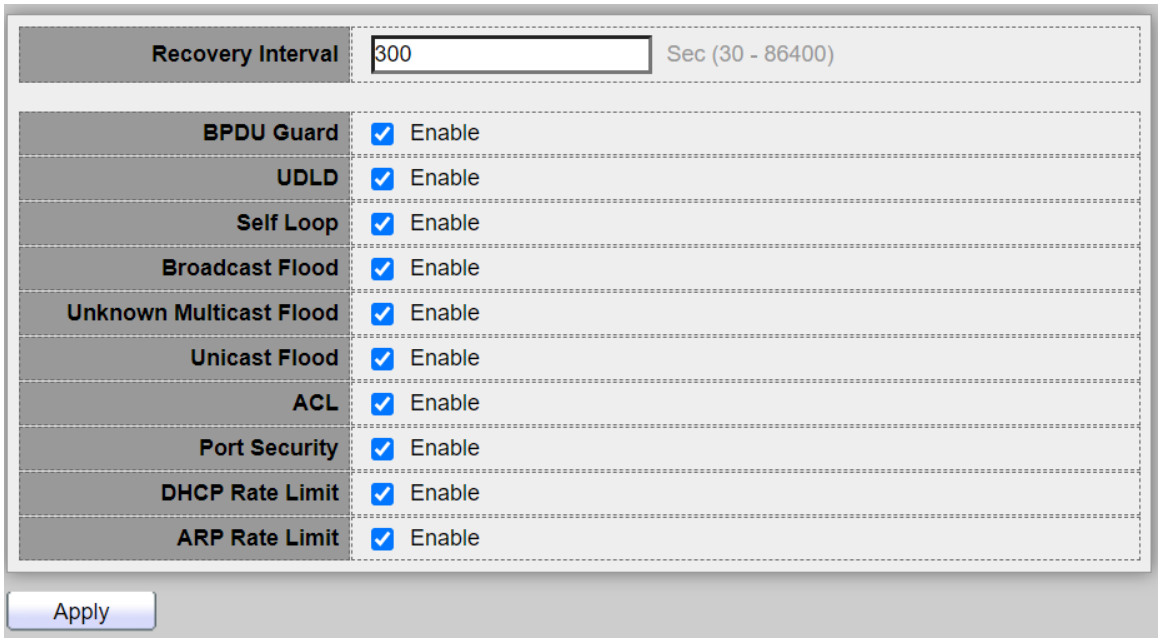
- **Port:** Selected port list.
- **Description:** Custom port description
- **State:** Port admin state.
  - **Enabled:** Enable the port.
  - **Disabled:** Disable the port.
- **Speed:** Port speed capabilities.
  - **Auto:** Auto speed with all capabilities
  - **Auto-10M:** Auto speed with 10M ability only
  - **Auto-100M:** Auto speed with 100M ability only
  - **Auto-1000M:** Auto speed with 1000M ability only
  - **Auto-10M/100M:** Auto speed with 10M/100M abilities
  - **10M:** Force speed with 10M ability
  - **100M:** Force speed with 100M ability
  - **1000M:** Force speed with 1000M ability
- **Duplex:** Port duplex capabilities.
  - **Auto:** Auto duplex with all capabilities
  - **Half:** Auto speed with 10M and 100M ability only
  - **Full:** Auto speed with 10M/100M/1000M ability only
- **Flow Control:** Port flow control.
  - **Auto:** Auto flow control by negotiation
  - **Enabled:** Enable flow control ability
  - **Disabled:** Disable flow control ability

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

4.2 Error Disabled

This function can block of faulty operation, including EPDU Guard / UDLD / Self Loop / Broadcast Flood / Unknown Multicast Flood / Unicast Flood / ACL / Port Security / DHCP Rate Limit / ARP Rate Limit etc.

After administrator enable this functions, if occur error in table functions then system will auto immediate block of faulty operation until the after the set time, system will auto re-enable.



- **Recovery Interval:** Auto recovery after this interval for error disabled port.
- **BPDU Guard:** Enabled to auto shutdown port when BPDU Guard reason occur.
  *This reason caused by STP BPDU Guard mechanism.
- **UDLD:** Enabled to auto shutdown port when UDLD violation occur.
- **Self Loop:** Enabled to auto shutdown port when Self Loop reason occur.
- **Broadcast Flood:** Enabled to auto shutdown port when Broadcast Flood reason occur.
  *This reason caused by broadcast rate exceed broadcast storm control rate.
- **Unknown Multicast Flood:** Enabled to auto shutdown port when Unknown Multicast Flood reason occur. This reason caused by unknown multicast rate exceed unknown multicast storm control rate.
- **Unicast Flood:** Enabled to auto shutdown port when Unicast Flood reason occur.
  *This reason caused by unicast rate exceed unicast storm control rate.
- **ACL:** Enabled to auto shutdown port when ACL shutdown port reason occur.
  * This reason caused packet match the ACL shutdown port action**.**
- **Port Security:** Enabled to auto shutdown port when Port Security Violation reason occur.
  *This reason caused by violation port security rules.
- **DHCP rate limit:** Enabled to auto shutdown port when DHCP rate limit reason occur.
  *This reason caused by DHCP packet rate exceed DHCP rate limit.
- **ARP rate limit:** Enabled to auto shutdown port when ARP rate limit reason occur.
  *This reason caused by DHCP packet rate exceed ARP rate limit.

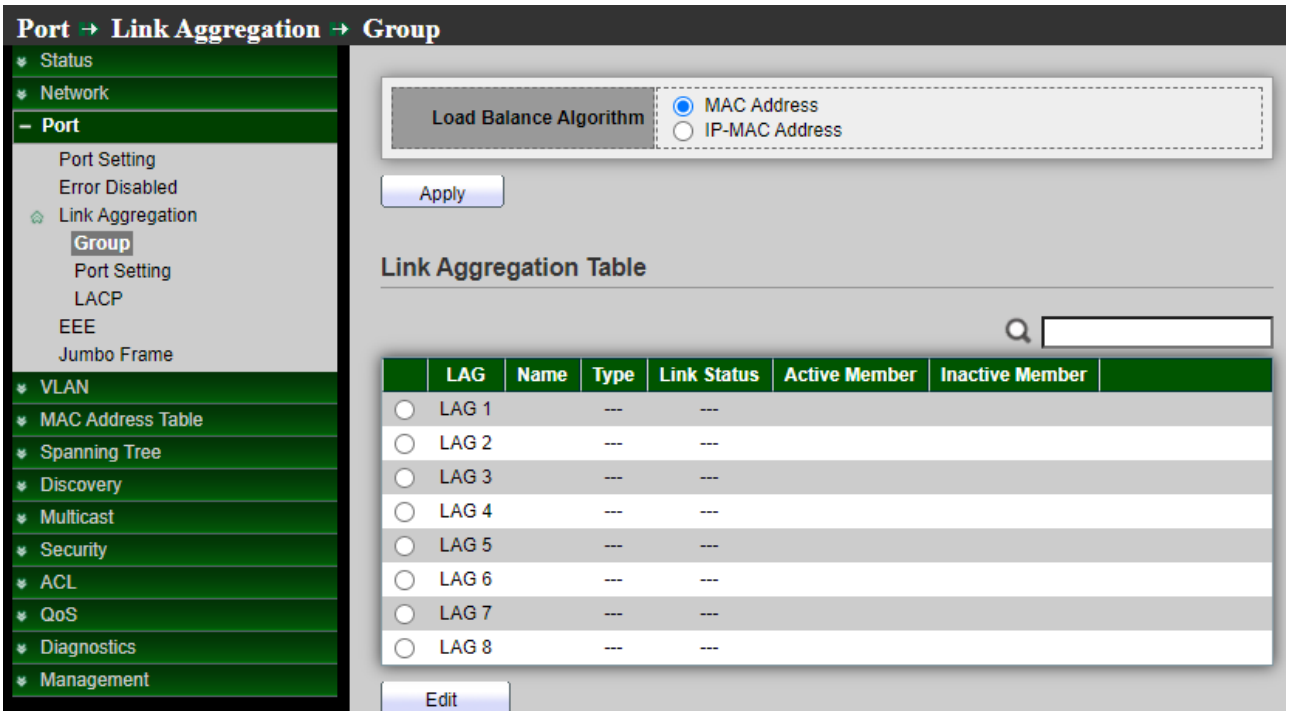
*Click the **"Apply"** button to save your changes settings.*

4.3 Link Aggregation

Link Aggregation is also referred to as link aggregation, teaming port, and port trunk for 802.3ad (LACP, Link Aggregation Control Protocol), The Port Aggregation can aggregate multiple Ethernet ports together to form a logical aggregation group. To upper layer entities, all the physical links in an aggregation group are a single logical link.

4.3.1 Group Configuration

Administrator can select use MAC Address or IP-MAC address of load balance Algorithm.
This system default can set 8 LA group, administrator can select LAG number and click Edit button go to set LA used ports.

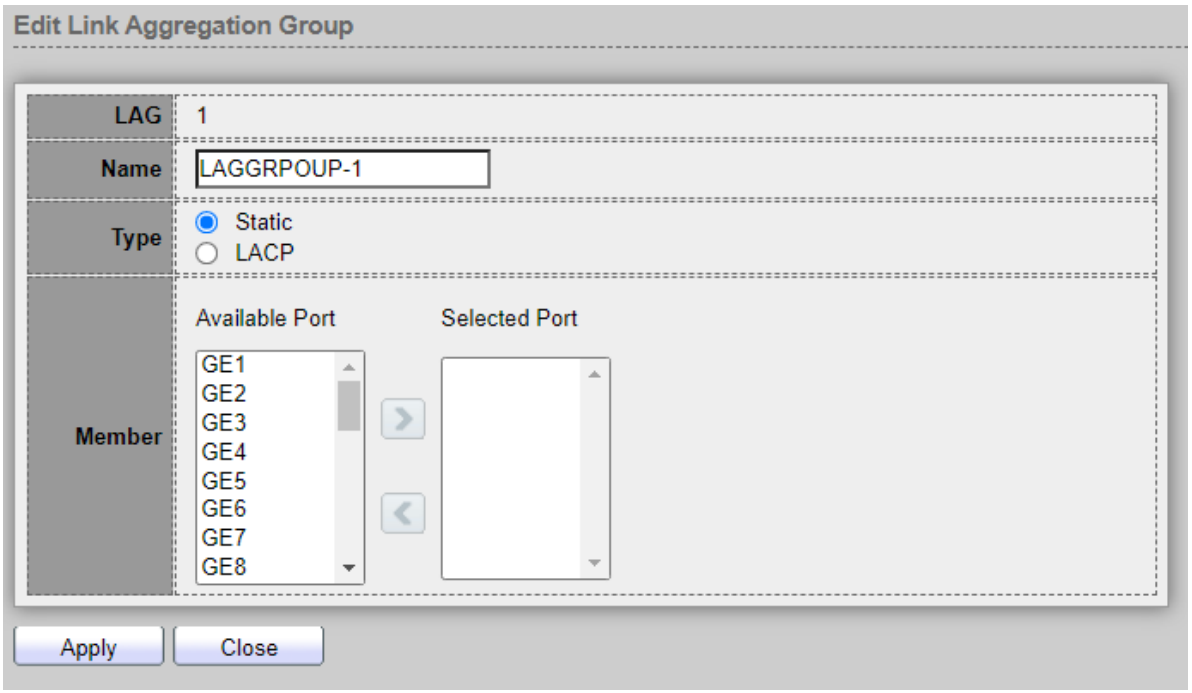


- **Load Balance Algorithm:** LAG load balance distribution algorithm.
  - **MAC Address:** Based on MAC address.
  - **IP-MAC Address:** Based on MAC address and IP address.

*Click the **"Apply"** button to save your changes settings.*

Field	Description
LAG	LAG Name.
Name	LAG port description.

Type	The type of the LAG. • **Static:** The group of ports assigned to a static LAG are always active members. • **LACP:** The group of ports assigned to dynamic LAG are candidate ports. LACP determines which candidate ports are active member ports.
Link Status	LAG port link status.
Active Member	Active member ports of the LAG.
Inactive Member	Inactive member ports of the LAG.

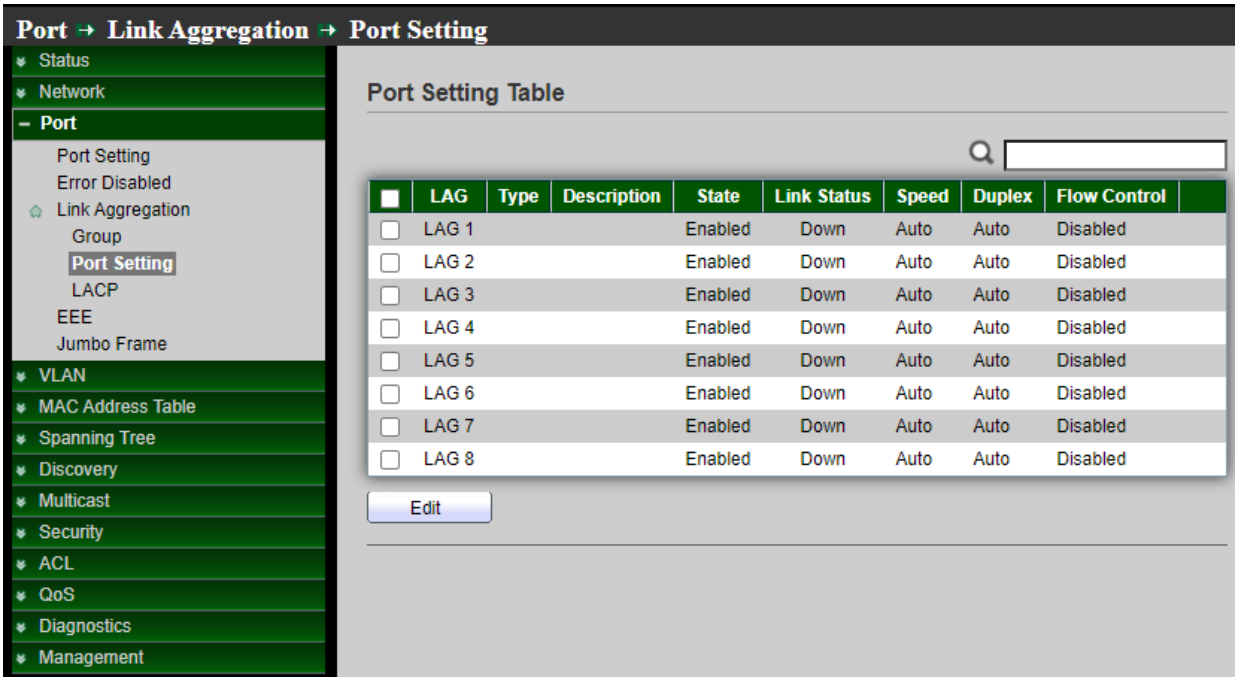


- **LAG:** Selected LAG group ID.
- **Name:** LAG port description.
- **Type:** The type of the LAG.
  - **Static:** The group of ports assigned to a static LAG are always active members.
  - **LACP:** The group of ports assigned to dynamic LAG are candidate ports. LACP determines which candidate ports are active member ports.
- **Member:** Select available port to be LAG group member port.

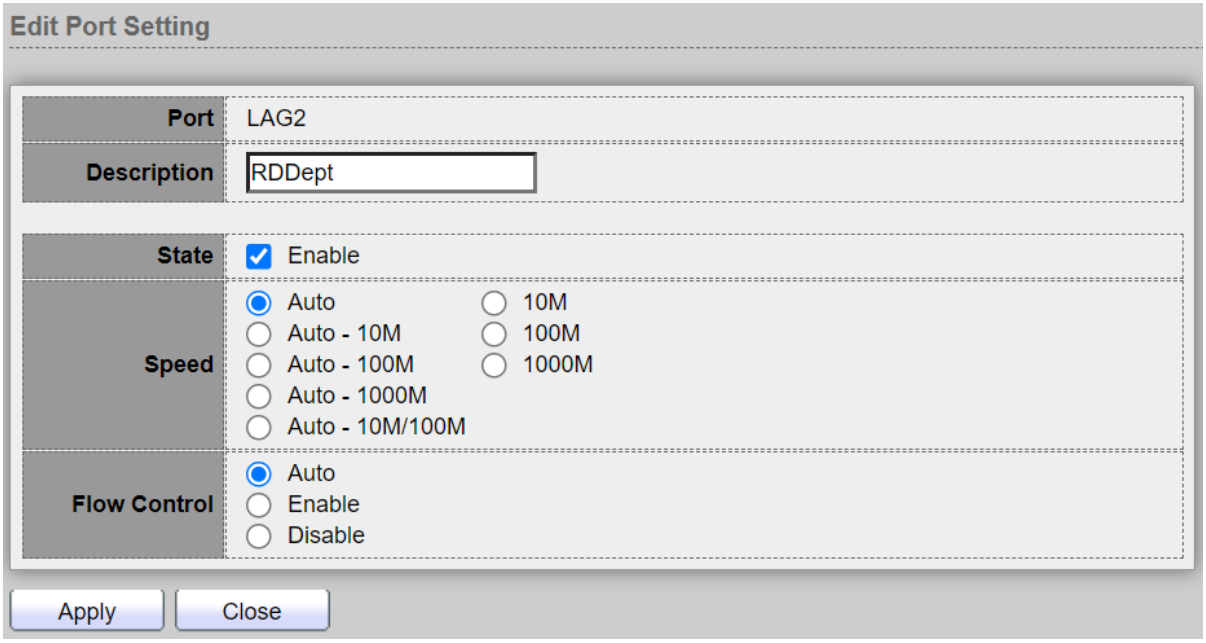
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

4.3.2 Port Setting

This page shows LAG port current status and allow user to edit LAG port configurations. Select LAG entry and click “Edit” button to edit LAG port configurations.



Field	Description
LAG	Display for LAG Port Name.
Type	Display for LAG Port media type.
Description	Display custom LAG Port description.
State	LAG Port admin state. • **Enabled:** Enable the port. • **Disabled:** Disable the port.
Link Status	Current LAG port link status. • **Up:** Port is link up. • **Down:** Port is link down.
Speed	Current LAG port speed configuration and link speed status.
Duplex	Current LAG port duplex configuration and link duplex status.
Flow Control	Current LAG port flow control configuration and link flow control status.

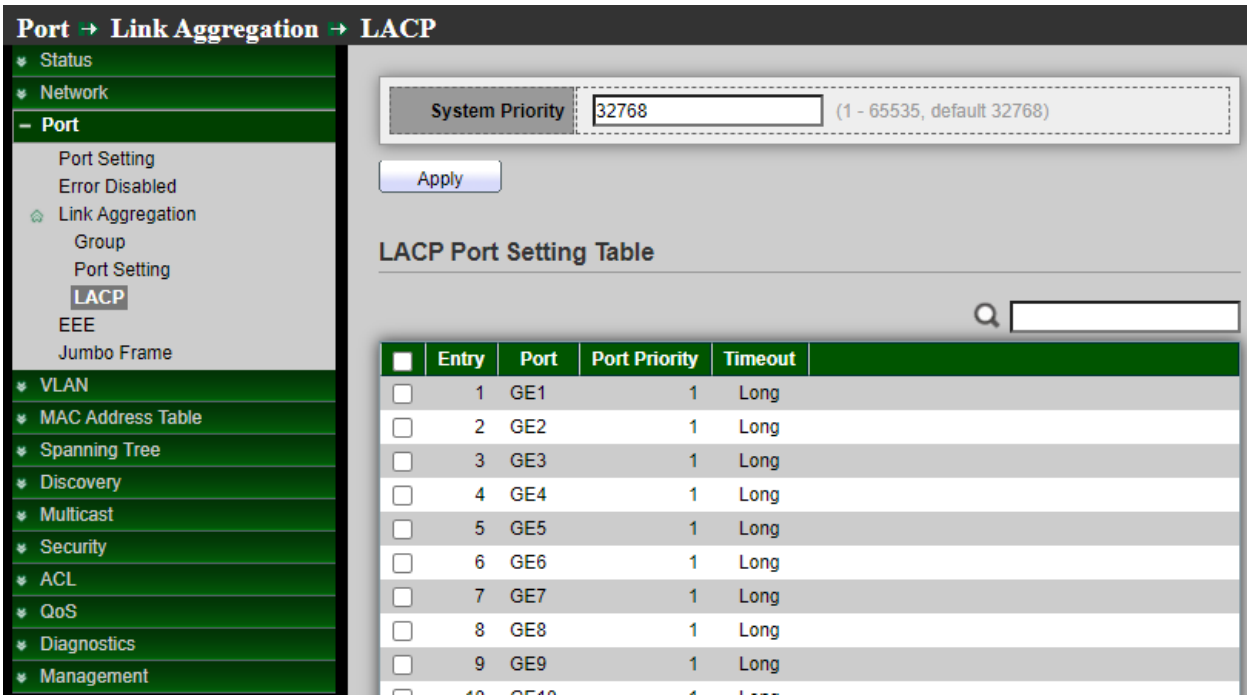


- **Port:** Selected port list.
- **Description:** Custom LAG Port description.
- **State:** Port admin state.
  - **Enabled:** Enable the port.
  - **Disabled:** Disable the port.
- **Speed:** Port speed capabilities.
  - **Auto:** Auto speed with all capabilities
  - **Auto-10M:** Auto speed with 10M ability only
  - **Auto-100M:** Auto speed with 100M ability only
  - **Auto-1000M:** Auto speed with 1000M ability only
  - **Auto-10M/100M:** Auto speed with 10M/100M abilities
  - **10M:** Force speed with 10M ability
  - **100M:** Force speed with 100M ability
  - **1000M:** Force speed with 1000M ability
- **Flow Control:** Port flow control.
  - **Auto:** Auto flow control by negotiation
  - **Enabled:** Enable flow control ability
  - **Disabled:** Disable flow control ability

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

4.3.3 LACP

The LACP can aggregate multiple Ethernet ports together to form a logical aggregation group. To upper layer entities, all the physical links in an aggregation group are a single logical link.
Administrator can to configure LACP global and port configurations. Select ports and click "Edit" button to edit port configuration.



- **System Priority:** Administrator configures the LACP system priority on each switch running LACP. LACP uses the system priority with the switch MAC address to form the system ID and also during negotiation with other switches. This decides the system priority field in LACP PDU.

*Click the **"Apply"** button to save your changes settings.*

Note	The function with the lower system priority value determines which links between LACP partner devices are active and which are in standby for each LACP group. The device on the controlling end of the link uses port priorities to determine which ports are bundled into the aggregated bundle and which ports are put in standby mode. Port priorities on the other device (the no controlling end of the link) are ignored. In priority comparisons, numerically lower values have higher priority. Therefore, the system with the numerically lower value (higher priority value) for LACP system priority becomes the controlling system. If both devices have the same LACP system priority (for example, they are both configured with the default setting of 32768), the device MAC address determines which switch is in control.

Field	Description
Port	Port Name.
Port Priority	LACP priority value of the port.
Timeout	The periodic transmissions type of LACP PDUs. • **Long:** Transmit LACP PDU with slow periodic (30s). • **Short:** Transmit LACPP DU with fast periodic (1s).

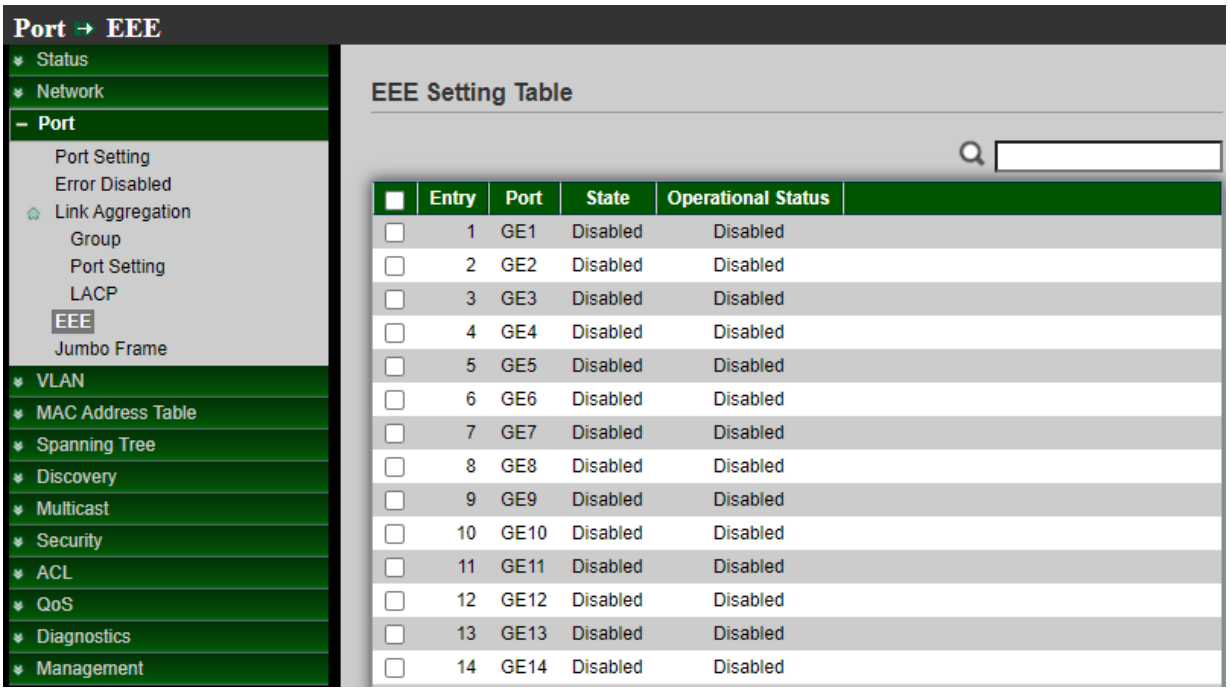
- **Port:** Selected port list.
- **Port Priority:** Enter the LACP priority value of the port.
- **Timeout:** The periodic transmissions type of LACP PDUs.
  - **Long:** Transmit LACP PDU with slow periodic (30s).
  - **Short:** Transmit LACPP DU with fast periodic (1s).

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

4.4 EEE

Energy Efficient Ethernet (EEE) combines the MAC with a family of physical layers that support operation in a low power mode. It is defined by IEEE 802.3az Energy Efficient Task Force. Lower power mode enables both the send and receive sides of the link to disable some functionality for power savings when lightly loaded. Transition to low power mode does not change the link status. Frames in transit are not dropped or corrupted in transition to and from low power mode. Transition time is transparent to upper layer protocols and applications.

This switch support Energy-effcient Ethernet(EEE) function. Administrator can by ports to setting Enable or Disable for the EEE function. The default is "Disable".



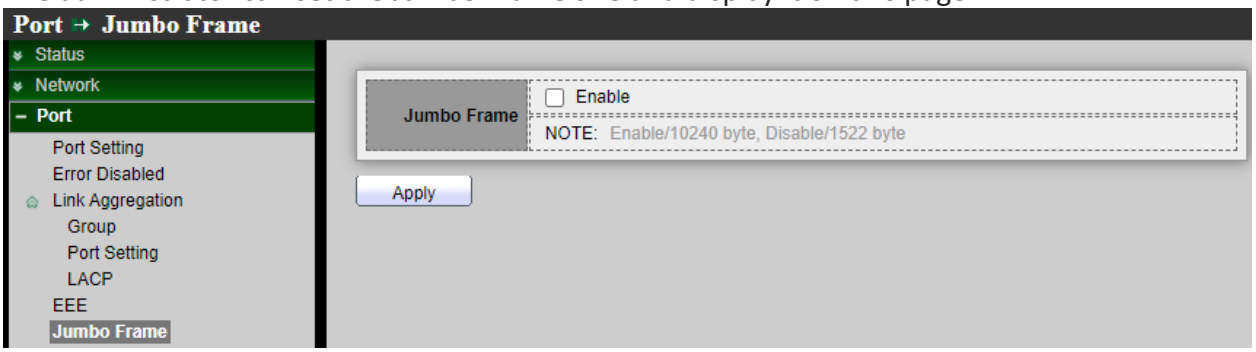
Field	Description
Port	Port Name.
State/Operational Status	Port EEE admin state. • **Enabled:** EEE is enabled/ is operating. • **Disabled:** EEE is disabled/ is no operating.

- **Port:** Selected port list.
- **State:** Port EEE admin state.
  - **Enable:** Enable EEE
  - **Disable:** Disable EEE

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

4.5 Jumbo Frame

The administrator can set the Jumbo Frame size and display it on this page.



- **Jumbo Frame:** Enable or disable jumbo frame. When jumbo frame is enabled, switch max frame size is allowed to configure. When jumbo frame is disabled, default frame size 1522 will be used.

Note	When jumbo frames are required, the maximum frame size (10000) of the switch is allowed to be configured. Uncheck to apply : When you click uncheck to **"Apply"** , The switch will back to default regular frame size "1522".

*Click the **"Apply"** button to save your changes settings.*

5. VLAN

A virtual local area network, virtual LAN or VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together even if they are not located on the same network switch.

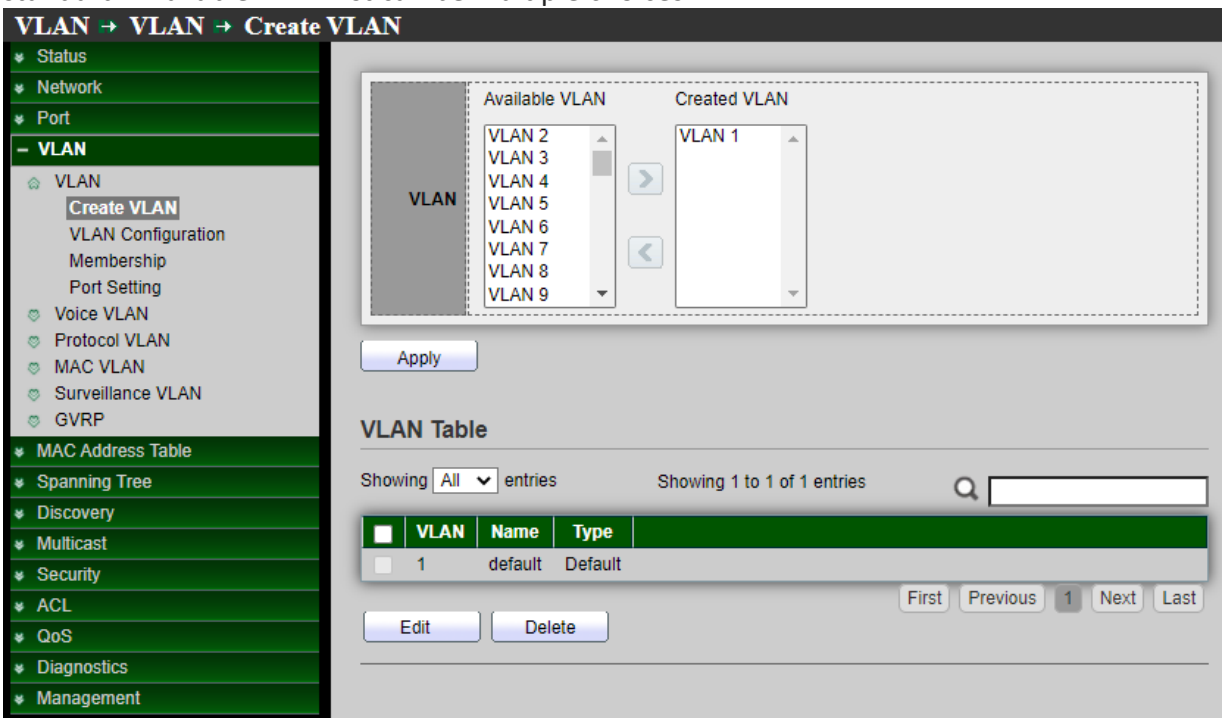
The **CS-2648XG** adding Virtual LAN (VLAN) support to a Layer 2 switch offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast, and like a router, it partitions the network into logical segments, which provides better administration, security and management of multicast traffic.

Administrator can set IEEE 802.1q Tag Based VLAN or Port Based VLAN. System default is VLAN1 Port based (PVID).

5.1 VLAN

5.1.1 Create VLAN

Administrator can select VLAN number in Available VLAN list, this VLAN number based on IEEE 802.1q standard. Available VLAN list can be multiple choices.



- **VLAN:** Administrator can select VLANs number in "Available VLAN" table and move to "Created VLAN" table will complete the 802.1q VLAN.

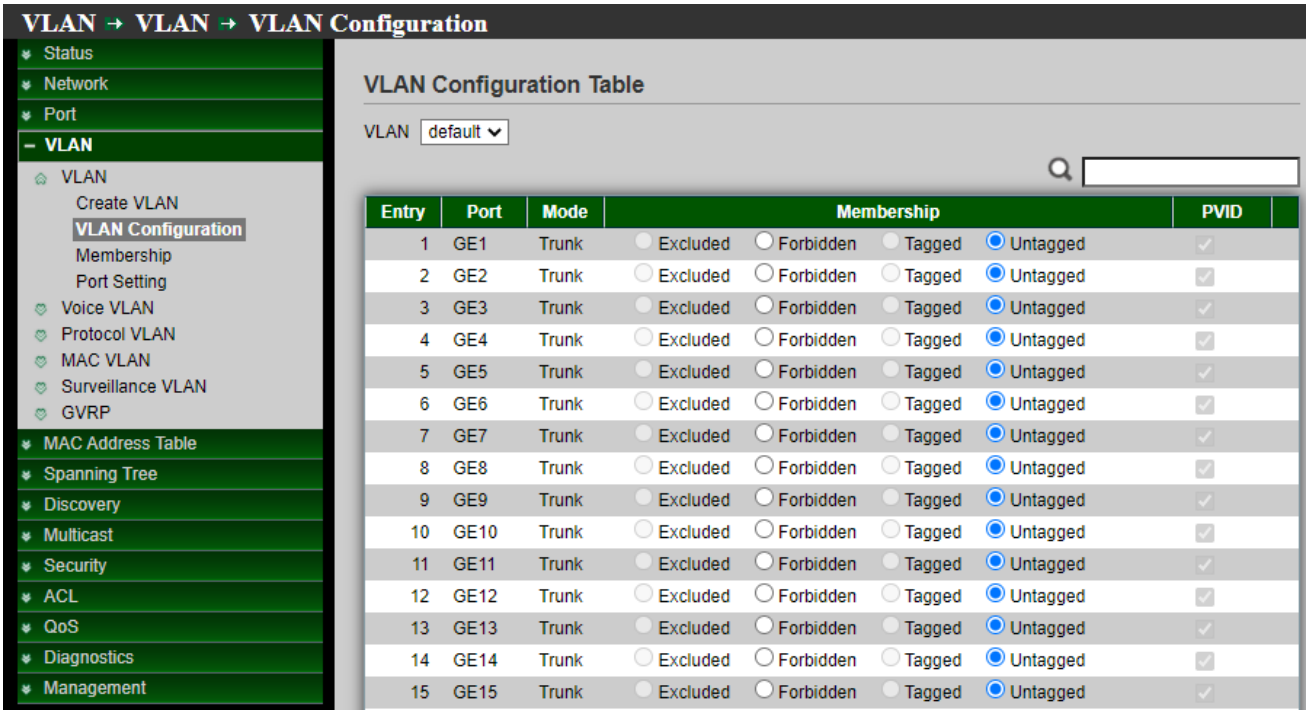
*Click the **"Apply"** button to save your changes settings.*

VLAN Table: Administrator can checkbox VLAN to edit or delete, if check and click "Edit" button then administrator can manual modify name description for this VLAN.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

5.1.2 VLAN Configuration

Administrator can choose set Excluded / Forbidden / Tagged / Untagged function in membership table of the Port and LAG.



Field	Description
VLAN	Select specified VLAN ID to configure VLAN configuration.
Port	Display the interface of port entry.
Mode	Display the interface VLAN mode of port.
Membership	Select the membership for this port of the specified VLAN ID. • **Forbidden:** Specify the port is forbidden in the VLAN. • **Excluded:** Specify the port is excluded in the VLAN. • **Tagged:** Specify the port is tagged member in the VLAN. • **Untagged:** Specify the port is untagged member in the VLAN.
PVID	Display if it is PVID of interface.
Forbidden	**Forbidden:** Specify the port is forbidden in the VLAN.

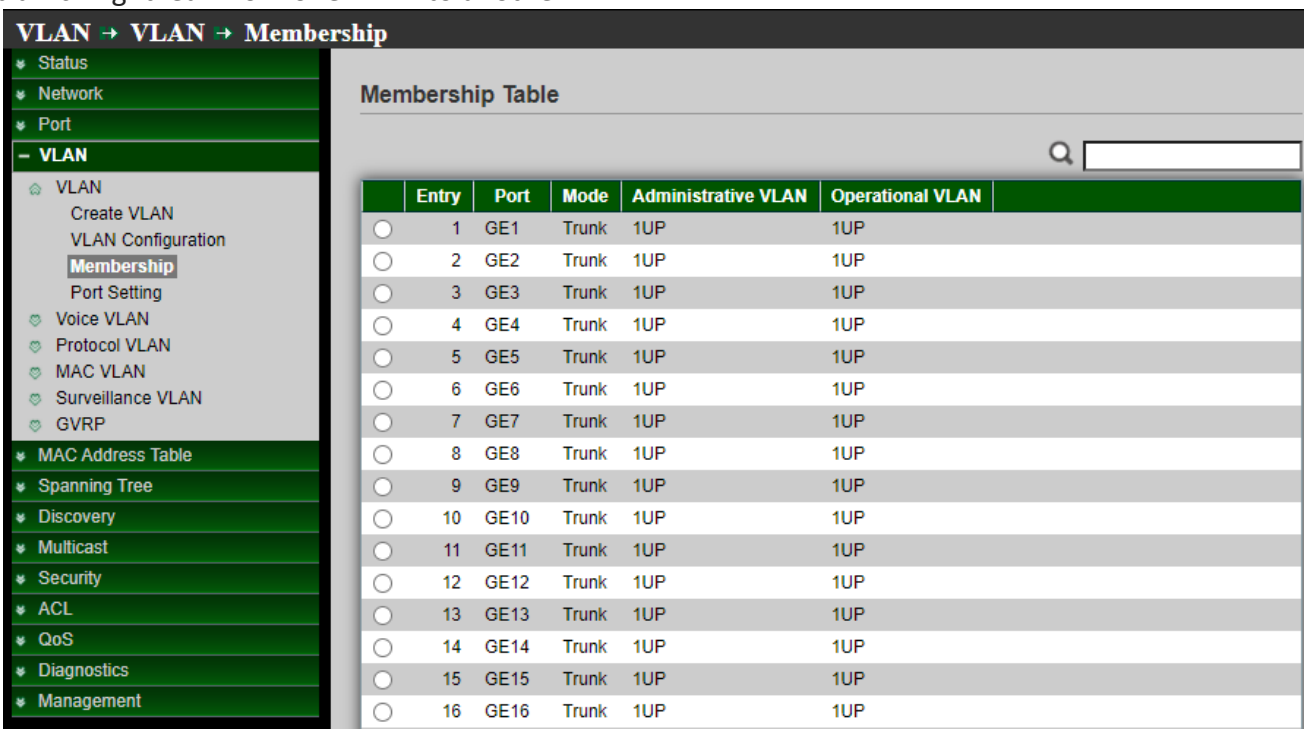
- **VLAN:** Administrator can click drop down menu to choose VLAN and set.
  - **Excluded:** This interface is currently not a member of the VLAN. This is the default for all the ports and LAGs.
  - **Tagged**: This interface is a tagged member of the VLAN.
  - **Untagged**: This interface is an untagged member of the VLAN. Frames of the VLAN are sent

untagged to the interface VLAN.

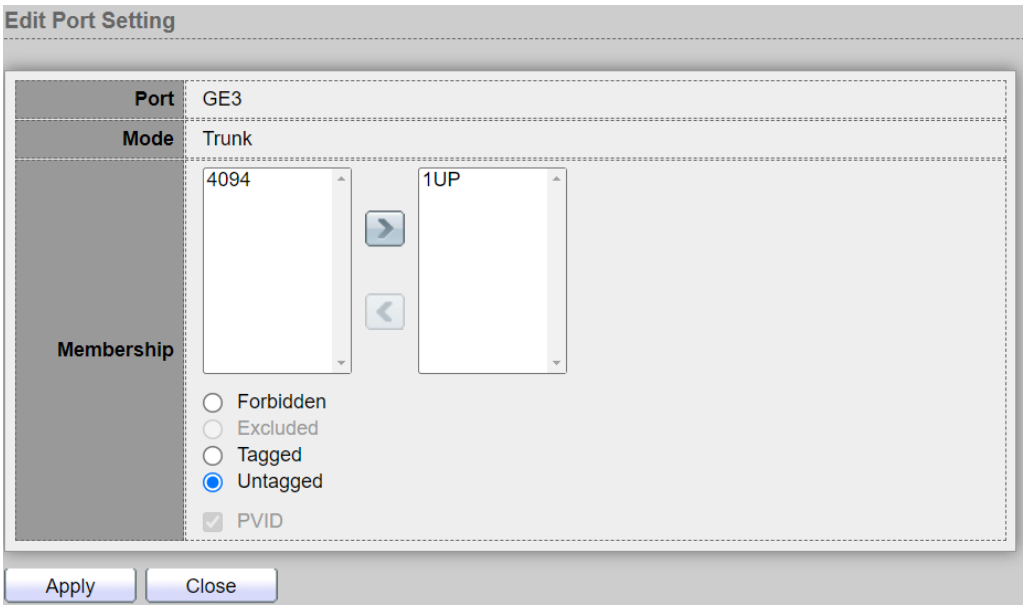
- **PVID**: Check to set the PVID of the interface to the VID of the VLAN. PVID is a per-port setting.
- **Forbidden:** Select for this specified port of the Forbidden.

5.1.3 Membership

Display all port setting information. Administrator can checkbox and click "**Edit**" button to modify VLAN type. *(Note: Number=VLAN number, F=Forbidden, T=Tagged, U=Untagged, P=PVID)*
When a port is forbidden default VLAN membership, that port is not allowed membership in any other VLAN. An internal VID of 4095 is assigned to the port. This PVID on the ports between the two devices must be the same if the ports are to send and receive untagged packets to and from the VLAN. Otherwise, traffic might leak from one VLAN to another.



Field	Description
Port	Display the interface of port entry.
Mode	Display the interface VLAN mode of port.
Administrative VLAN	Display the administrative VLAN list of this port.
Operational VLAN	Display the operational VLAN list of this port. Operational VLAN means the VLAN status that really runs in device. It may different to administrative VLAN.

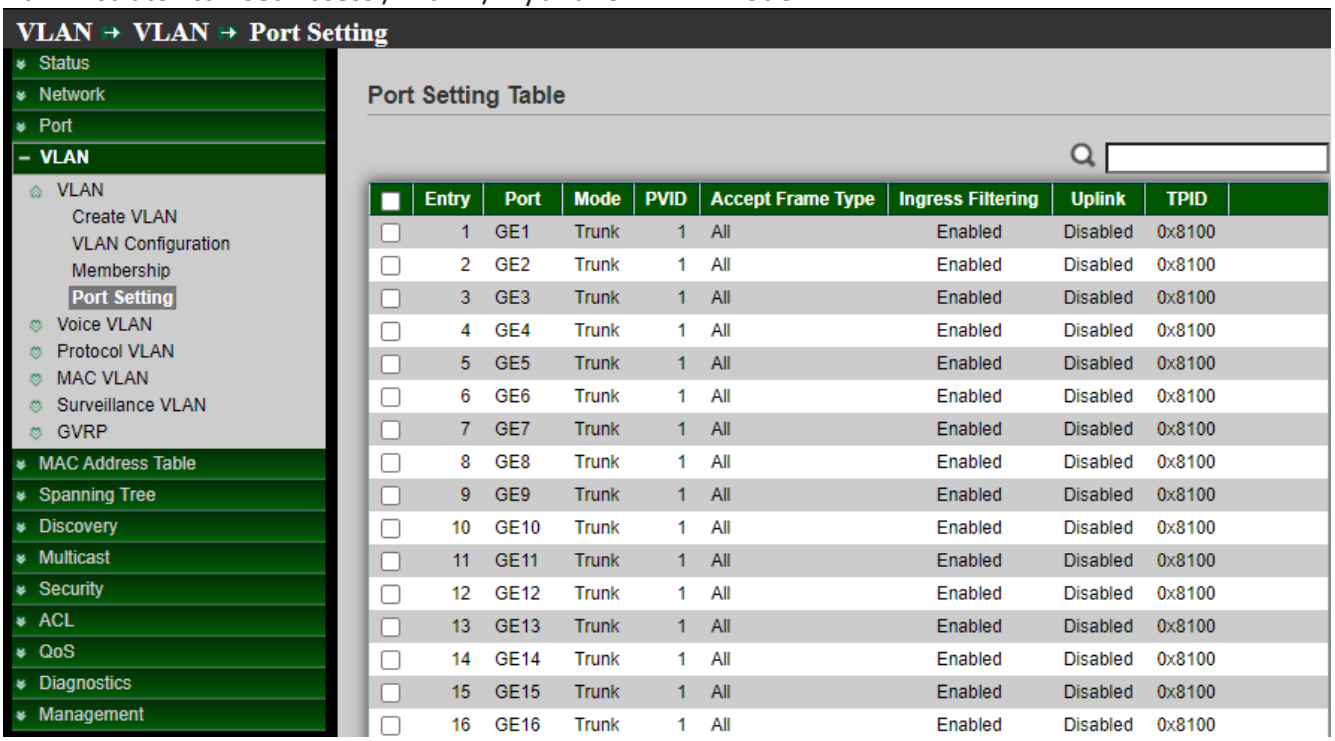


- **Port:** Display selected port number.
- **Mode:** Displays the port VLAN mode that was selected on the Interface Settings page.
- **Membership:** Move the VLAN IDs from the left list to the right list by using the arrow buttons. The default VLAN might appear in the right list if it is tagged, but it cannot be selected.

Cli*ck the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

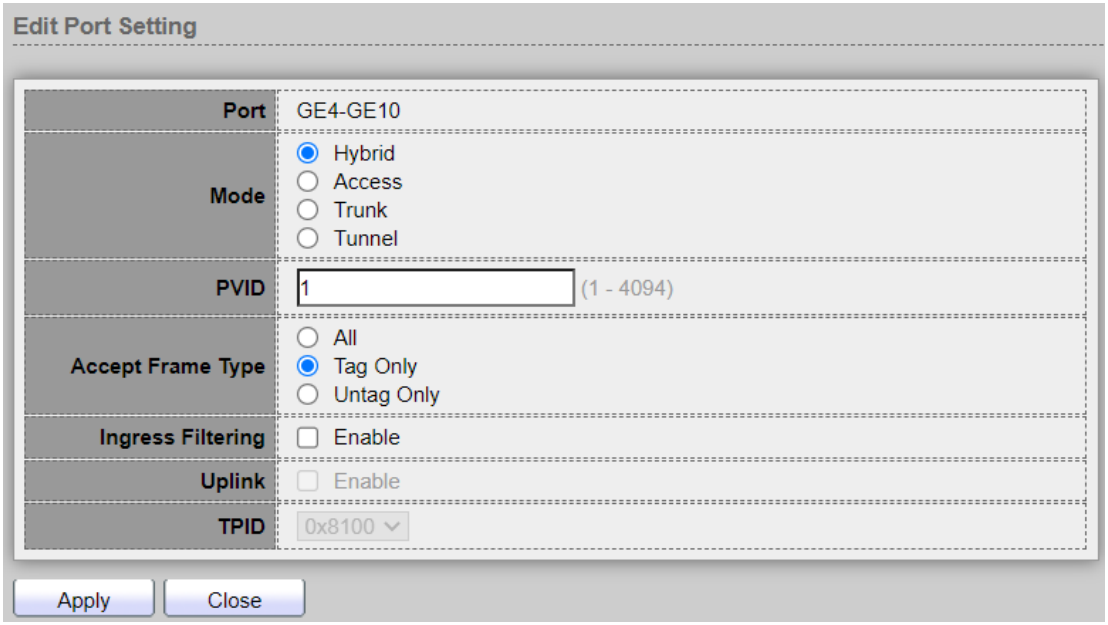
5.1.4 Port Setting

Administrator can set Access / Trunk / Hybrid for VLAN mode.



Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
1	GE1	Trunk	1	All	Enabled	Disabled	0x8100
2	GE2	Trunk	1	All	Enabled	Disabled	0x8100
3	GE3	Trunk	1	All	Enabled	Disabled	0x8100
4	GE4	Trunk	1	All	Enabled	Disabled	0x8100
5	GE5	Trunk	1	All	Enabled	Disabled	0x8100
6	GE6	Trunk	1	All	Enabled	Disabled	0x8100
7	GE7	Trunk	1	All	Enabled	Disabled	0x8100
8	GE8	Trunk	1	All	Enabled	Disabled	0x8100
9	GE9	Trunk	1	All	Enabled	Disabled	0x8100
10	GE10	Trunk	1	All	Enabled	Disabled	0x8100
11	GE11	Trunk	1	All	Enabled	Disabled	0x8100
12	GE12	Trunk	1	All	Enabled	Disabled	0x8100
13	GE13	Trunk	1	All	Enabled	Disabled	0x8100
14	GE14	Trunk	1	All	Enabled	Disabled	0x8100
15	GE15	Trunk	1	All	Enabled	Disabled	0x8100
16	GE16	Trunk	1	All	Enabled	Disabled	0x8100

Field	Description
Port	Display the interface.
Mode	Display the VLAN mode for Hybrid/Access/Trunk/Tunnel mode of port.
PVID	Display the Port-based VLAN ID of port.
Accept Frame Type	Display accept frame type of port.
Ingress Filtering	Display ingress filter status of port.
Uplink	Display uplink status.
TPID	Display TPID used of interface.



- **Hybrid:** The interface can be a tagged or untagged member of one or more VLANs.
- **Access:** The interface is an untagged member of a single VLAN. A port configured in this mode is known as an access port.
- **Trunk:** The interface is an untagged member of one VLAN at most, and is a tagged member of zero or more VLANs. A port configured in this mode is known as a trunk port.
- **Tunnel:** This enables the user to use own VLAN arrangements (PVID) across the provider network.
- **PVID:** Enter the Port VLAN ID (PVID) of the VLAN to which incoming untagged and priority tagged frames are classified.
- **Accept Frame Type:** Select the type of frame that the interface can receive. Frames that are not of the configured frame type are discarded at ingress. These frame types are only available in General mode. As follow.

- **All:** The interface accepts all types of frames: untagged frames, tagged frames, and priority tagged frames.
- **Tag Only:** The interface accepts only tagged frames.
- **Untag Only:** The interface accepts only untagged and priority frames.

➢ **Ingress Filtering:** Administrator can check Enable to enable ingress filtering. When an interface is ingress filtering enabled, the interface discards all incoming frames that are classified as VLANs of which the interface is not a member. Ingress filtering can be disabled or enabled on general ports. It is always enabled on access ports and trunk ports.

➢ **Uplink:** Administrator can check **Enable** to set the interface as an uplink port.

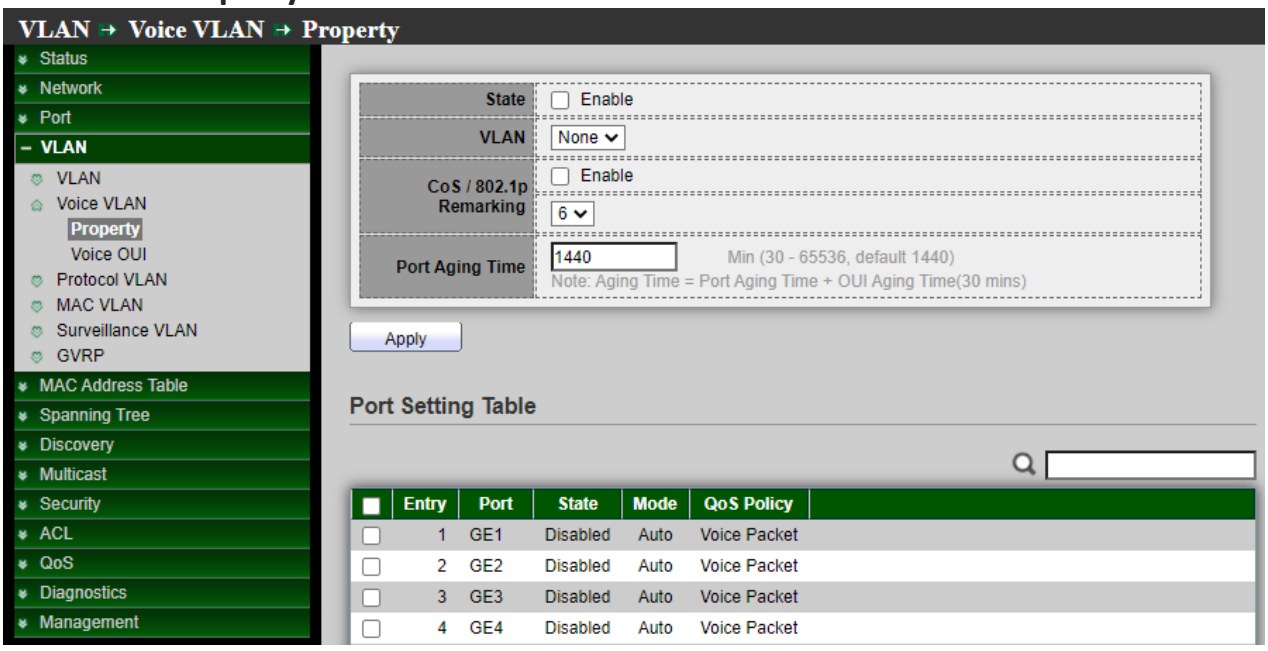
➢ **TPID:** If Unlink is enabled, select the Modified Tag Protocol Identifier (TPID) value for the interface.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

5.2 Voice VLAN

Voice VLAN allows you to enhance VoIP service by configuring ports to carry IP Voice traffic from IP phones on a specific VLAN. VoIP traffic has a preconfigured OUI prefix in the source MAC address. Administrator can set VLAN ID in the range of 1 to 4094.

5.2.1 Property



*Click the **"Apply"** button to save your changes settings.*

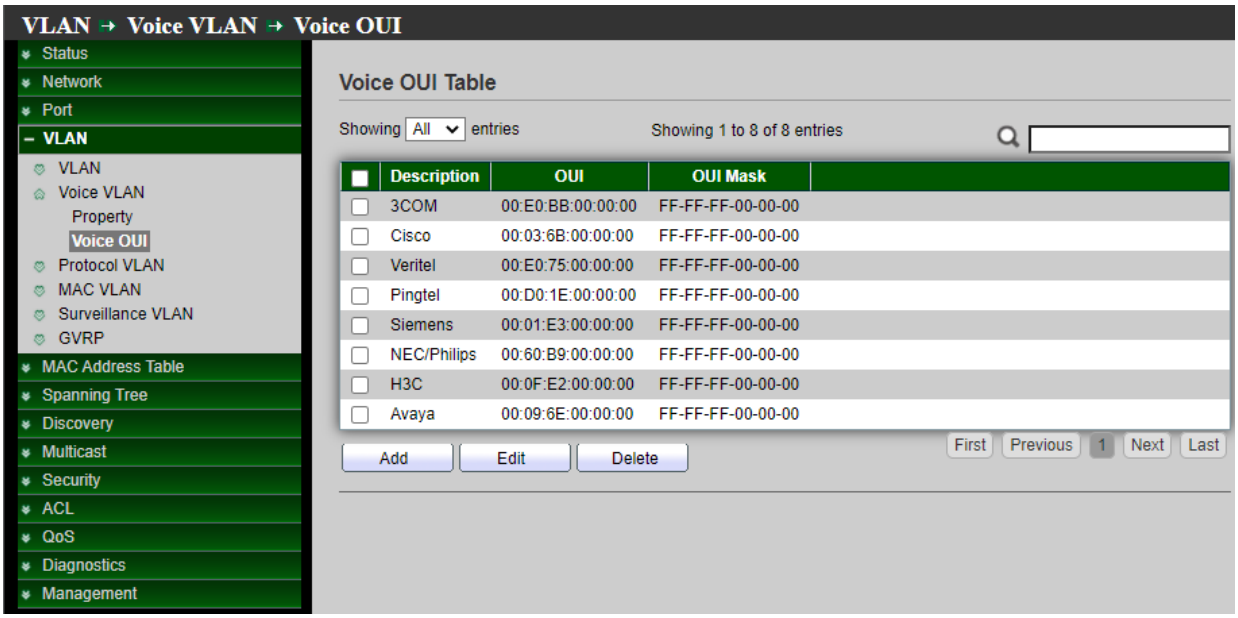
Field	Description
Port	Display port entry.
State	Display enable/disabled status of interface.
Mode	Display voice VLAN mode.
QoS Policy	Display voice VLAN remark will effect which kind of packet.

- **State:** Administrator can choose Enable or Disable this function.
- **VLAN:** Administrator can choose VLAN.
- **CoS / 802.1P Remarking**: Administrator can set CoS 802.1p priority level for the VLAN.
- **Port Aging Time:** Administrator can set aging time for this rule.

Click t*he **"Apply"** button to save your changes or **"Close"** the button to close settings.*

5.2.2 Voice OUI

Organizationally Unique Identifiers (OUI) is the first three bytes of a MAC Address, while the last three bytes contain a unique station ID. Administrator can add a specific manufacturer with the OUI. Once the OUI is added, all traffic received on voice VLAN ports from the specific IP phone with a listed OUI is forwarded on the voice VLAN. Unlike the telephony OUI mode that detects voice devices based on telephony OUI, Auto Voice VLAN mode depends on auto smart port to dynamically add the ports to the voice VLAN. The default has set 8 companies for the voice phone.



Field	Description
OUI	Display OUI MAC address.
Description	Display description of OUI entry.

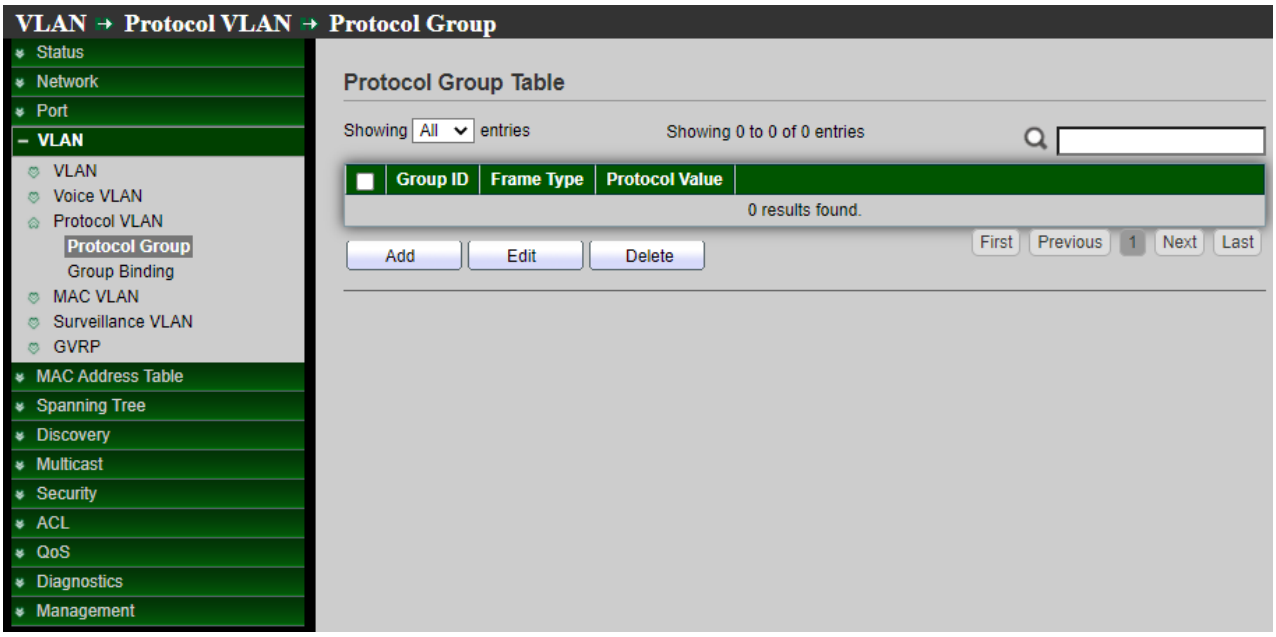
Administrator can create new OUI or modify or delete OUI in table
Click **“add”** button can create new OUI.
Click “**Edit**” button can modify OUI data.
Click **“Delete”** button can delete OUI data.

Click *the **“Apply”** button to save your changes or **“Close”** the button to close settings.*

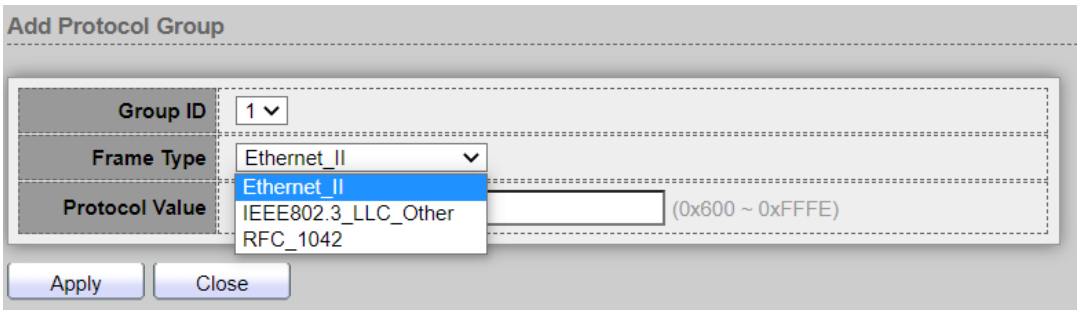
5.3 Protocol VLAN

5.3.1 Protocol Group

Administrator can configure this page to add or edit groups settings of protocol VLAN, Setting **"add"** and "Edit" and **"Delete"** function for this management.



Field	Description
Group ID	Display group ID of entry.
Frame Type	Display frame type of entry.
Protocol Value	Display protocol value of entry.



- **Group ID :** Select group ID of list. The range from 1 to 8.
- **Frame Type :** Select frame type of list that maps packets to protocol-defined VLANs by examining the type octet within the packet header to discover the type of protocol associated with it.
  - **Ethernet_II :** packet type is Ethernet version 2.
  - **IEEE802.3_LLC_Other :** packet type is 802.3 packet with LLC other header.

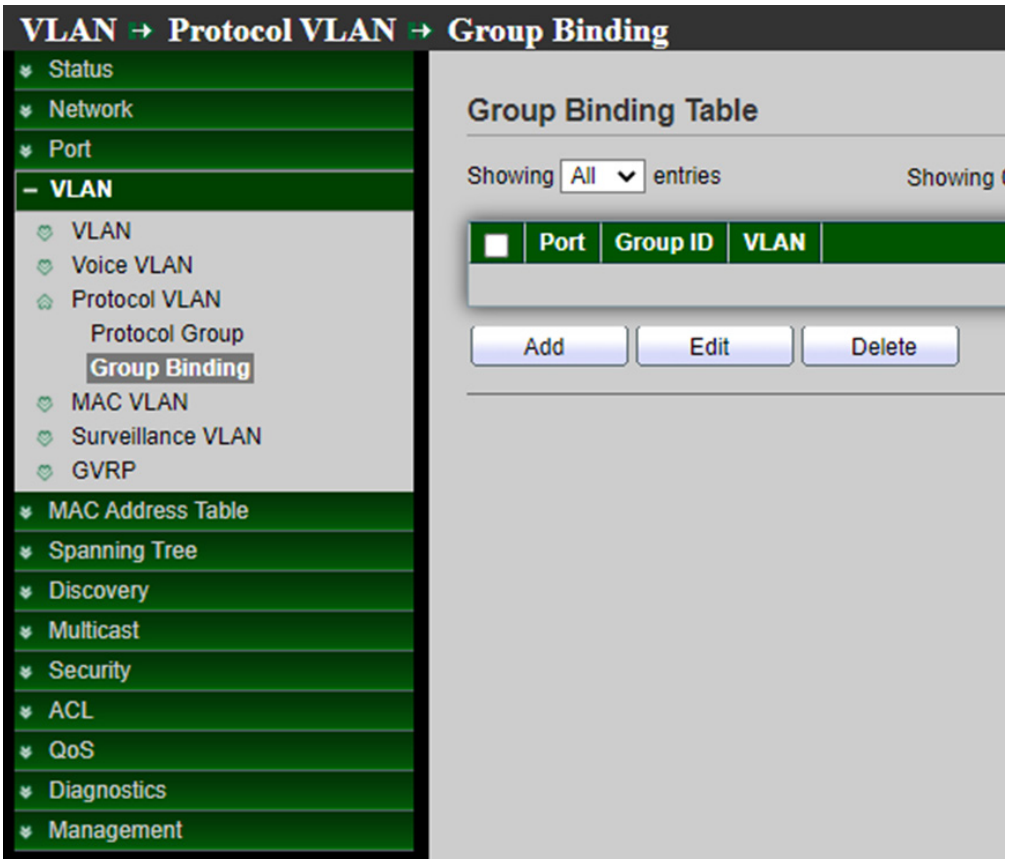
- **RFC_1042 :** packet type is rfc 1042 packet.

➢ **Protocol Value :** Input protocol value of the target protocol. Packets match this protocol value classified to specified VLAN ID.

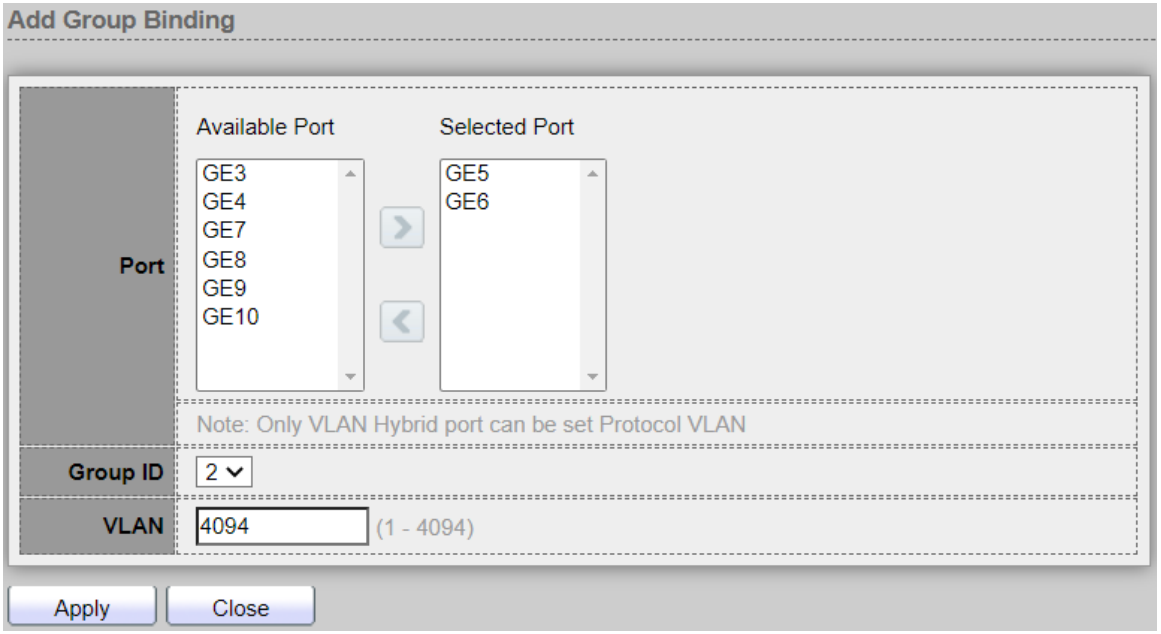
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

5.3.2 Group Binding

Administrator can configure this bind protocol VLAN group to each port with VLAN ID, Setting **"add"** and "Edit" and **"Delete"** function for this management.



Field	Description
Port	Display port ID that binding with protocol group entry.
Group ID	Display group ID that port binding with.
VLAN	Display VLAN ID that assign to packets which match protocol group.



- **Port :** Select ports in left box then move to right to binding with protocol group. Or select ports in right box then move to left to unbind with protocol group. Only interface has hybrid VLAN mode can be selected and bound with protocol group. Only available on Add dialog. .
- **Group ID :** Select a Group ID to associate with port. Only available on Add dialog.
- **VLAN :** Input VLAN ID that will assign to packets which match protocol group.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

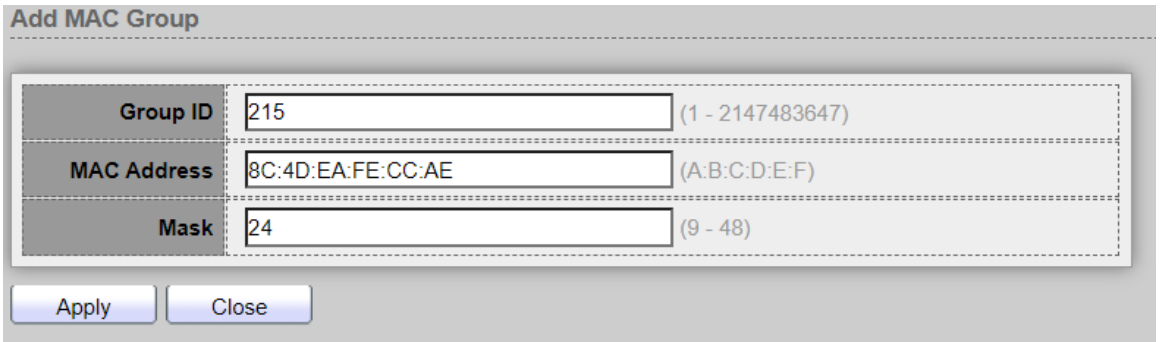
5.4 MAC VLAN

5.4.1 MAC Group

The MAC VLAN feature allows incoming untagged packets to be assigned to a VLAN and thus classify traffic based on the source MAC address of the packet. You define a MAC to VLAN mapping by configuring an entry in the MAC to VLAN table. An entry is specified using a source MAC address and the appropriate VLAN ID. The MAC to VLAN configurations are shared across all ports of the device (i.e., there is a system-wide table that has MAC address to VLAN ID mappings).

When untagged or priority tagged packets arrive at the switch and entries exist in the MAC to VLAN table, the source MAC address of the packet is looked up. If an entry is found, the corresponding VLAN ID is assigned to the packet. If the packet is already priority tagged it will maintain this value; otherwise, the priority will be set to 0 (zero). The assigned VLAN ID is verified against the VLAN table. If the VLAN is valid, ingress processing on the packet continues; otherwise, the packet is dropped. This implies that you can configure a MAC address mapping to a VLAN that has not been created on the system, Setting **"add"** and "Edit" and **"Delete"** function for this management.

Field	Description
Group ID	Display group ID of entry.
MAC Address	Display mac address of entry.
Mask	Display mask of mac address for classified packet.

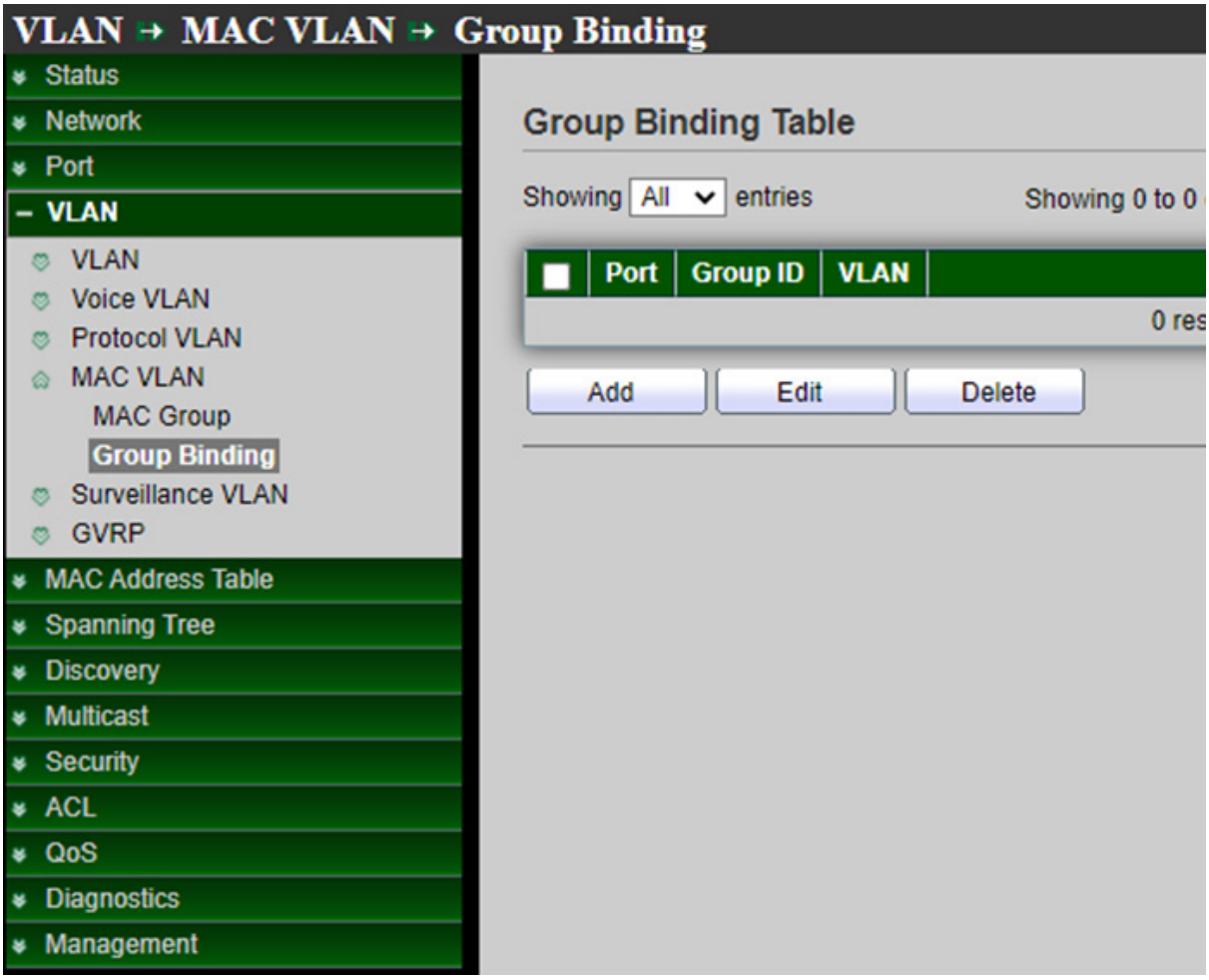


- **Group ID:** Add a Group ID number.
- **MAC Address :** Enter the MAC Address.
- **Mask**: Enter the mask of mac address for classified packet..

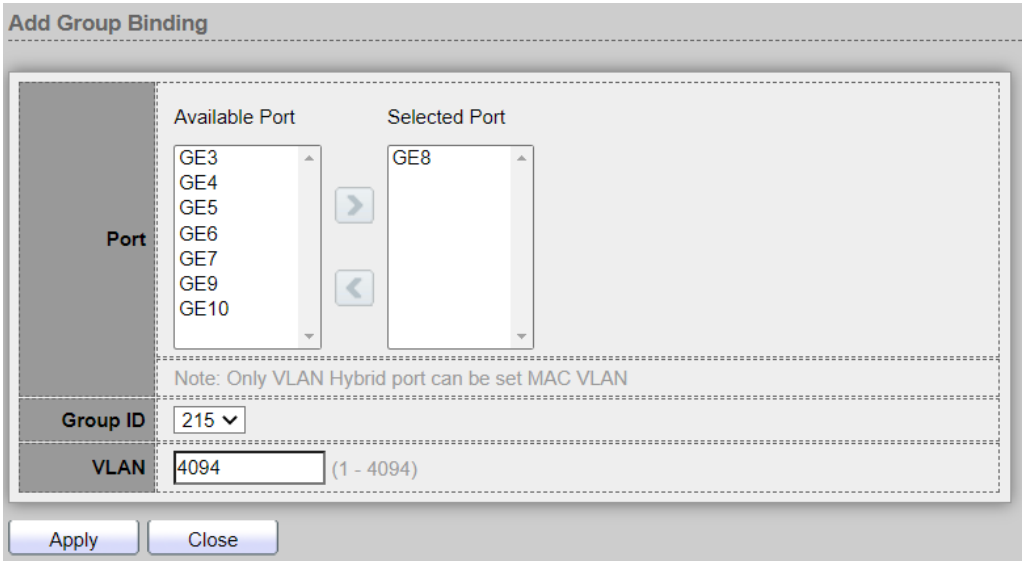
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

5.4.2 Group Binding

The Group Binding allows user to bind MAC VLAN group to each port with VLAN ID, Setting **"add"** and "Edit" and **"Delete"** function for this management.



Field	Description
Port	Display port ID that binding with protocol group entry.
Group ID	Display group ID that port binding with.
VLAN	Display VLAN ID that assign to packets which match protocol group.



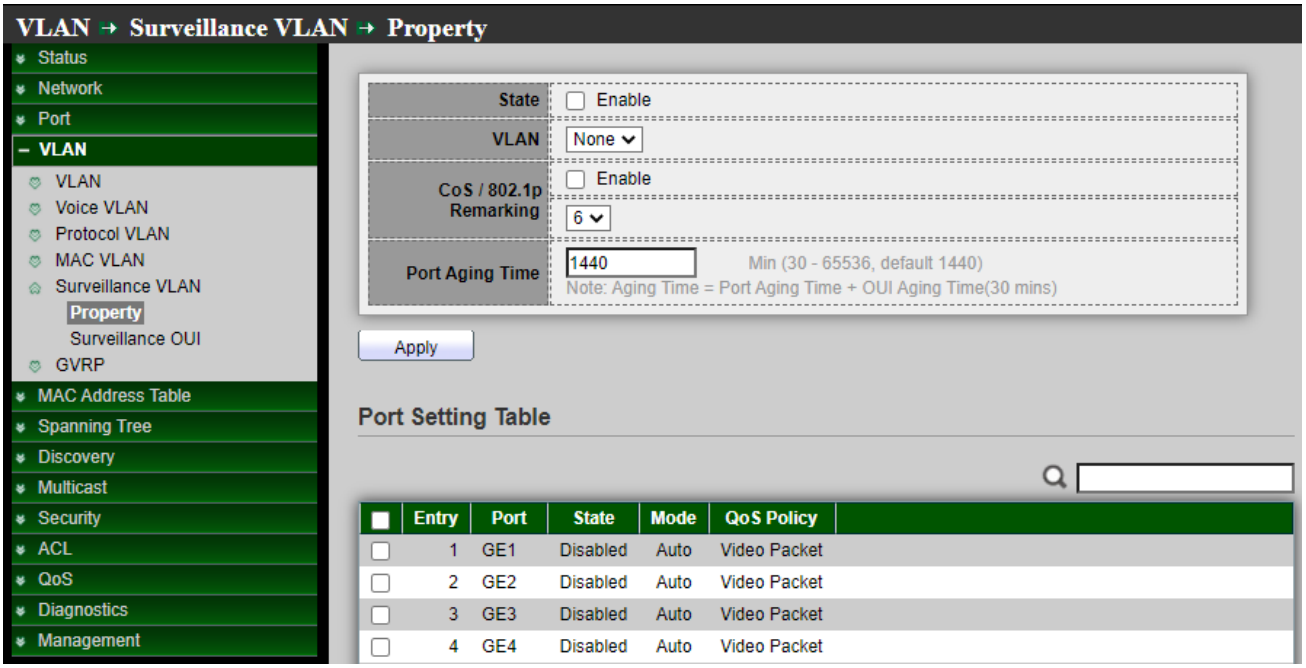
- **Port:** Select the port in the left frame and move to the right to bind to the mac group; or select the port in the right frame and move to the left to bind to the mac group. Only interfaces with mixed VLAN mode can be selected and bound to the protocol group.
- **Group ID:** Choose a Group ID associated with the port.
- **VLAN**: Enter the VLAN ID that will be assigned to packets matching the MAC Group.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

5.5 Surveillance VLAN

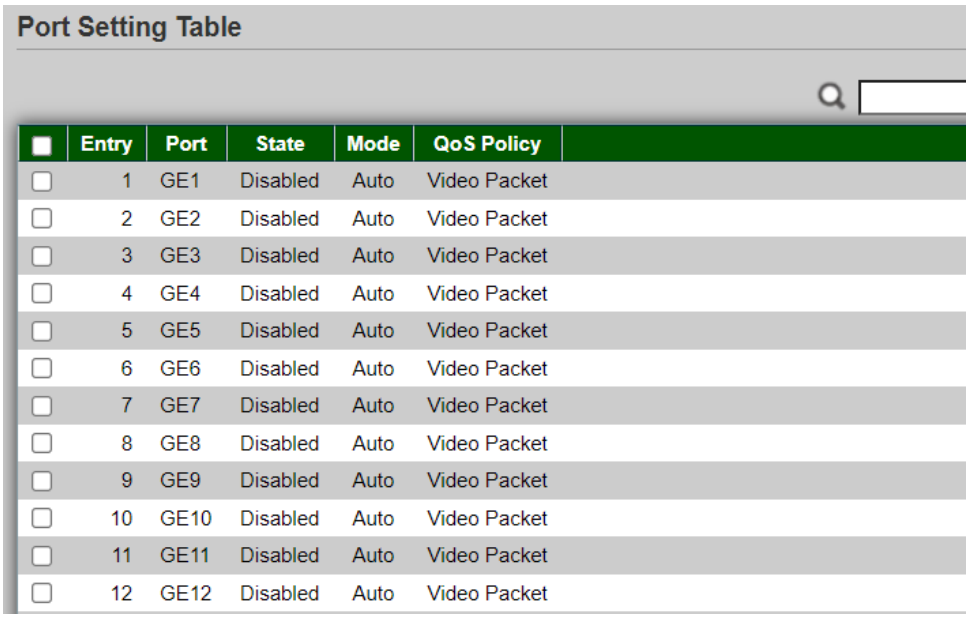
5.5.1 Property

Administrator can configure this page to configure global and per interface settings of Surveillance VLAN.



- **State :** Set checkbox to enable or disable Surveillance VLAN function. .
- **VLAN :** Select Surveillance VLAN ID. Surveillance VLAN ID cannot be default VLAN.
- **Cos/802.1p :** Select a value of VPT. Qualified packets will use this VPT value as inner priority.
- **Remarking:** Set checkbox to enable or disable 1p remarking. If enabled, qualified packets will be remark by this value.
- **Aging Time :** Input value of aging time. Default is 1440 minutes. A video VLAN entry will be age out after this time if without any packet pass through.

*Click the **"Apply"** button to save your changes settings.*



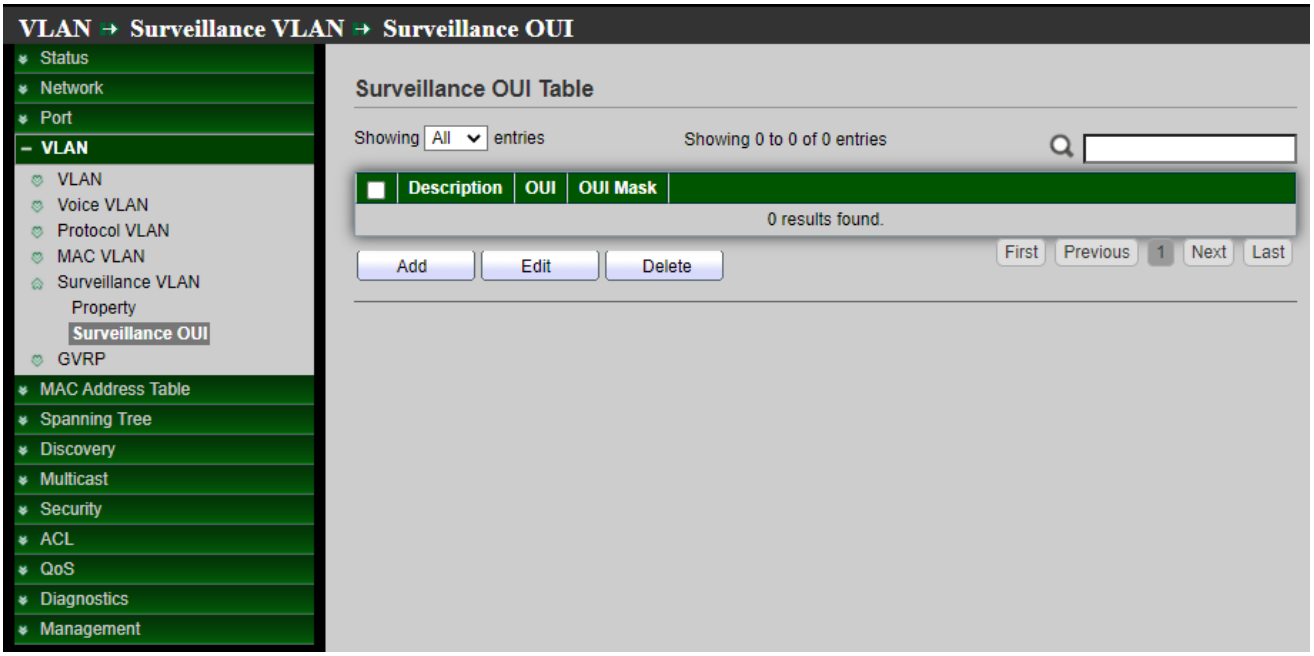
Field	Description
Port	Display port entry.
State	Display enable/disabled status of interface.
Mode	Display voice VLAN mode.
QoS Policy	Display Surveillance VLAN remark will effect which kind of packet.

- **Port :** Display selected port to be edited.
- **State :** Set checkbox to enable/disabled Surveillance VLAN function of interface.
- **Mode :** Select port Surveillance VLAN mode.
  - **Auto :** Video VLAN auto detect packets that match OUI table and add received port into surveillance VLAN ID tagged member.
  - **Manual :** User need add interface to VLAN ID tagged member manually.
- **QoS Policy :** Select port QoS Policy mode.
  - **Video Packet :** Video Packet: 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 Surveillance VLAN.

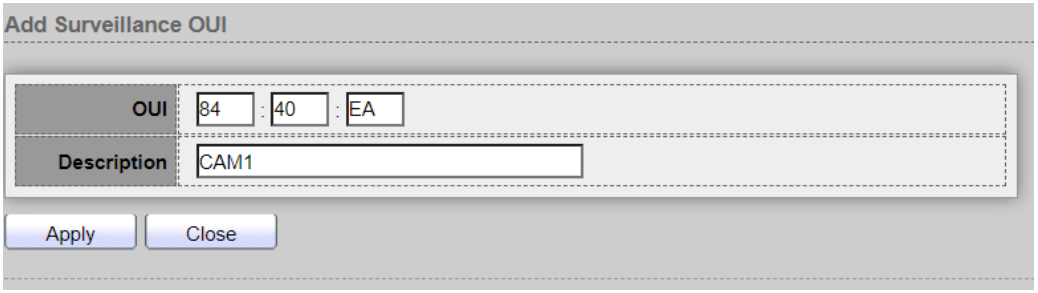
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

5.5.2 Surveillance OUI

Administrator can configure this page to add, edit or delete OUI MAC addresses, Setting **"add"** and "Edit" and **"Delete"** function for this management.



Field	Description
OUI	Display OUI MAC address.
Description	Display description of OUI entry.



- **OUI :** Input OUI MAC address. Can't be edited in edit dialog. .
- **Description :** Input description of the specified MAC address to the Surveillance VLAN OUI table.

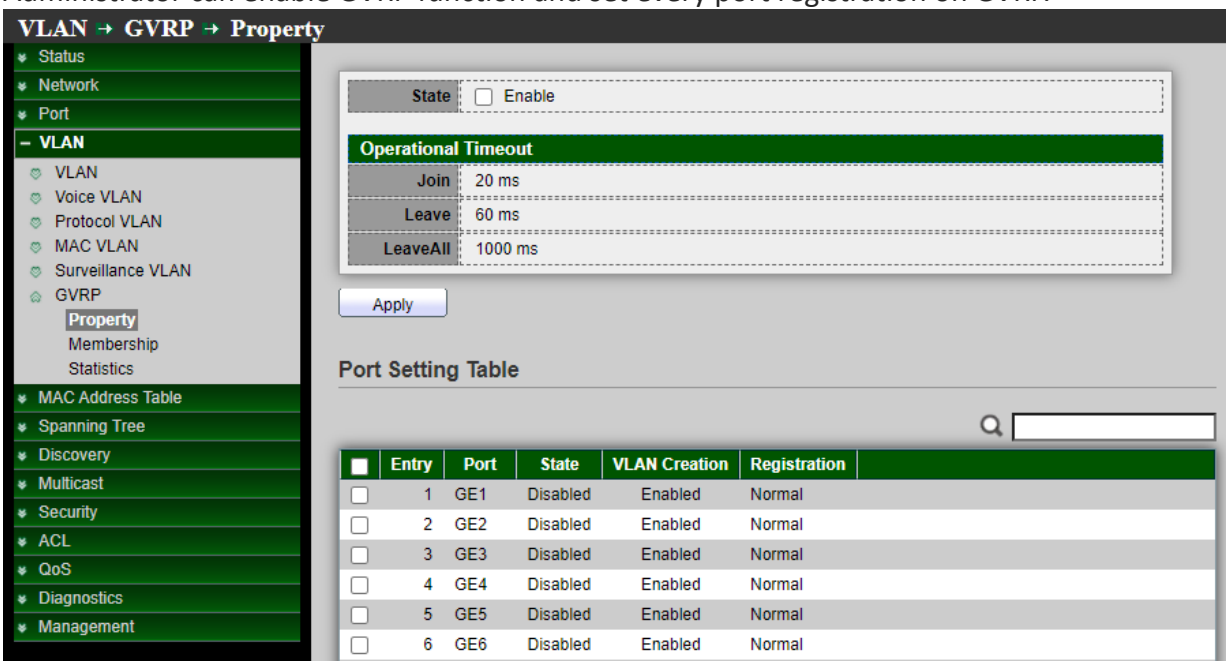
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

5.6 GVRP

The GVRP (Generic VLAN Registration Protocol) is described in the IEEE 802.1p standard; It's an IEEE 802.1Q-compliant method for facilitating automatic (dynamic) VLAN membership configuration. GVRP-enabled switches can exchange VLAN configuration information with other GVRP-enabled switches. Policy rules or other network management methods can determine who is admitted to a VLAN. When a node requests admission to a specific VLAN, GVRP handles the registration of the node with GVRP-enabled switches and maintains that information.
GVRP reduces the chance of errors in VLAN configuration by automatically providing VLAN ID (VID) consistency across the network. In addition, you can use GVRP to dynamically enable port membership in static VLANs configured on a switch. Once GVRP creates a dynamic VLAN will can also reduce unnecessary broadcast traffic and unicast traffic.

5.6.1 Property

Administrator can enable GVRP function and set every port registration on GVRP.



- **State :** Set the enabling status of GVRP functionality
  - **Enable:** if Checked Enable GVRP, else is Disable GVRP.
- **Operational Timeout:** The port will not learn any dynamic VLAN. Only send static VLAN information to
  - **Join.:** GVRP Join time out.
  - **Leave:** GVRP leave time out.

*Click the **"Apply"** button to save your changes settings.*

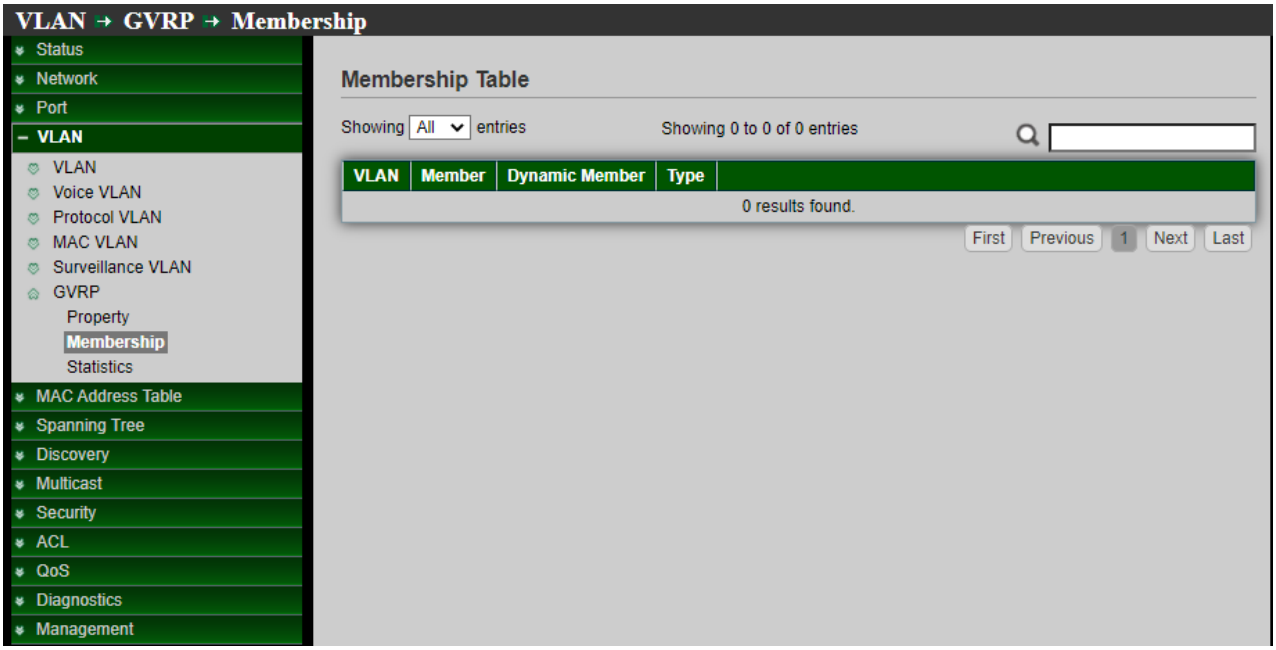
Field	Description
Port	Port Name.
State	Display port GVRP state.
VLAN Creation	Display port GVRP creation VLAN state.
Registration	Display port GVRP registration mode.

- **Port:** Display port number.
- **State:** Displays whether GVRP is enabled or disabled on the interface.
- **VLAN Creation:** Displays whether Dynamic VLAN creation is enabled or disabled on the interface. If it is disabled, GVRP can operate but new VLANs are not created.
- **Registration:** Displays the VLAN registration mode on the interface.
  - **Normal: Normal mode.**.
  - **Fixed:** The port will not learn any dynamic VLAN. Only send static VLAN information to neighbor and allow static VLAN packet pass..
  - **Forbidden:** The port will not learn any dynamic VLAN and only allow default VLAN packet pass

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

5.6.2 Member ship

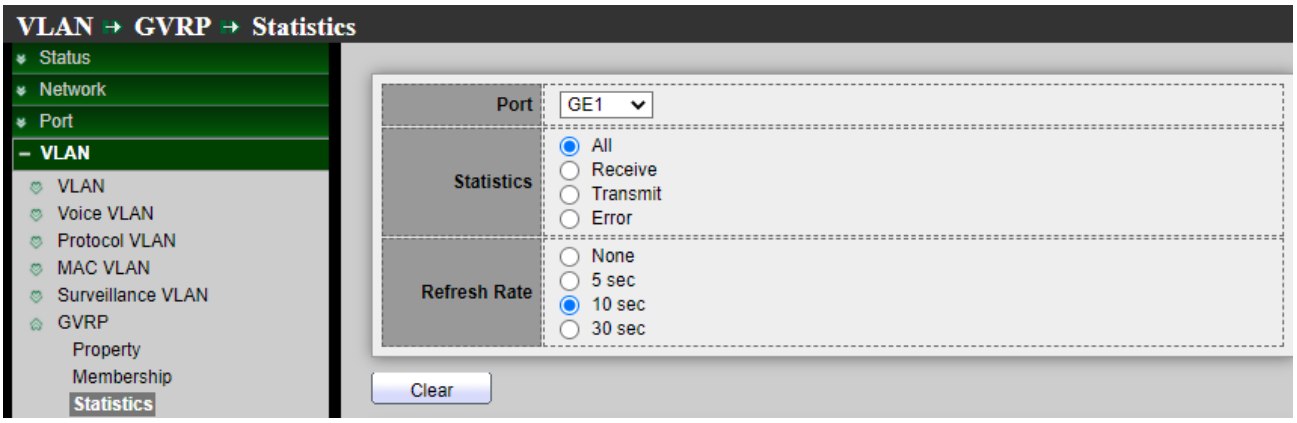
When enable GVRP function and state ports in GVRP then administrator can check GVRP member information.



Field	Description
VLAN	VLAN ID.
Member	VLAN port members include static and dynamic member.
Dynamic Ports	GVRP learned dynamic ports.
Type	The type of VLAN is static or dynamic.

5.6.3 Statistics

When enable and set GVRP function then administrator can check every port in GVRP include Receive / Transmit and Error information.



*Click the **"Clear"** button to clear this page.*

Receive	
Join empty	0
Empty	0
Leave Empty	0
Join In	0
Leave In	0
Leave All	0

Transmit	
Join empty	0
Empty	0
Leave Empty	0
Join In	0
Leave In	0
Leave All	188

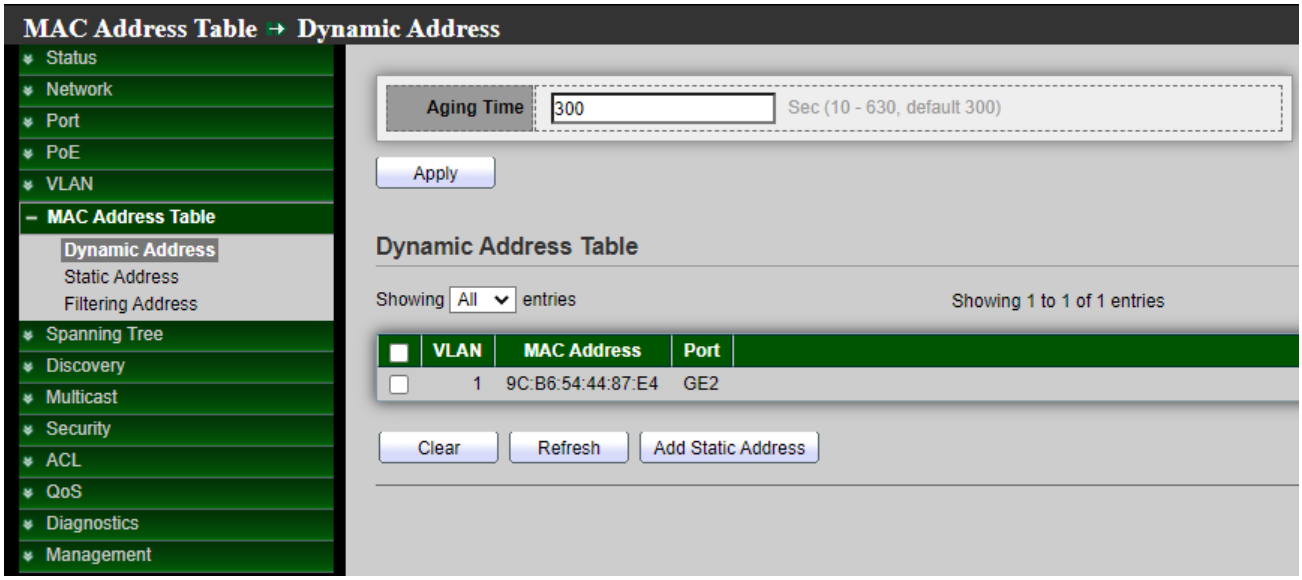
Error	
Invalid Protocol ID	0
Invalid Attribute Type	0
Invalid Attribute Value	0
Invalid Attribute Length	0
Invalid Event	0

Field	Description
Join empty	The number of Receive or Transmit Join empty attribute value.
Empty	The number of Receive or Transmit Empty attribute value.
Leave Empty	The number of Receive or Transmit Leave Empty attribute value.
Join In	The number of Receive or Transmit Join In attribute value.
Leave In	The number of Receive or Transmit Leave In empty attribute value.
Leave All	The number of Receive or Transmit Leave All attribute value.
Invalid Protocol ID	The number of Receive Invalid Protocol ID.
Invalid Attribute Type	The number of Receive Invalid Attribute Type.
Invalid Attribute Value	The number of Receive Invalid Attribute value.
Invalid Attribute Length	The number of Receive Invalid Attribute Length.
Invalid Event	The number of Receive Invalid Event.

6. MAC Address Table

6.1 Dynamic Address

This page can display MAC address for connected device. Administrator can set aging time for connected port.



- **Aging Time :** The time in seconds that an entry remains in the MAC address table. Its valid range is from 10 to 630 seconds, and the default value is 300 seconds.

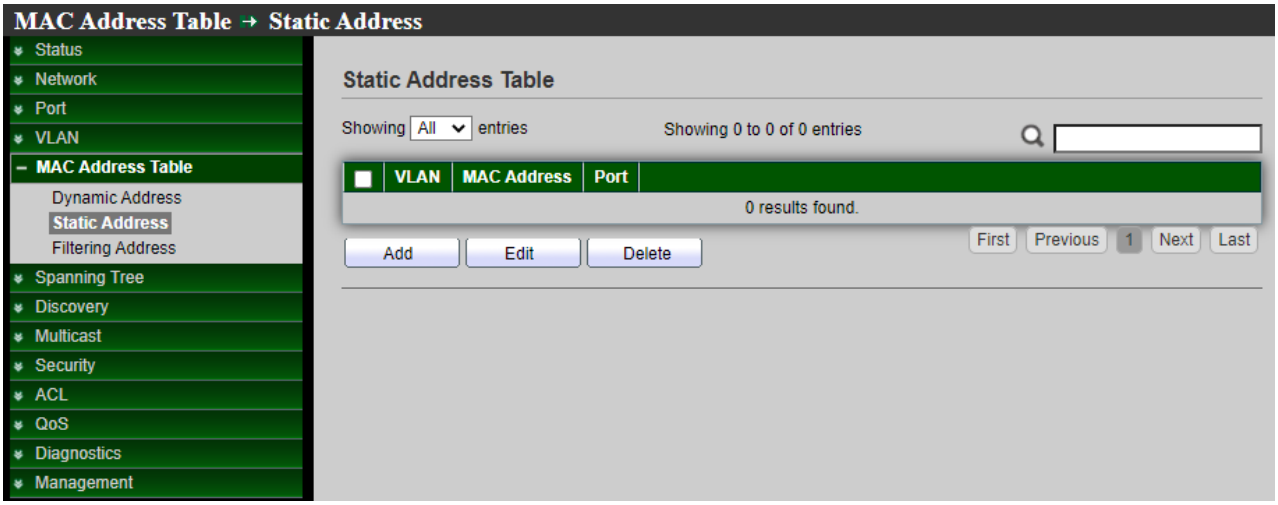
*Click the **"Apply"** button to save your changes settings.*

Field	Description
MAC Address	The MAC address to which packets will be statically forwarded.
VLAN	Specify the VLAN to show or clear MAC entries.
Port	Interface or port number.

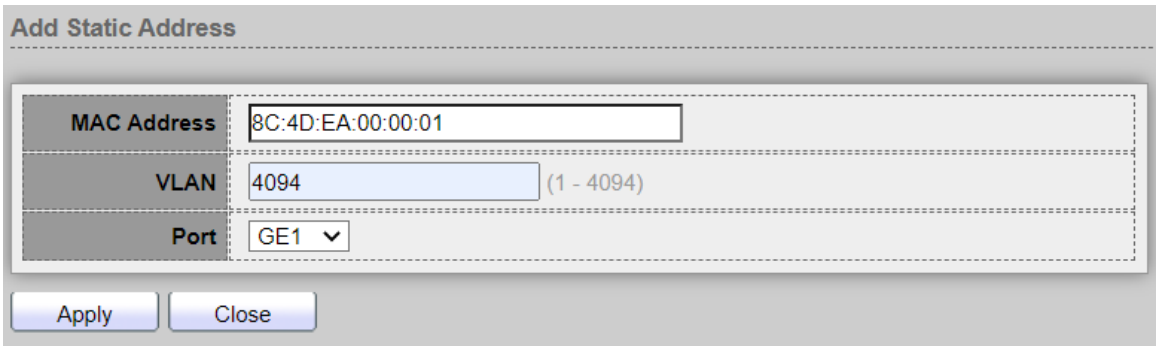
When administrator select checkbox MACs address and click "**Add Static Address**" button then selected MAC address will move to "**Static Address**" function.

6.2 Static Address

If administrator fixed an MAC address in the port then device MAC address will bind in the port, if device connection other port will can't working only connection bind port, Setting **"add"** and "Edit" and **"Delete"** function for this management.



Field	Description
MAC Address	The MAC address to which packets will be statically forwarded.
VLAN	Specify the VLAN to show or clear MAC entries.
Port	Interface or port number.

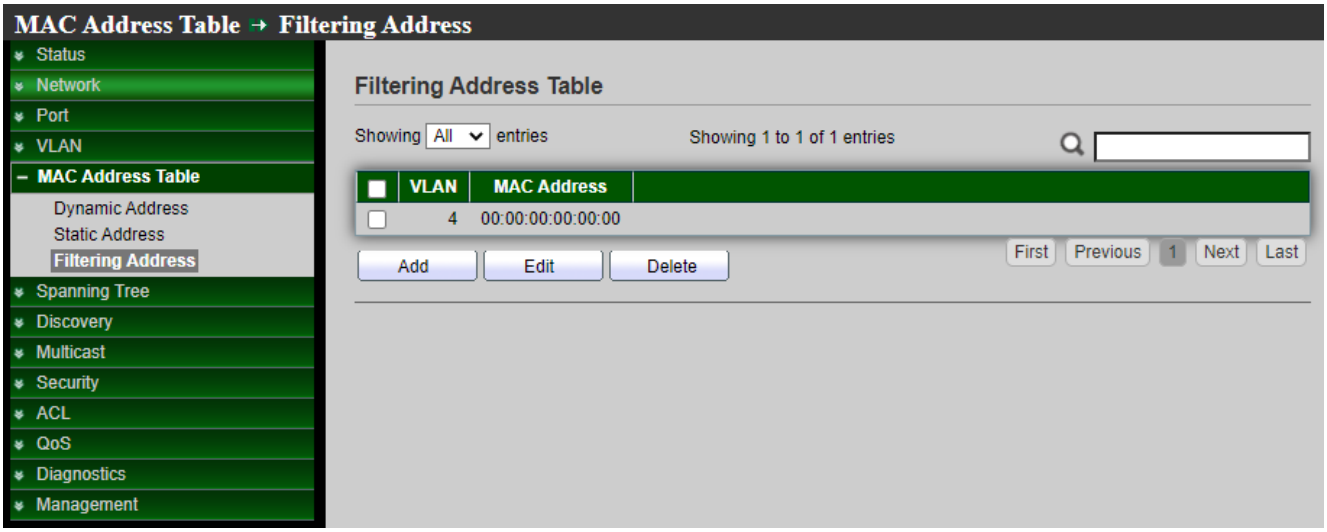


- **MAC Address :** Enter the MAC address to which packets will be statically forwarded.
- **VLAN :** Enter the Specify the VLAN ID
- **Port :** Select an interface or port number.

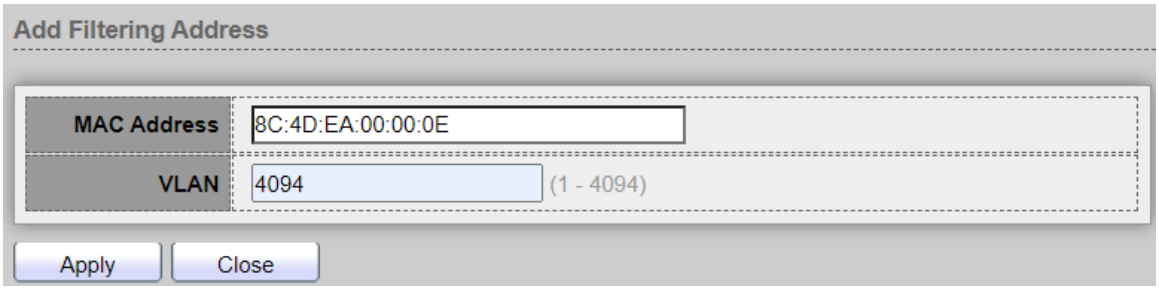
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

6.3 Filtering Address

Administrator can set need filtering MAC address in the MAC table. If MAC is added on table this MAC will be blocked, Setting **"add"** and "Edit" and **"Delete"** function for this management.



Field	Description
MAC Address	Specify unicast MAC address in the packets to be dropped.
VLAN	Specify the VLAN ID for the specific MAC address.



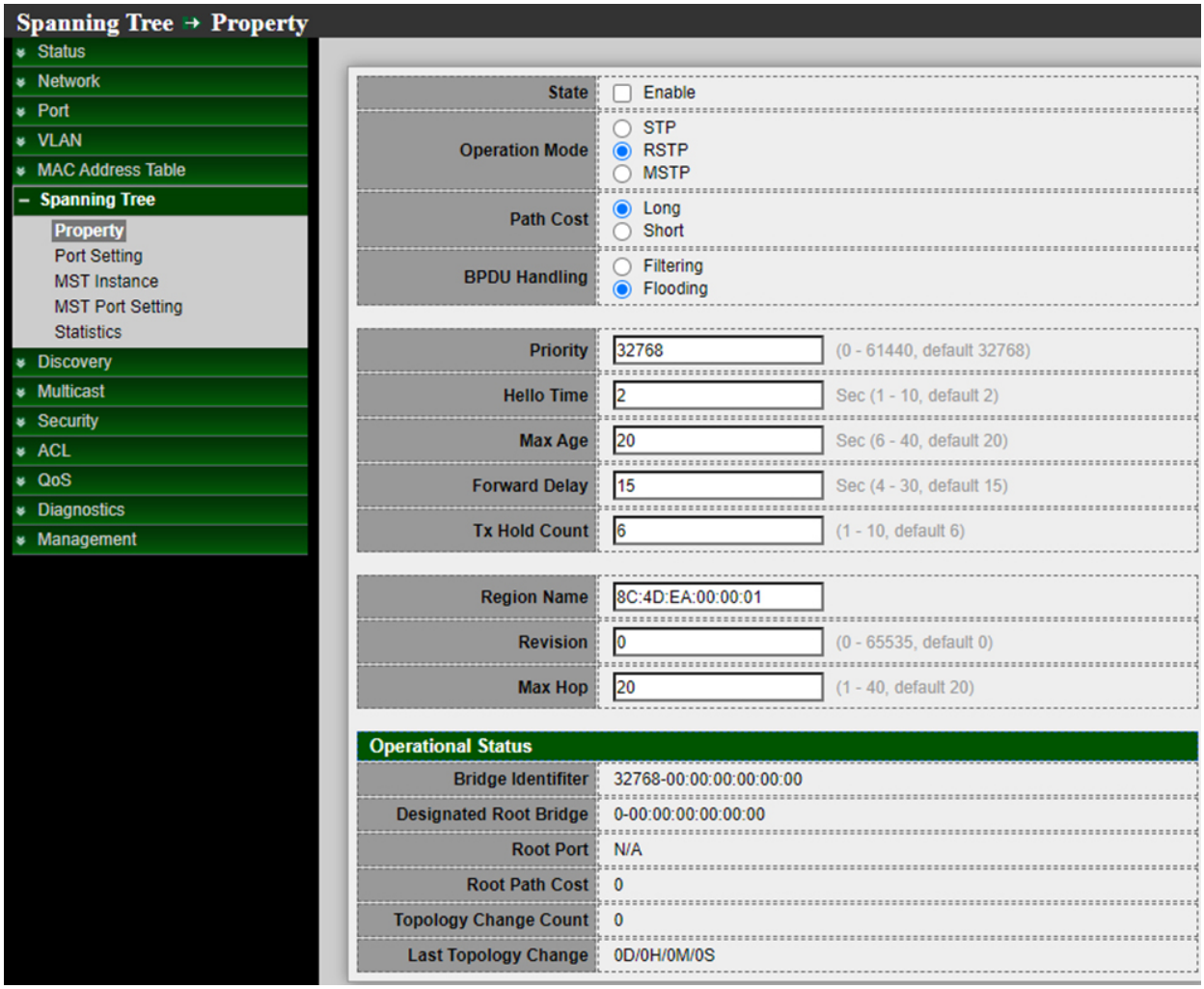
- **MAC Address :** Enter to specify the unicast MAC address in the packets to be dropped.
- **VLAN :** Enter a VLAN ID that specifies a specific MAC address.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

7. Spanning Tree

Spanning Tree function allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If Spanning Tree costs change, or if one network segment in the Spanning Tree becomes unreachable, the spanning tree algorithm reconfigures the spanning tree topology and reestablishes the link by activating the standby path. Without spanning tree in place, it is possible that both connections may be simultaneously live, which could result in an endless loop of traffic on the LAN.

7.1 Property



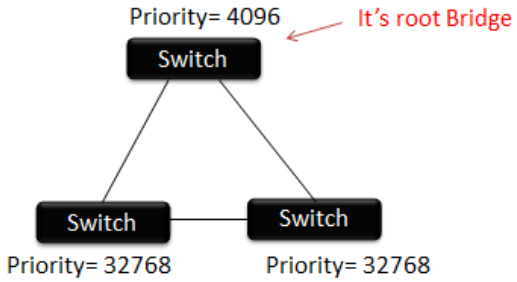
- **State:** Administrator can choose Enable or Disable this function.
- **Operation Mode:** Administrator can choose use Spanning Tree (STP) or Rapid Spanning Tree (RSTP) or Multiple Spanning Tree (MSTP).
- **Path Cost:** Administrator can choose STP judgment use Path cost for Long or Short.

- **Long :** Specifies that the default port path costs are within the range: 1-200,000,000.
- **Short:** Specifies that the default port path costs are within the range:1-65,535.

➢ **BPDU Handling:** When the Switch receives the BPDU frame, Administrator can choose the BPDU Handling mode for Filtering or Flooding. Specify the BPDU forward method when the STP is disabled.

- **Filtering :** Filter the BPDU when STP is disabled.
- **Flooding :** Flood the BPDU when STP is disabled.

➢ **Priority:** Administrator can set bridge priority, default is 32768. The lower value (priority) is the root bridge. Specify the bridge priority. The valid range is from 0 to 61440, and the value should be the multiple of 4096. It ensures the probability that the switch is selected as the root bridge, and the lower value has the higher priority for the switch to be selected as the root bridge of the topology.



➢ **Hello Time:** The hello time is the time between each bridge protocol data unit (BPDU) that is sent on a port. This time is equal to 2 seconds (sec) by default, but you can tune the time to be between 1 and 10 sec.

➢ **Max. Age / Forward delay :** *2*(Forward Delay-1) >=* ***Max Age*** *>= 2*(Hello Time+1),* the time interval in seconds for a switch to wait the configuration messages, without attempting to redefine its own configuration.

➢ **Forward Delay :** Specify the STP forward delay time, which is the amount of time that a port remains in the Listening and Learning states before it enters the Forwarding state. Its valid range is from 4 to 10 seconds.

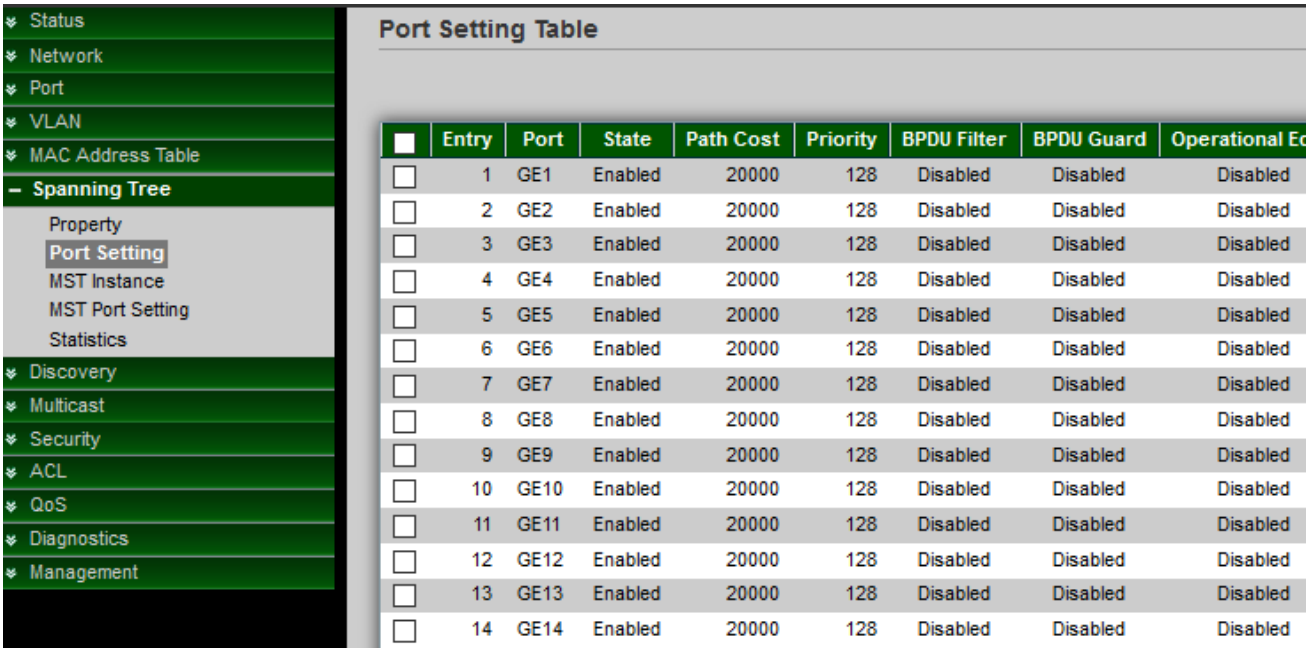
➢ **TX hold Count:** Specify the tx-hold-count used to limit the maximum numbers of packets transmission per second. The valid range is from 1 to 10.

➢ **Region Name:** The MSTP instance name. Its maximum length is 32 characters. The default value is the MAC address of the switch.

➢ **Revision:** Administrator every time change MST value, customary "Revision" to add 1 value. The MSTP revision number. Its valid rage is from 0 to 65535.

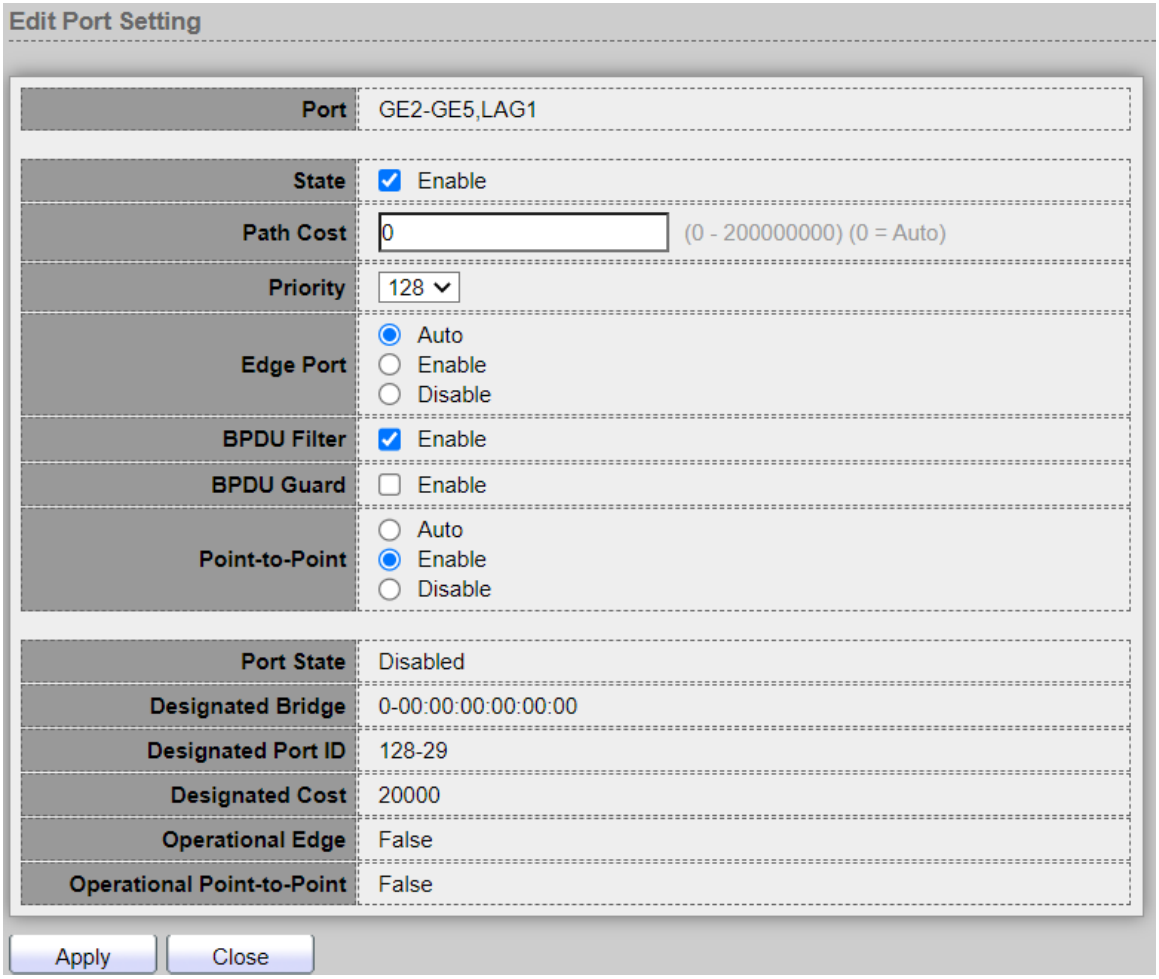
➢ **Max. Hop:** Set max. hop of switch. Specify the number of hops in an MSTP region before the BPDU is discarded. The valid range is 1 to 40.

7.2 Port Setting



Field	Description
Port	Specify the interface ID or the list of interface IDs.
State	The operational state on the specified port.
Path Cost	STP path cost on the specified port.
Priority	STP priority on the specified port.
BPDU Filter	The states of BPDU filter on the specified port.
BPDU Guard	The states of BPDU guard on the specified port.
Operational Edge	The operational edge port status on the specified port.
Operational Point-to-Point	The operational point-to-point status on the specified port.
Port Role	The current port role on the specified port. The possible values are: "Disabled", "Master", "Root", "Designated", "Alternative", and Backup".
Port State	The current port state on the specified port. The possible values are: "Disabled", "Discarding", "Learning", and "Forwarding".

Designated Bridge	The bridge ID of the designated bridge.
Designated Port ID	The designated port ID on the switch.
Designated Cost	The path cost of the designated port on the switch.



- **State:** Administrator can set Enable or Disable.
- **Path Cost:** Path Cost (1-200000000) This parameter is used determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short, the maximum path cost is 65,535. Range: 1-200000000, (set 0 = Auto, default is 0).
- **Priority:** If the path cost for all ports on a switch is the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. Where more than

one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. Range: 0-240, default is 128.

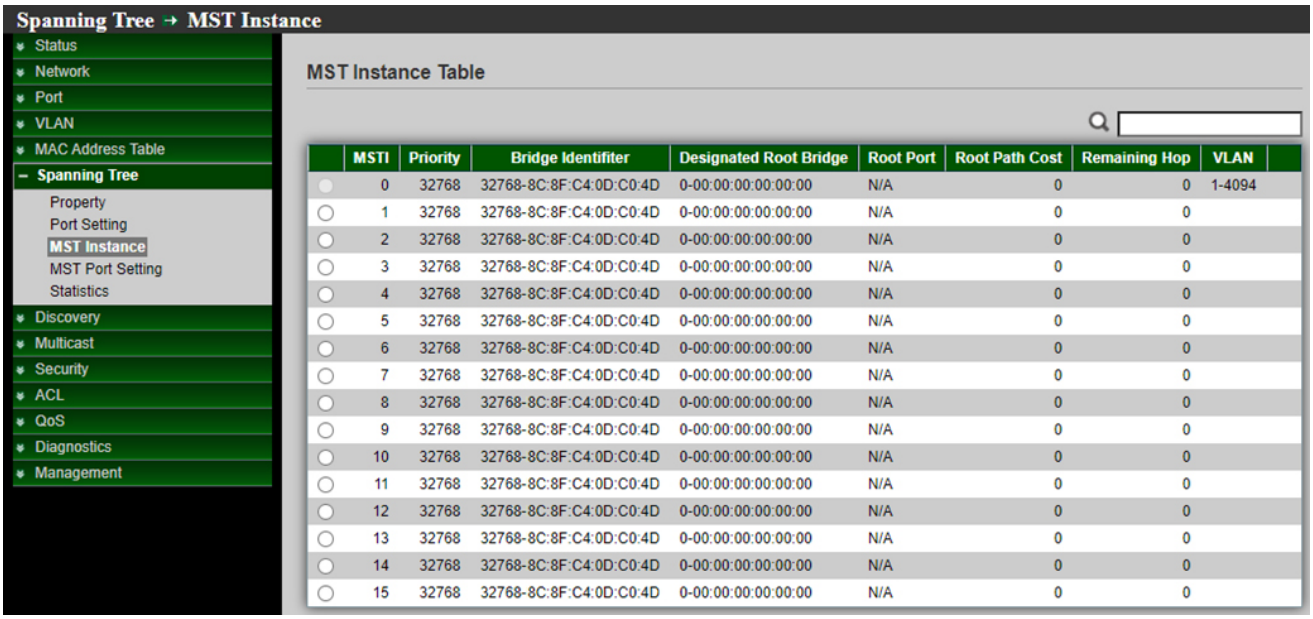
- **Edge Port:** Specify the edge mode..
  - **Enable :** Force to true state (as link to a host).
  - **Disable :** Force to false state (as link to a bridge).

  In the edge mode, the interface would be put into the Forwarding state immediately upon link up. If the edge mode is enabled for the interface and there are BPDUs received on the interface, the loop might be occurred in the short time before the STP state change.
- **BPDU Filter :** The BPDU Filter configuration avoids receiving/transmitting BPDU from the specified ports.
  - **Enable :** Enable BPDU filter function.
  - **Disable :** Disable BPDU filter function.
- **BPDU Filter :** The BPDU Guard configuration to drop the received BPDU directly.
  - **Enable :** Enable BPDU guard function.
  - **Disable :** Disable BPDU guard function.
- **Point-to-Point :** Specify the Point-to-Point port configuration:
  - **Auto :** The state is depended on the duplex setting of the port.
  - **Enable :** Force to true state.
  - **Disable:** Force to false state.
- **Port State :** The current port state on the specified port. The possible values are : "Disabled", "Discarding", "Learning", and "Forwarding".
- **Designated Bridge :** The bridge ID of the designated bridge.
- **Designated Port ID :** The designated port ID on the switch.
- **Designated Cost :** The path cost of the designated port on the switch.
- **Operational Edge :** Show the "false" and "true" status.
- **Operational Point-to-Point :** Show the "false" and "true" status.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

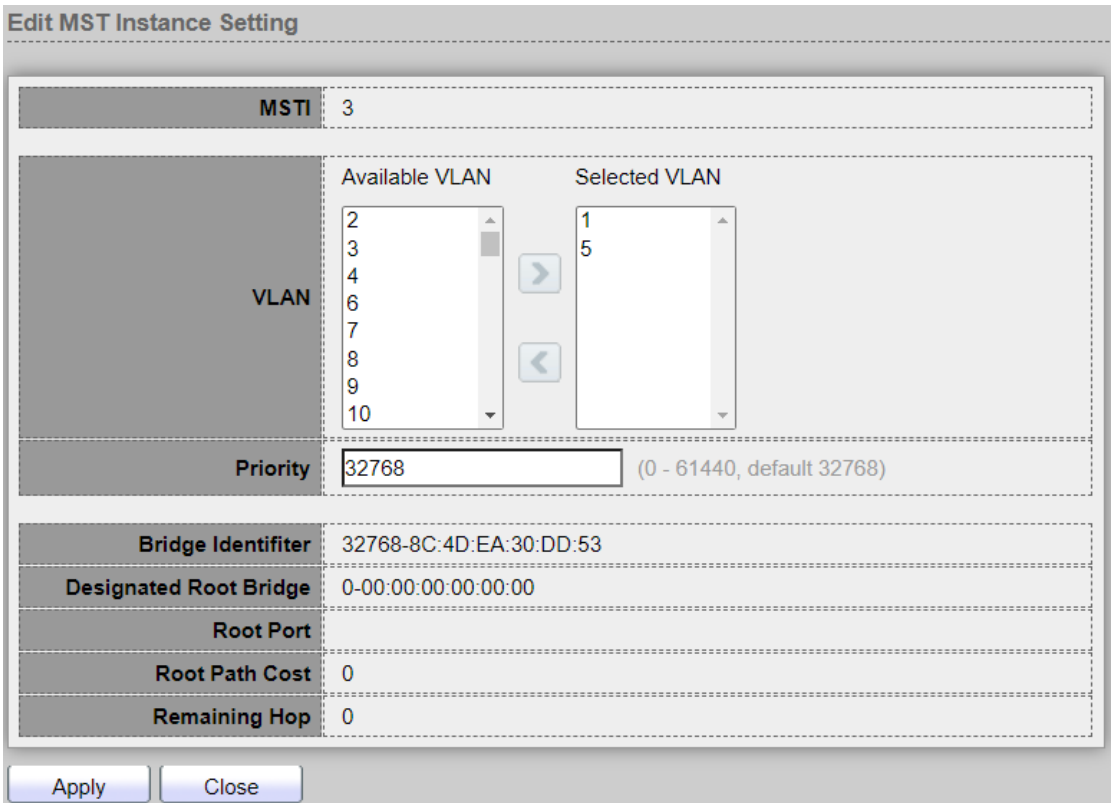
7.3 MST Instance

MST can have multiple sets of STP instances. Each instance is independently formed as a logical spanning tree. And instance has its own VLAN and port state, can independently set the priority of each port.



MSTI	Priority	Bridge Identifiter	Designated Root Bridge	Root Port	Root Path Cost	Remaining Hop	VLAN
0	32768	32768-8C:8F:C4:0D:C0:4D	0-00:00:00:00:00:00	N/A	0	0	1-4094
1	32768	32768-8C:8F:C4:0D:C0:4D	0-00:00:00:00:00:00	N/A	0	0	
2	32768	32768-8C:8F:C4:0D:C0:4D	0-00:00:00:00:00:00	N/A	0	0	
3	32768	32768-8C:8F:C4:0D:C0:4D	0-00:00:00:00:00:00	N/A	0	0	
4	32768	32768-8C:8F:C4:0D:C0:4D	0-00:00:00:00:00:00	N/A	0	0	
5	32768	32768-8C:8F:C4:0D:C0:4D	0-00:00:00:00:00:00	N/A	0	0	
6	32768	32768-8C:8F:C4:0D:C0:4D	0-00:00:00:00:00:00	N/A	0	0	
7	32768	32768-8C:8F:C4:0D:C0:4D	0-00:00:00:00:00:00	N/A	0	0	
8	32768	32768-8C:8F:C4:0D:C0:4D	0-00:00:00:00:00:00	N/A	0	0	
9	32768	32768-8C:8F:C4:0D:C0:4D	0-00:00:00:00:00:00	N/A	0	0	
10	32768	32768-8C:8F:C4:0D:C0:4D	0-00:00:00:00:00:00	N/A	0	0	
11	32768	32768-8C:8F:C4:0D:C0:4D	0-00:00:00:00:00:00	N/A	0	0	
12	32768	32768-8C:8F:C4:0D:C0:4D	0-00:00:00:00:00:00	N/A	0	0	
13	32768	32768-8C:8F:C4:0D:C0:4D	0-00:00:00:00:00:00	N/A	0	0	
14	32768	32768-8C:8F:C4:0D:C0:4D	0-00:00:00:00:00:00	N/A	0	0	
15	32768	32768-8C:8F:C4:0D:C0:4D	0-00:00:00:00:00:00	N/A	0	0	

Field	Description
MSTI	MST instance ID.
Priority	The bridge priority on the specified MSTI.
Bridge Identifier	The bridge identifier on the specified MSTI.
Designated Root Bridge	The designated root bridge identifier on the specified MSTI.
Root Port	The designated root port on the specified MSTI.
Root Path Cost	The designated root path cost on the specified MSTI.
Remaining Hop	The configuration of remaining hop on the specified MSTI.
VLAN	The VLAN configuration on the specified MSTI.

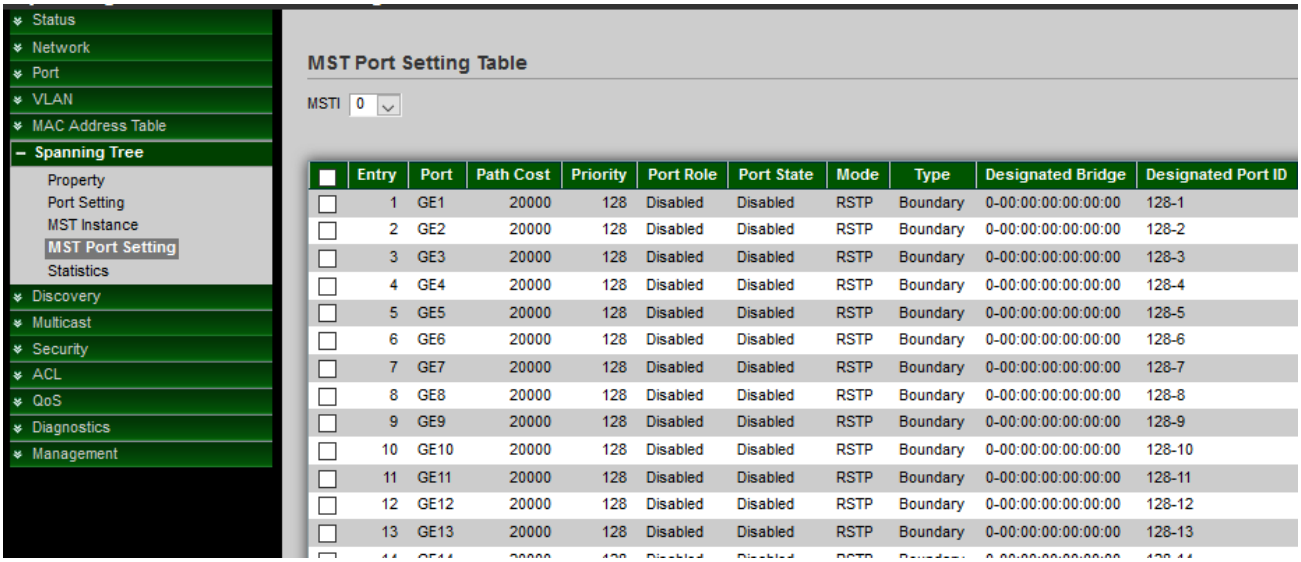


- **VLAN :** Select the VLAN list for the specified MSTI.
- **Priority:** Specify the bridge priority on the specified MSTI. The valid range is from 0 to 61440, and the value must be the multiple of 4096. It ensures the probability that the switch is selected as the root bridge, and the lower values has the higher priority for the switch to be selected as the root bridge of the STP topology.
- **Bridge Identifier:** Displays the priority and MAC address of the Root Bridge for the selected MST instance.
- **Root Port:** Displays the root port of the selected MST instance.
- **Root Path Cost:** Displays the root path cost of the selected MST instance.
- **Remaining Hops:** Displays the number of hops remaining to the next destination.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

7.4 MST Port Setting

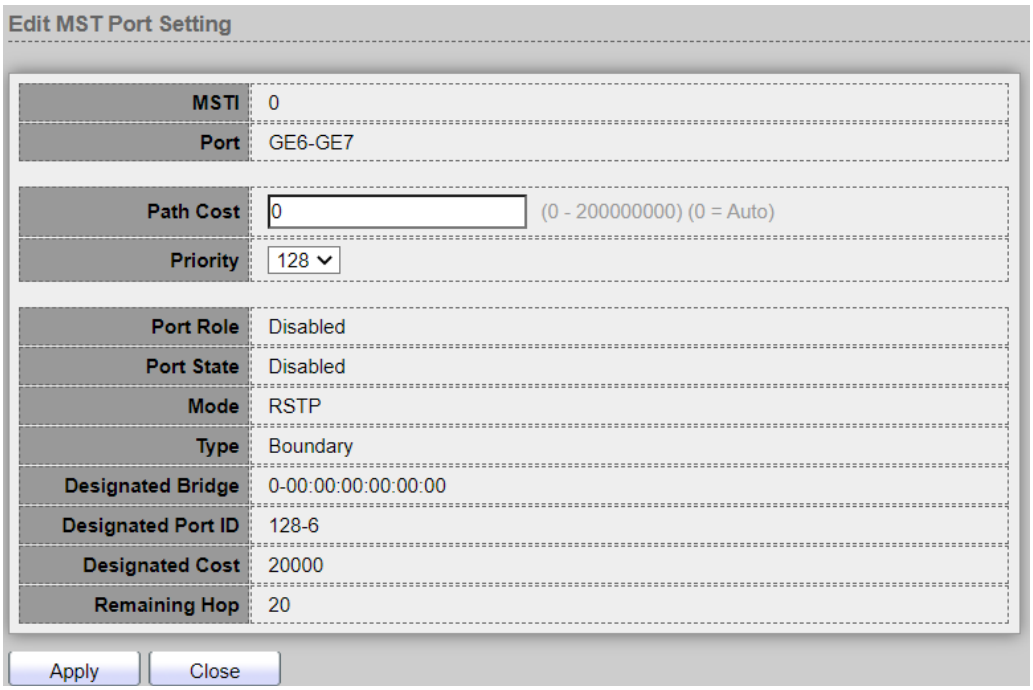
MST (Multiple Spanning Tree) is an extension to RST (Rapid Spanning Tree). MST further develops the usefulness of VLANs. MST configures a separate spanning tree for each VLAN group and blocks all but one possible alternate path within each spanning tree. A Multiple Spanning Tree Instance (MSTI) calculates and builds a loop-free topology to bridge packets from the VLANs that map to the instance.



MST Port Settings is used to configure the port MSTP settings for every MST instance. It is also used to view statistics that have been learned from the protocol.

Field	Description
MSTI	Specify the port setting on the specified MSTI.
Port	Specify the interface ID or the list of interface IDs.
Path Cost	The port path cost on the specified MSTI.
Priority	The port priority on the specified MSTI.
Port Role	The current port role on the specified port. The possible values are: “Disabled”, “Master”, “Root”, “Designated”, “Alternative”, and “Backup”.
Port State	The current port state on the specified port. The possible values are: “Disabled”, “Discarding”, “Learning”, and “Forwarding”.
Mode	The operational STP mode on the specified port.
Type	The possible value for the port type are: • **Boundary**: The port attaching an MST Bridge to a LAN that is not in the same region. • **Internal**: The port attaching an MST Bridge to a LAN that is not in the same region.
Designated Bridge	The bridge ID of the designated bridge.

Designated Port ID	The designated port ID on the switch.
Designated Cost	The path cost of the designated port on the switch.
Remaining Hop	The remaining hops count on the specified port.



- **MTSI :** Specify the port setting on the specified MSTI.
- **Port :** Specify the interface ID or the list of interface IDs..
- **Path Cost:** Specify the STP port path cost on the specified MSTI,Path cost default value is 0 (auto) depends on source device rate.
  If network is a loop occurs, the MST uses cost when selecting an interface to put in the forwarding state. Administrator can assign lower cost values to interfaces that you want selected first and higher cost values that you want selected last. If all interfaces have the same cost value, the MST puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.
- **Priority:** Specify the STP port priority on the specified MSTI,Administrator can configure the MTP priority and make it more likely that the switch will be chosen as the root switch.
- **Port Role:** Displays the port role per instance, assigned by the MSTP algorithm to provide STP paths. The current port role on the specified port. The possible values are :
  "Disabled", "Master", "Root", "Designated", "Alternative", and "Backup".
- **Port State:** The current port state on the specified port. The possible values are:

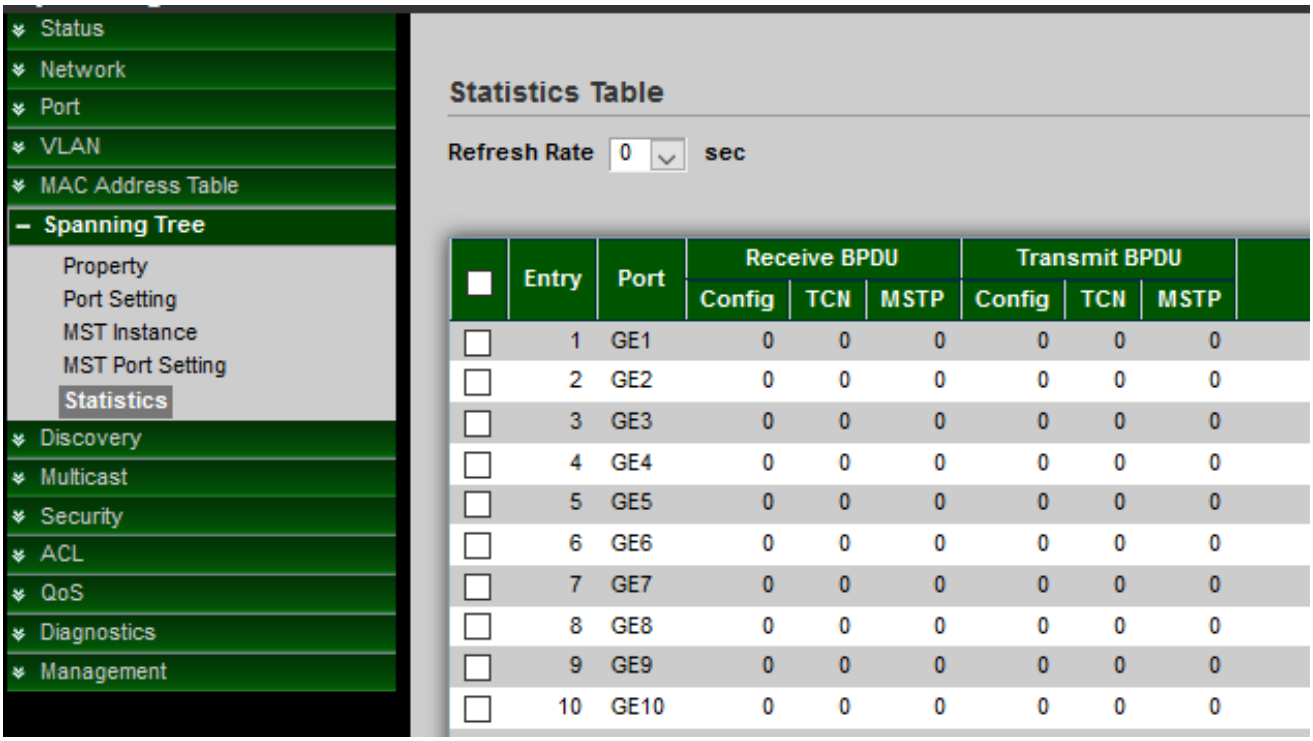
"Disabled", "Discarding", "Learning", and "Forwarding".

- **Mode:** The operational STP mode on the specified port.
  - **RSTP:** RSTP is enabled on the port.
  - **STP:** Classic STP is enabled on the port.
  - **MSTP:** MSTP is enabled on the port.
- **Type :** Displays the MSTP type of the port. The possible value for the port type are :
  - **Boundary :** The port attaching an MST Bridge to a LAN that is not in the same region.
  - **Internal:** The port attaching an MST Bridge to a LAN that is not in the same region.
- **Designated Bridge:** Displays the bridge ID number that connects the link or shared LAN to the root.
- **Designated Port ID:** Displays the priority and port ID on the designated bridge that connects the link or the shared LAN to the root.
- **Designated Cost:** Displays the cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
- **Remaining Hops :** Displays the hops remaining to the next destination.

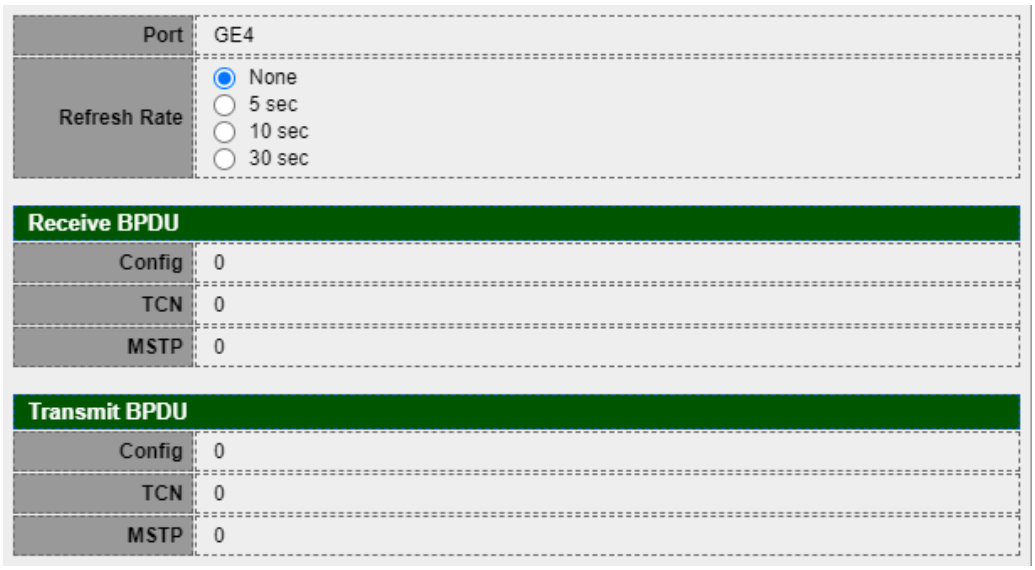
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

7.5 Statistics

This page can check Receive / Transmit BPDU information of the STP Port.



Field	Description
Refresh Rate	The option to refresh the statistics automatically.
Receive BPDU (Config)	The counts of the received CONFIG BPDU.
Receive BPDU (TCN)	The counts of the received TCN BPDU.
Receive BPDU (MSTP)	The counts of the received MSTP BPDU.
Transmit BPDU (Config)	The counts of the transmitted CONFIG BPDU.
Transmit BPDU (TCN)	The counts of the transmitted TCN BPDU.
Transmit BPDU (MSTP)	The counts of the transmitted MSTP BPDU.
Clear	Clear the statistics for the selected interfaces
View	View the statistics for the interface.



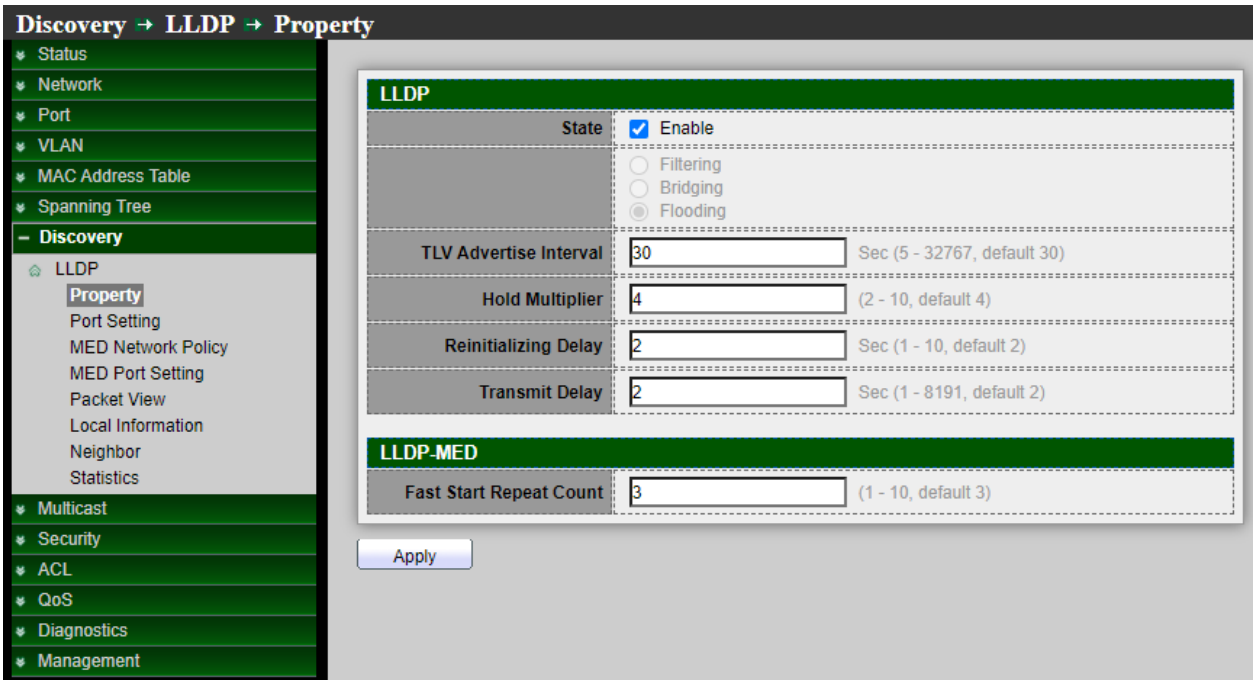
- **Refresh Rate :** The option to refresh the statistics automatically : None , 5 sec , 10 sec , 30sec for refresh level.
- **Clear :** Clear the statistics for the selected interfaces.

8. Discovery(LLDP)

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet.

LLDP information is sent by devices from each of their interfaces at a fixed interval, in the form of an Ethernet frame. Each frame contains one LLDP Data Unit (LLDPDU). Each LLDPDU is a sequence of type-length-value (TLV) structures.

8.1 Property



- **State:** Administrator can choose Enable or disable this LLDP function.
- **LLDP Handing:** If cancel checkbox then administrator can choose Filtering / Bridging / Flooding for LLDP handing. Select LLDP PDU handling action to be filtered, bridging or flooded when LLDP is globally disabled
  - **Filtering:** Deletes the packet.
  - **Bridging:** (VLAN-aware flooding) Forwards the packet to all VLAN members.
  - **Flooding:** Forwards the packet to all ports
- **TLV Advertise Interval:** Select the interval at which frames are transmitted. (range 5-32760, default is 30)
- **Hold Multiplier:** Set Hold value (Range 2-10, default is 4). Administrator can control the aging time of local information on the neighbor device by configuring the value of the Hold multiplier.

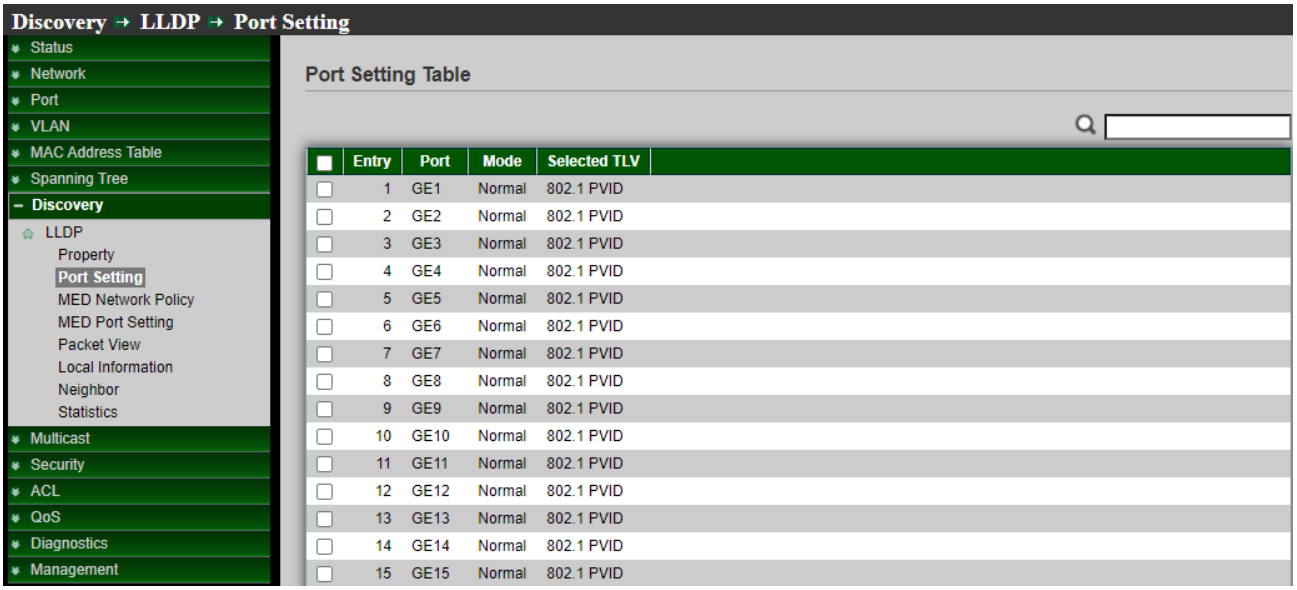
*TTL=Hold multiplier * TLV Advertise Interval.*

- **Reinitializing Delay:** S Select the delay before a re-initialization (range 1–10 seconds, default = 2)..
- **Transmit Delay:** Select the delay after an LLDP frame is sent (range 1–8191 seconds, default = 3).
- **Fast Start Repeat Count:** The fast start repeat count when port link up(range 1–10,default = 3).

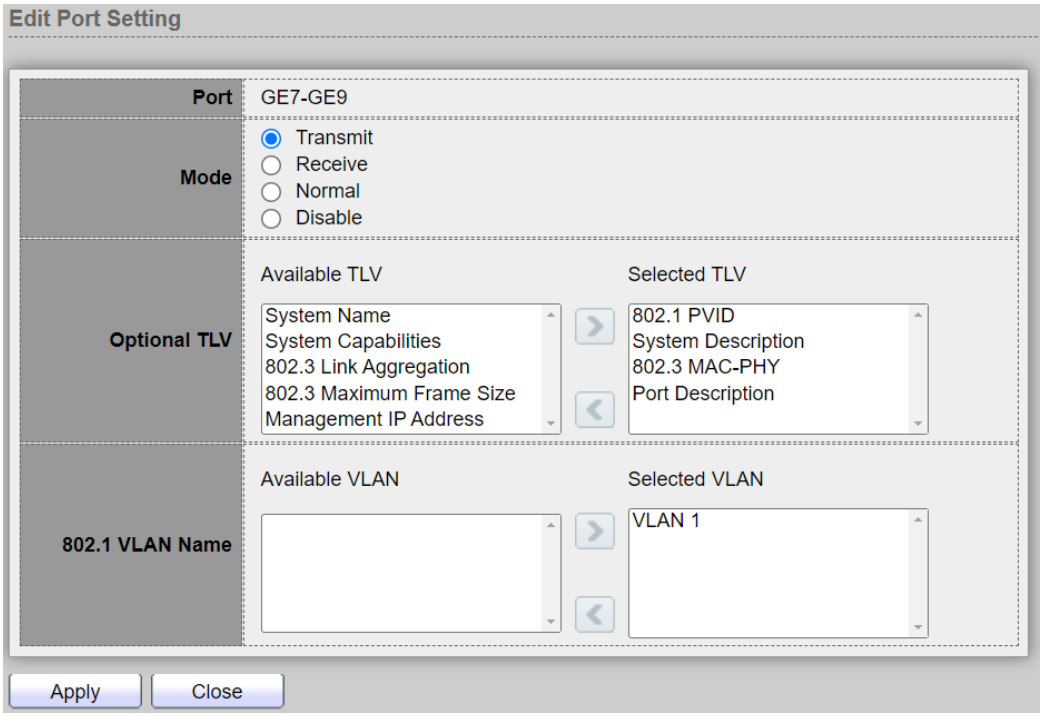
*Click the **"Apply"** button to save your changes settings.*

8.2 Port Setting

Administrator can configure each port of the LLDPDU Transmit / Receive / Normal or Disable the mode and choose from "Optional TLV" list send the TLV type of port.



Field	Description
Port	Display the port of LLDP state.
Mode	Display the Transmit (TX Only),Receive (RX Only),Normal (TX And RX),Disable
Selected TLV	Display the TLVs for your selected.

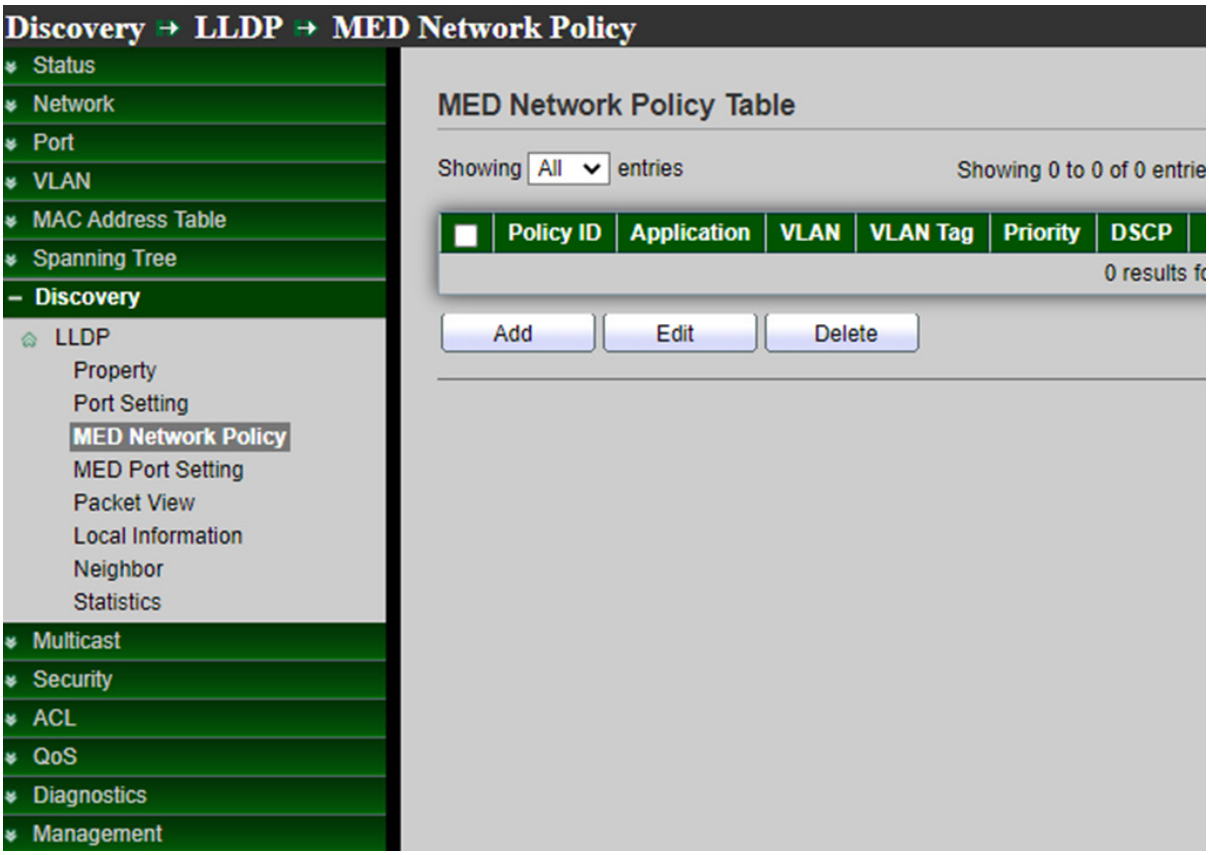


- **Mode :** Administrator can choose Transmit(TX) / Receive(RX) or Normal(TX+RX) and Disable, if choose disable will don't send and receive LLDPDU.
  - Transmit (TX Only): Transmit LLDP PDUs only.
  - Receive (RX Only): Receive LLDP PDUs only.
  - Normal (TX And RX): Transmit and receive LLDP PDUs both
  - Disable : Disable the transmission of LLDP PDUs
- **Optional TLV :** Administrator can be configuration information into different TLV, encapsulates LLDPDU and issued to the neighbor device.
  - System Name
  - Port Description
  - System Description
  - System Capability
  - 802.3 MAC-PHY
  - 802.3 Link Aggregation
  - 802.3 Maximum Frame Size
  - Management Address
  - 802.1 PVID
- **802.1 VLAN Name :** Select the VLAN Name ID to be carried (multiple selection is allowed).

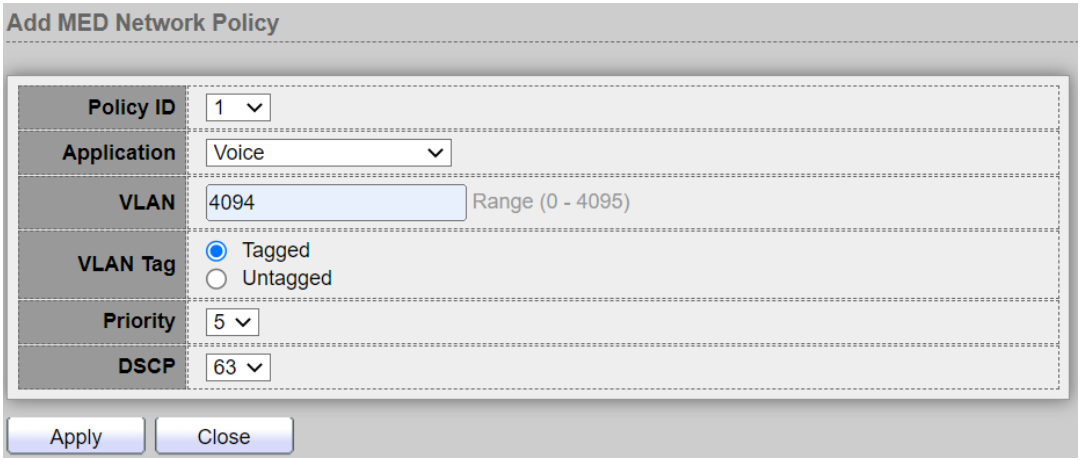
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

8.3 MED Network Policy

Administrator can see the display for LLDP MED Network Policy Setting, Setting **"add"** and "Edit" and **"Delete"** function for this management.



Field	Description
Policy ID	Display the policy ID.
Application	Display the network policy type.
VLAN	Display the VLAN ID.
VLAN Tag	Display the VLAN tag status.
Priority	Display the L2 priority.
DSCP	Display the DSCP value.

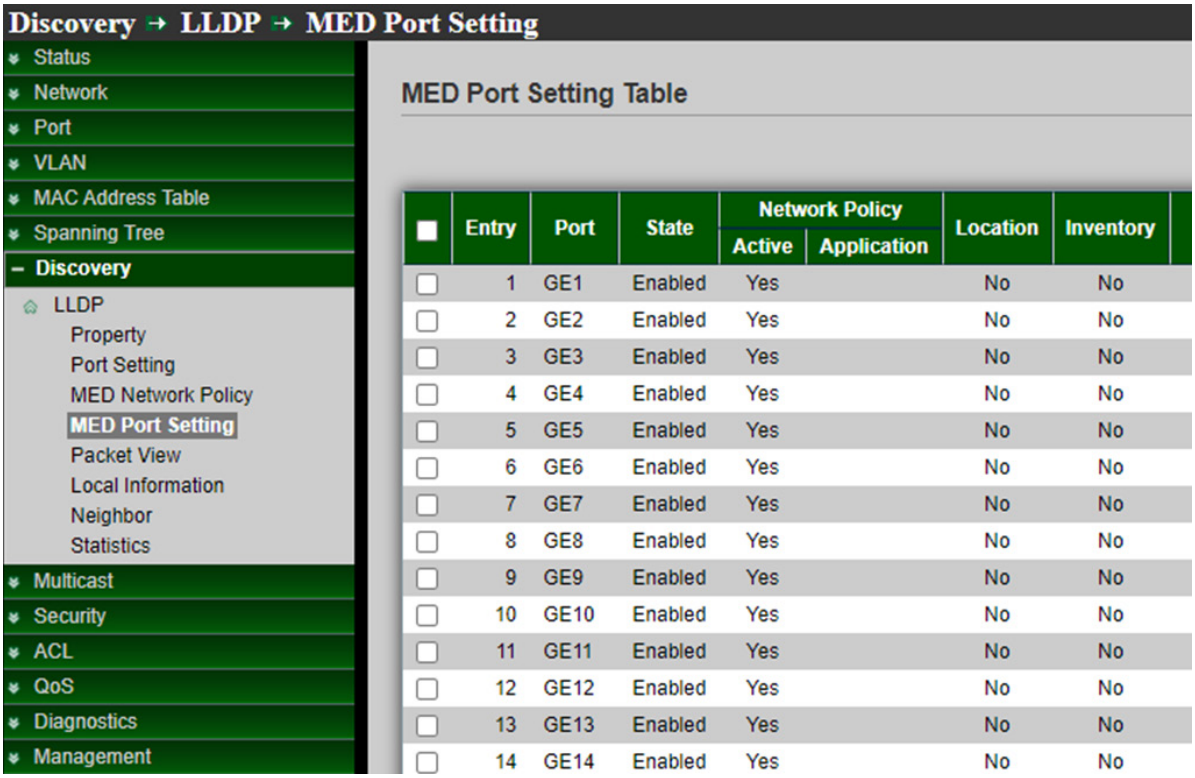


- **Policy ID :** Select specified network policy ID to configure..
- **Application : S**elect the network policy application type.
  - Voice
  - Voice Signaling
  - Guest Voice
  - Guest Voice Signaling
  - Softphone Voice
  - Video Conferencing
  - App Streaming Video
  - VideoSignaling
- **VLAN :** Set the VLAN ID, range from 1 to 4094..
- **VLAN Tag :** Set the VLAN tag status.
- Select the network policy application type.
  - **Tagged :** Traffic is tagged.
  - **Untagged :** Traffic is untagged.
- **Priority :** Set the L2 priority, range from 0 to 7.
- **DSCP :** Set the DSCP value, range from 0 to 63.

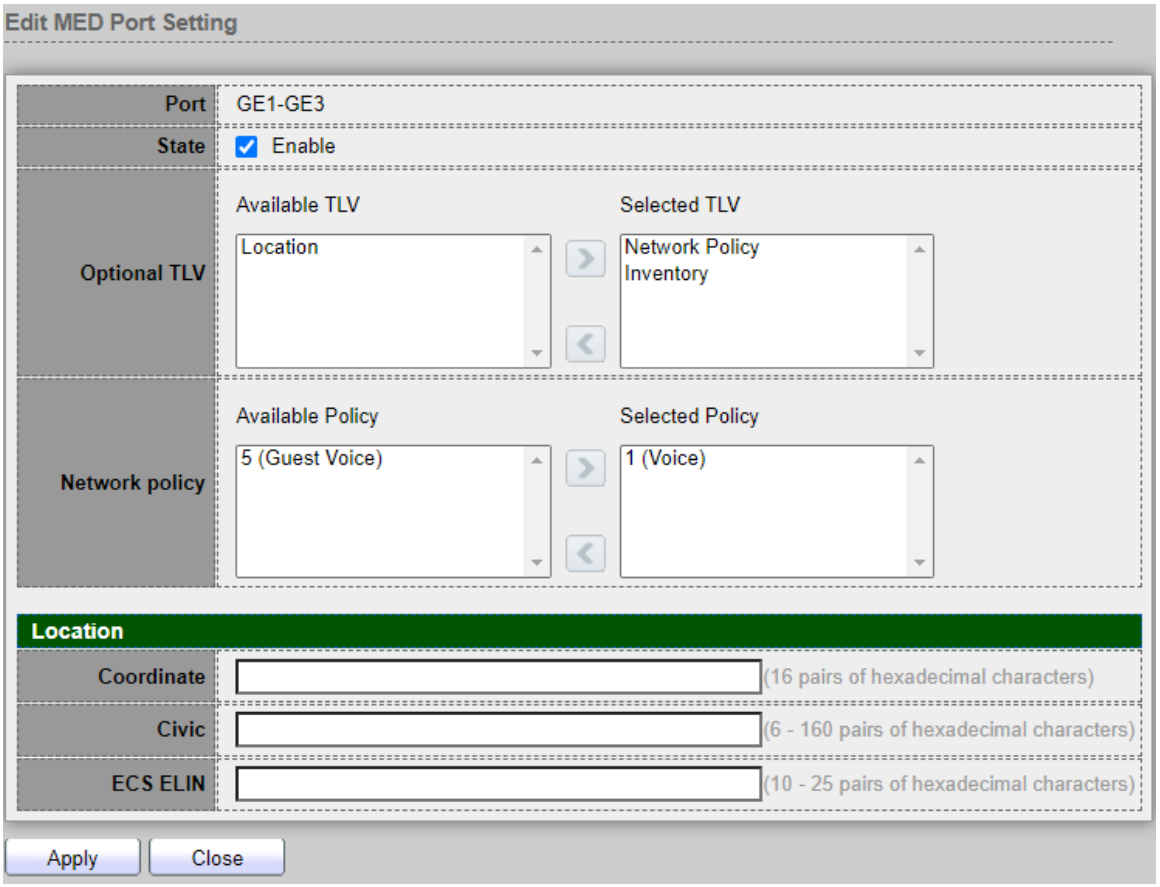
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

8.4 MED Port Setting

Administrator can see the display for LLDP MED Port Setting.



Field	Description
Port	Display the LLDP MED specified port.
State	Display the LLDP MED status
Optional TLV	Display the LLDP MED optional TLVs.
Network Policy	Display the LLDP MED network policy Active and Application IDs.
Location	Display the location status.
Inventory	Display the inventory by yes or no.

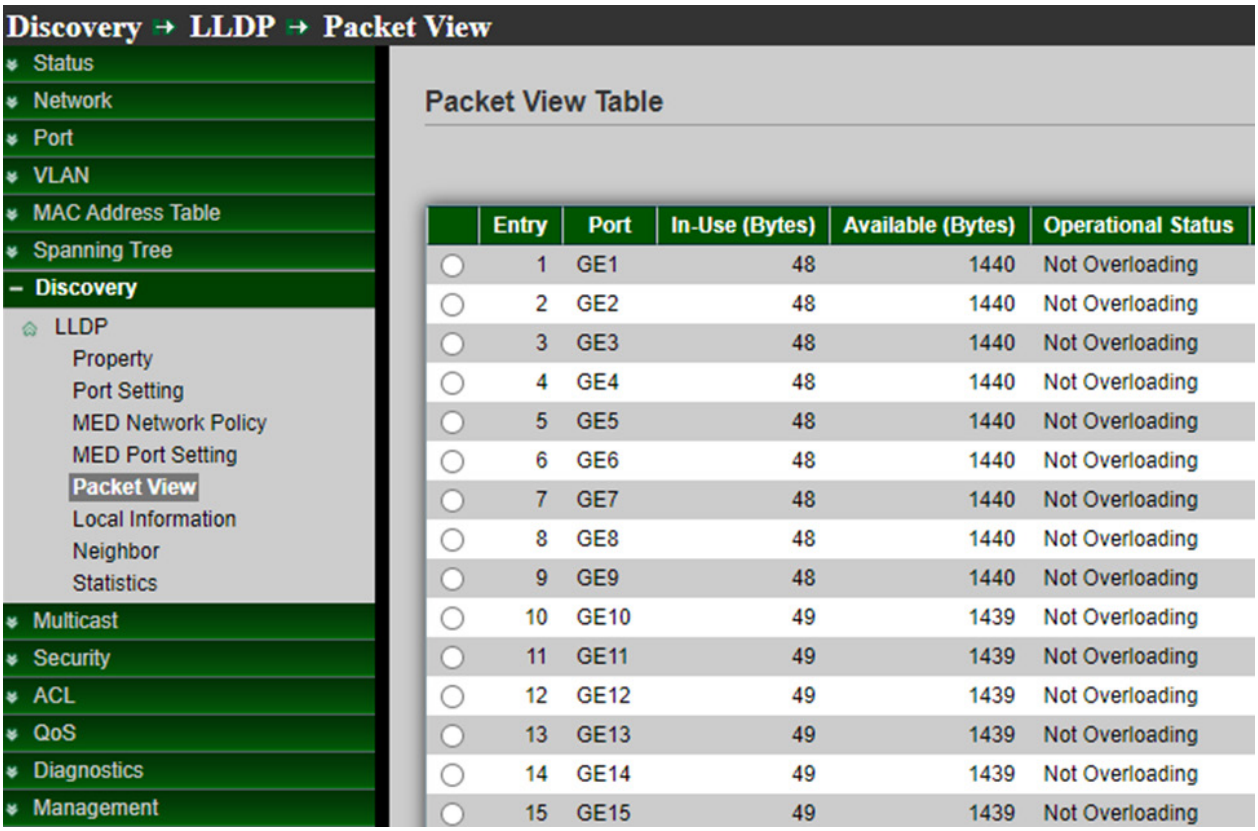


- **Port :** Select specified port or all ports to configure LLDP MED.
- **State :** Select LLDP MED enable status
- **Optional TLV :** Select LLDP MED optional TLVs (multiple selection is allowed).
  - Network Policy
  - Location
  - Inventory
- **Network Policy :** Select the network policy IDs to be bound to ports. The network policy should be created in MED Network Policy page at first.
- **Location:**
  - **Coordinate : Set Coordinate**
  - **Civic : Set Civic**
  - **ECS ELIN : Set ECS ELIN**

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

8.5 Packet View

Administrator can select which port to view and click on the "**Detail**" button to view the information of the LLDP packet on the selected port.



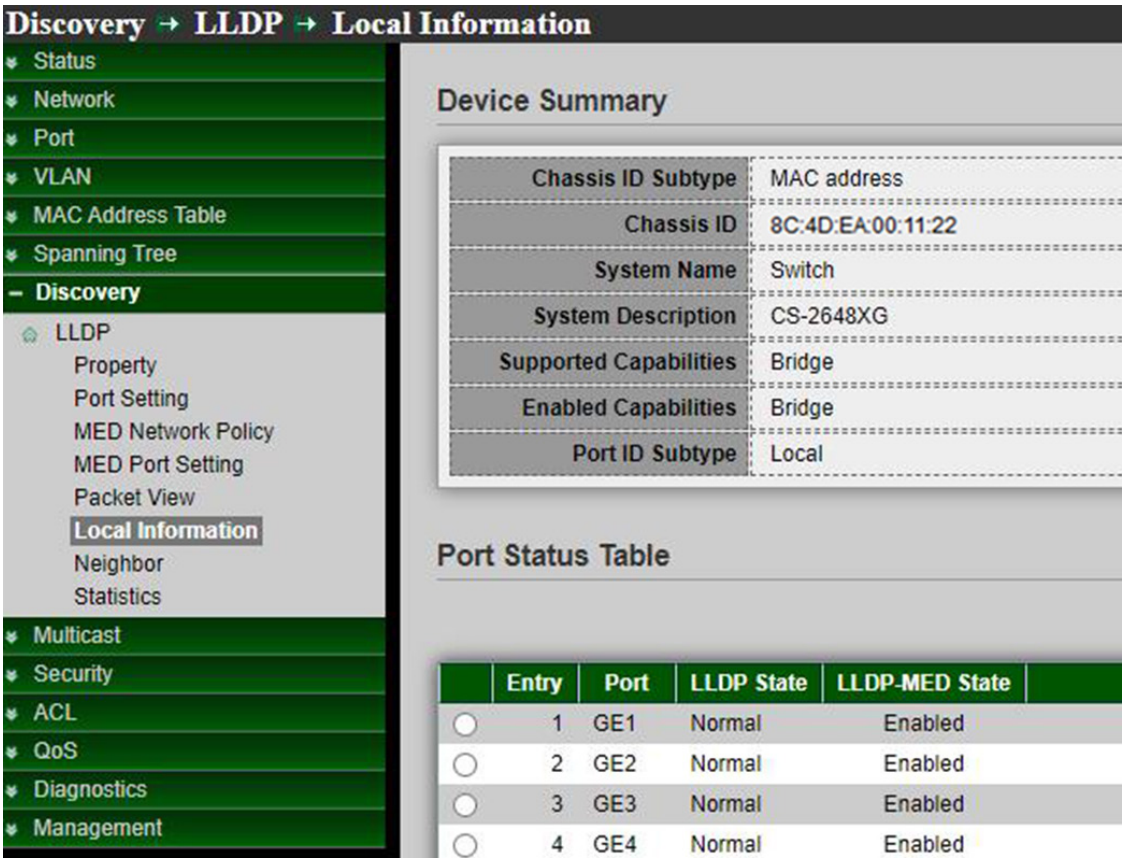
Field	Description
Port	Port Name
In-Use (Bytes)	Total number of bytes of LLDP information in each packet.
Available (Bytes)	Total number of available bytes left for additional LLDP information in each packet.
Operational Status	Overloading or not

*Click the **"Close"** button to close the view detail page.*

Field	Description
Port	Port Name
Mandatory TLVs	Total mandatory TLV byte size. Status is sent or overloading.
MED Capabilities	Total MED Capabilities TLV byte size. Status is sent or overloading.
MED Location	Total MED Location byte size. Status is sent or overloading.
MED Network Policy	Total MED Network Policy byte size. Status is sent or overloading.
MED Inventory	Total MED Inventory byte size. Status is sent or overloading.
MED Extended Power via MDI	Total MED Extended Power via MDI byte size. Status is sent or overloading.
802.3 TLVs	Total 802.3 TLVs byte size. Status is sent or overloading.
Optional TLVs	Total Optional TLV byte size. Status is sent or overloading.
802.1 TLVs	Total 802.1 TLVs byte size. Status is sent or overloading.
Total	Total number of bytes of LLDP information in each packet.

8.6 Local Information

Displays switch summary and every port status of LLDP. Administrator can select which port to view and click on the "**detail**" button to view the information of the local device as well as the information of selected port LLDP property.



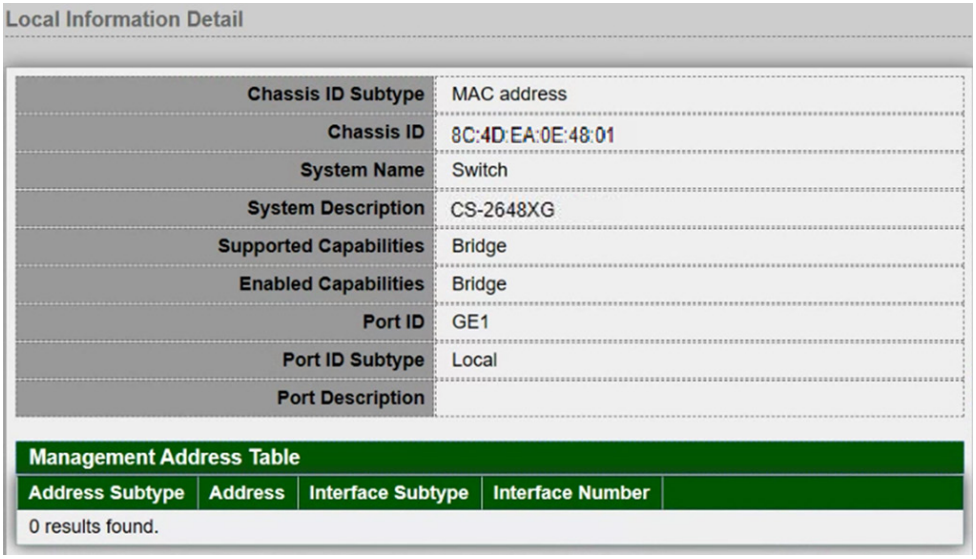
Device Summary

Field	Description
Chassis ID Subtype	Type of chassis ID, such as the MAC address.
Chassis ID	Identifier of chassis. Where the chassis ID subtype is a MAC address, the MAC address of the switch is displayed.
System Name	Name of switch.
System Description	Description of the switch.
Supported Capabilities	Primary functions of the device, such as Bridge, WLAN AP, or Router.
Enabled Capabilities	Primary enabled functions of the device.
Port ID Subtype	Type of the port identifier that is shown.

Port Status Table

Field	Description
Port	Type of the port number
LLDP Status	LLDP Tx and Rx abilities.
LLDP Med Status	LLDP MED enable state.

*Click **"detail"** button on the page to view detail information of the selected port.*



Management Address Table

Field	Description
Address Subtype	Type of the port number
Address	Display management IP address type.
Interface Subtype	Returned address most appropriate for management use, typically a Layer 3 address.
Interface number	Specific interface associated with this management address.

MAC/PHY Details

MAC/PHY Detail	
Auto-Negotiation Supported	True
Auto-Negotiation Enabled	True
Auto-Negotiation Advertised Capabilities	1000baseTFD , 100baseTXFD , 100baseTX , 10baseTFD , 10baseT
Operational MAU Type	Other

Field	Description
Auto-Negotiation Supported	Port speed auto-negotiation support status.
Auto-Negotiation Enabled	Port speed auto-negotiation active status.
Auto-Negotiation Advertised Capabilities	Port speed auto-negotiation capabilities, for example, 1000BASE-T half-duplex mode, 100BASE-TX full-duplex mode.
Operational MAU Type	Medium Attachment Unit (MAU) type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interfaces' collision detection and bit injection into the network, for example, 100BASE-TX full duplex mode.

802.3 Detail

802.3 Detail	
802.3 Maximum Frame Size	1522

Field	Description
802.3 Maximum Frame Size	The maximum supported IEEE 802.3 frame size.

802.3 Link Aggregation

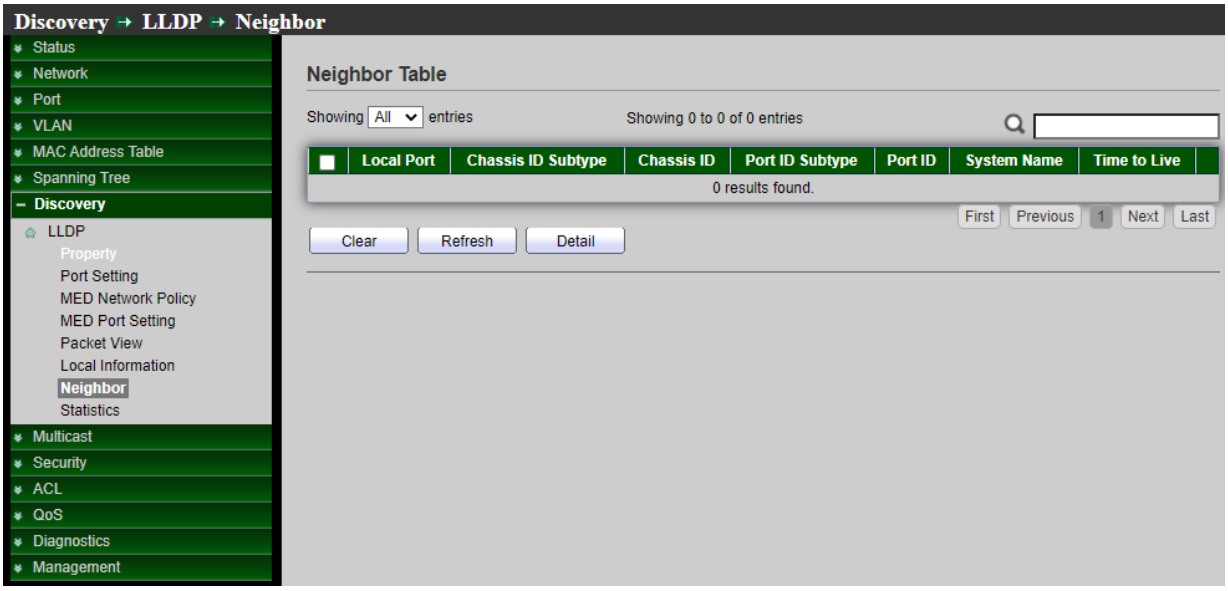
802.3 Link Aggregation	
Aggregation Capability	N/A
Aggregation Status	N/A
Aggregation Port ID	N/A

Field	Description
Aggregation Capability	Indicates whether the interface can be aggregated.
Aggregation Status	Indicates whether the interface is aggregated.
Aggregation Port ID	Advertised aggregated interface ID.

*Click the **"Close"** button to close the information page.*

8.7 Neighbor

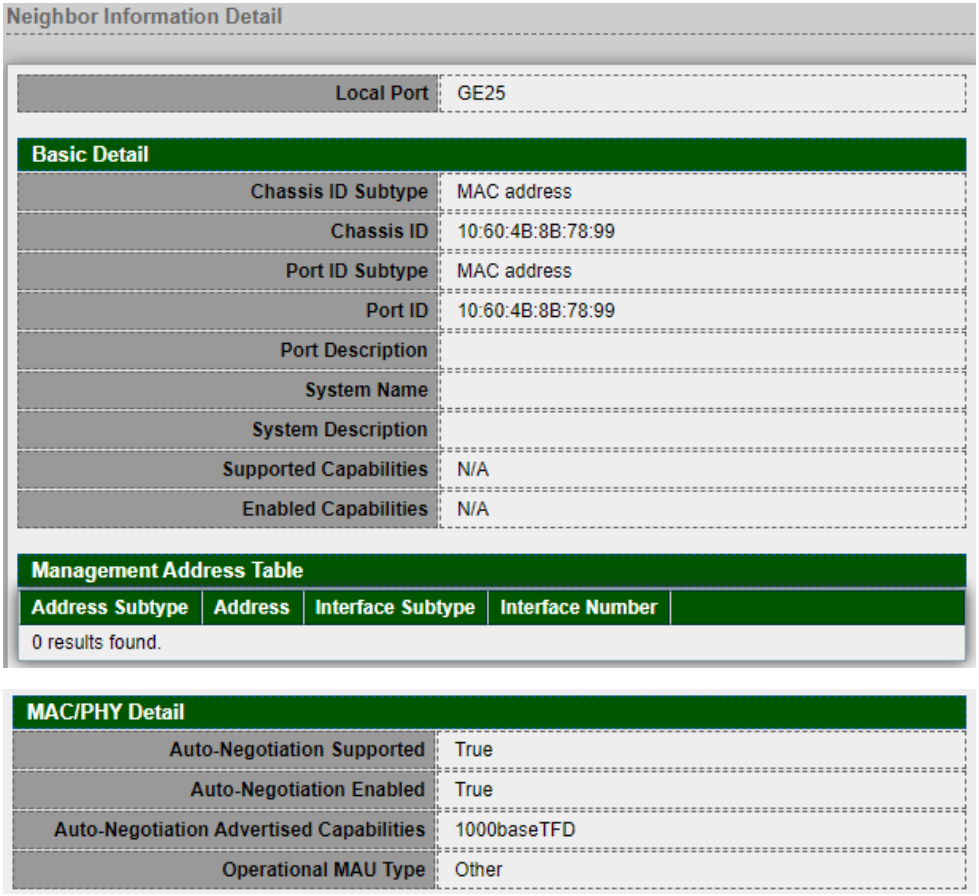
The page displays information that was received using the LLDP protocol from neighboring devices. After timeout the information is deleted. (Based on the value received from the neighbor time to Live TLV during which no LLDP PDU was received from a neighbor), Setting **"add"** and "Edit" and **"Delete"** function for this management.



Field	Description
Local Port	Number of the local port to which the neighbor is connected.
Chassis ID Subtype	Type of chassis ID (for example, MAC address).

Chassis ID	Identifier of the 802 LAN neighboring device's chassis.
Port ID Subtype	Type of the port identifier that is shown.
Port ID	Identifier of port.
System Name	Published name of the switch.
Time to Live	Time interval in seconds after which the information for this neighbor is deleted.

Click “detail” to view selected neighbor detail information.



802.3 Power via MDI	
MDI Power Support Port Class	N/A
PSE MDI Power Support	N/A
PSE MDI Power State	N/A
PSE Power Pair Control Ability	N/A
PSE Power Pair	N/A
PSE Power Class	N/A
Power Type	N/A
Power Source	N/A
Power Priority	N/A
PD Request Power Value	N/A
PSE Allocated Power Value	N/A

802.3 Detail	
802.3 Maximum Frame Size	N/A

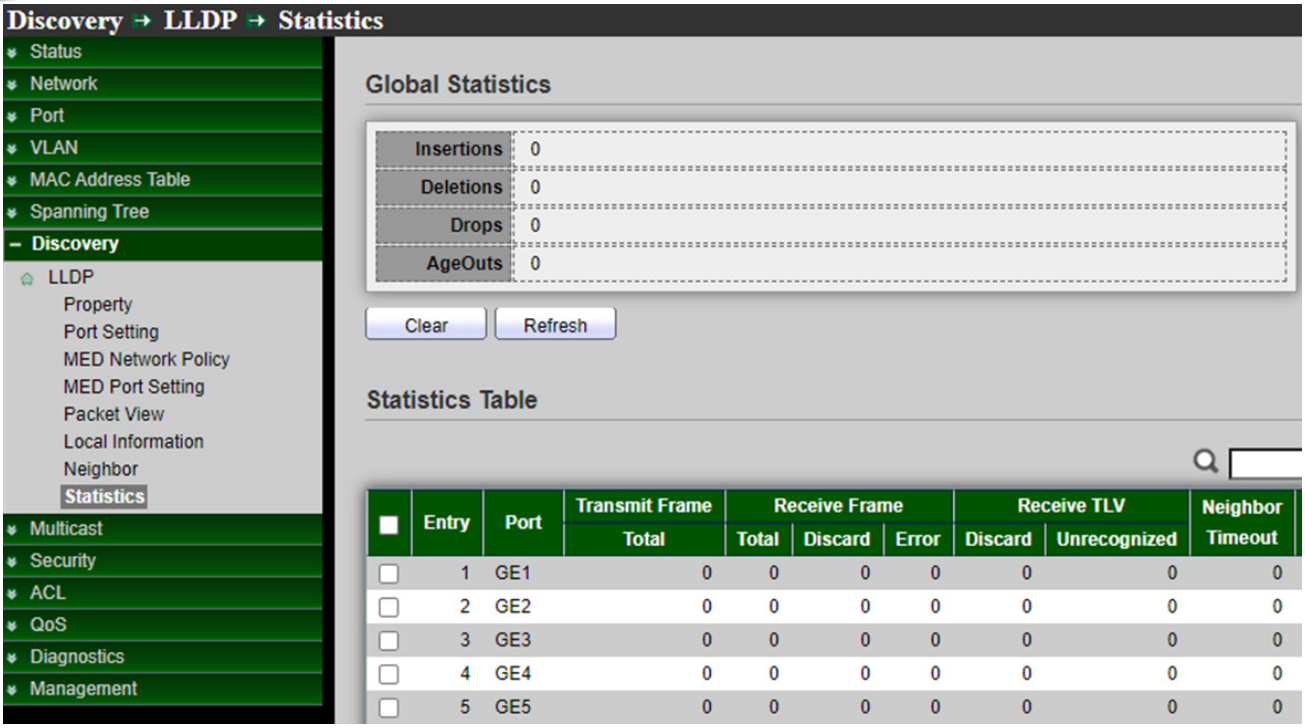
802.3 Link Aggregation	
Aggregation Capability	N/A
Aggregation Status	N/A
Aggregation Port ID	N/A

802.1 VLAN and Protocol	
PVID	
VLAN Name	N/A

*Click the **"Close"** button to close the information page.*

8.8 Statistics

This page displays LLDP statistical information per port. The Link Layer Discovery Protocol (LLDP) Statistics page displays summary and per-port information for LLDP frames transmitted and received on the switch.



Global Statistics

Field	Description
Insertions	The number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) has been inserted into tables associated with the remote systems.
Deletions	The number of times the complete set of information advertised by MSAP has been deleted from tables associated with the remote systems.
Drops	The number of times the complete set of information advertised by MSAP could not be entered into tables associated with the remote systems because of insufficient resources.
Age Outs	The number of times the complete set of information advertised by MSAP has been deleted from tables associated with the remote systems because the information timeliness interval has expired.

*Click the **"Clear"** button to clear this page or click the **"Refresh"** button to refresh the page .*

Statistics Table

Field	Description
Port	Interface or port number.
Transmit Frame Total	Number of LLDP frames transmitted on the corresponding port.
Receive Frame	● **Total:** Number of LLDP frames received by this LLDP agent on the corresponding port, while the LLDP agent is enabled ● **Discarded:** Number of LLDP frames discarded for any reason by the LLDP agent on the corresponding port. ● **Errors:** Number of invalid LLDP frames received by the LLDP agent on the corresponding port, while the LLDP agent is enabled.
Receive TLV	● **Discarded:** Number of TLVs of LLDP frames discarded for any reason by the LLDP agent on the corresponding port. ● **Unrecognized:** Number of TLVs of LLDP frames that are unrecognied while the LLDP agent is enabled ● **Neighbor Timeout:** Number of TLVs of LLDP frames that are unrecognied while the LLDP agent is enabled
Neighbor Timeout	Number of age out LLDP frames.

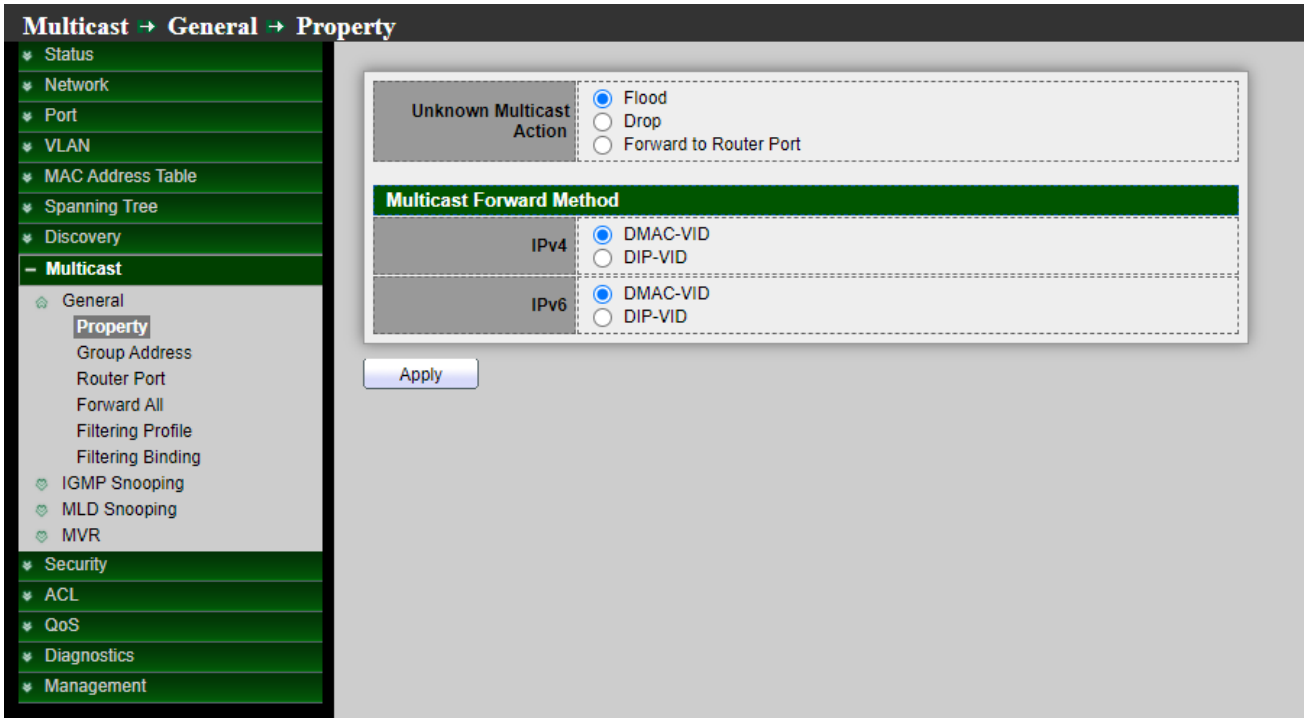
9. Multicast

Multicast is the only type of IPv4 multicast that is supported by the Ethernet gateway.

9.1 General

9.1.1 Property

This page can be configured with unknown multicast action, administrator can set the forwarding method is based on the DMAC or the DIP, the function implements high performance data transfer from point to multipoint in network will be reduce the loading on the network.

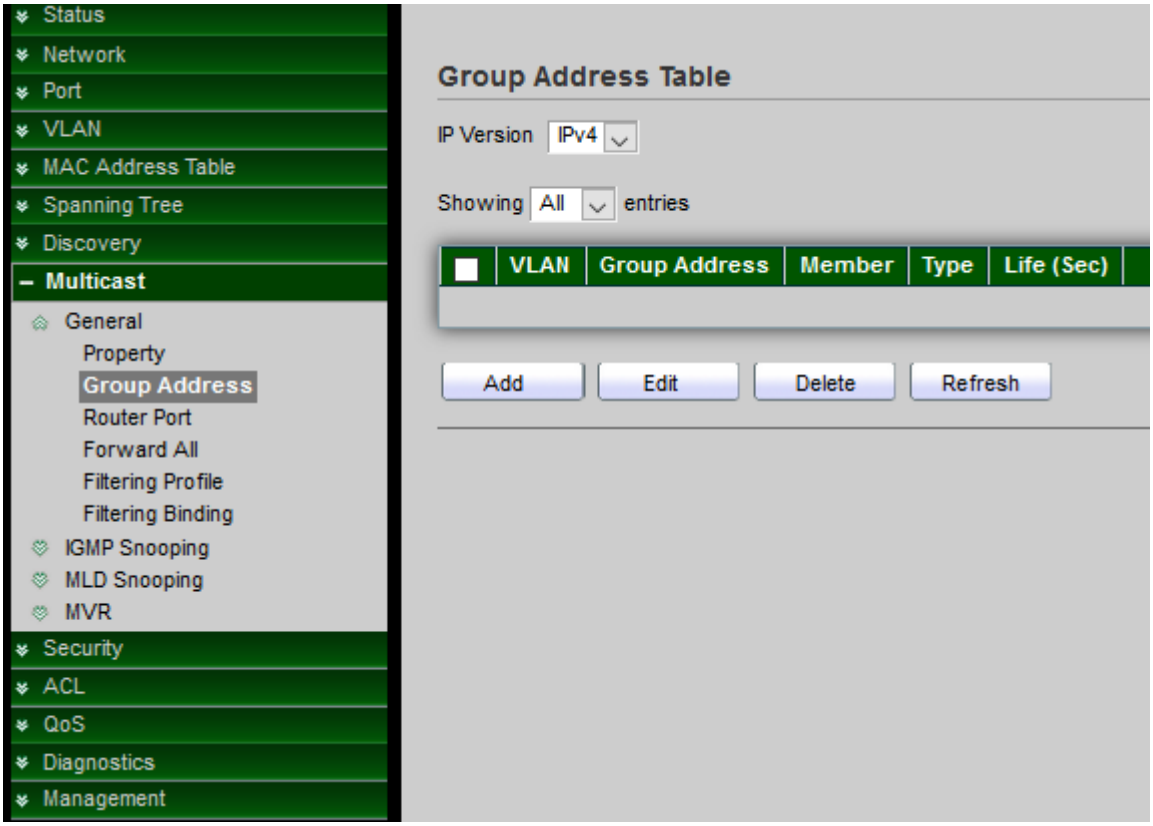


- **Unknown Multicast Action :** Set the unknown multicast action
  - **Drop:** drop the unknown multicast data.
  - **Flood:** flood the unknown multicast data.
  - **Router port:** forward the unknown multicast data to router port.
- **Multicast Forward Method :** Assign the subnet mask of IP address.
- **IPV4 :** Set the ipv4 multicast forward method.
  - **MAC-VID :** forward method dmac+vid.
  - **DIP-VID :** forward method dip+vid.
- **IPV6 :** Set the ipv6 multicast forward method.
  - **MAC-VID :** forward method dmac+vid.
  - **DIP-VID :** forward method dip+vid(dip is ipv6 low 32 bit).

*Click the **"Apply"** button to save your changes settings.*

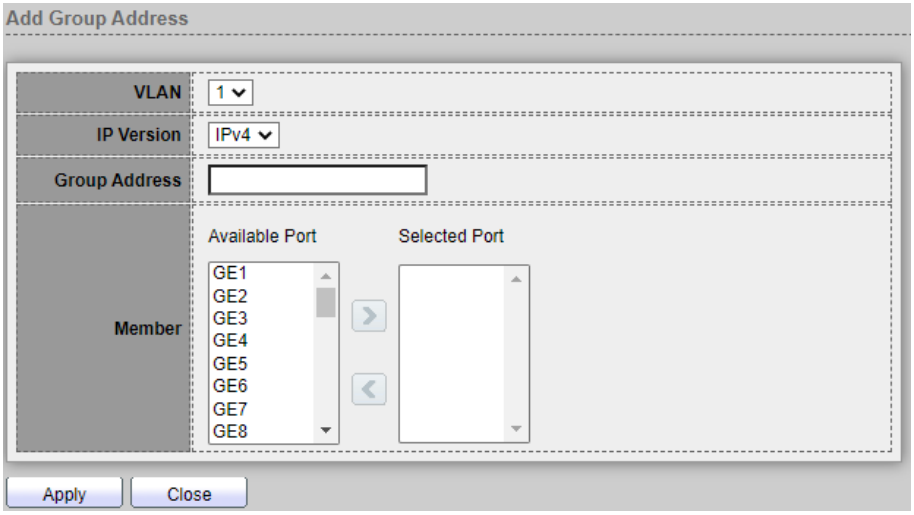
9.1.2 Group Address

The multicast address range is 224.0.0.0 to 239.255.255.255 and forms the Class D range which is made up of the high order bits 1110 followed by the 28 bit multicast group ID. There is no subletting with these Class D addresses. A multicast group can have a permanently-assigned address or the group may be Transient, , Setting **"add"** and **"Edit"** and **"Delete"** and **"Refresh"** function for this management.



- **IPV4 Version :** Select the IP Version.
  - **IPv4 :** ipv4 multicast group.
  - **IPv6 :** ipv6 multicast group.

Field	Description
VLAN	The VLAN ID of group.
Group Address	The group IP address.
Member	The member ports of group.
Type	The type of group. Static or Dynamic.
Life(Sec)	The life time of this dynamic group.

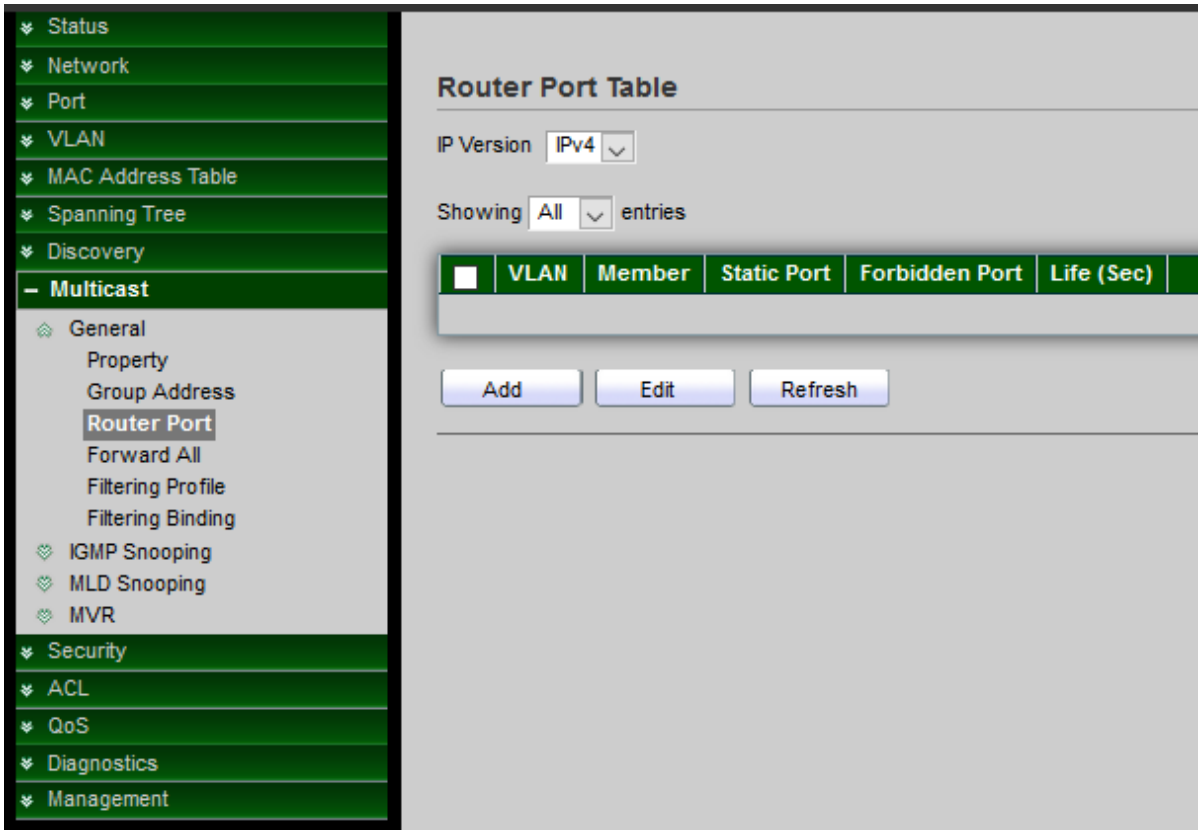


- **VLAN :** The VLAN ID of group.
- **IP Version :**
  - **IPv4 :** ipv4 multicast group.
  - **IPv6 :** ipv6 multicast group.
- **Group Address :** The group IP address.
- **Member :** The member ports of group.
  - **Available Port:** Optional port member.
  - **Selected Port**: Selected port member.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

9.1.3 Router Port

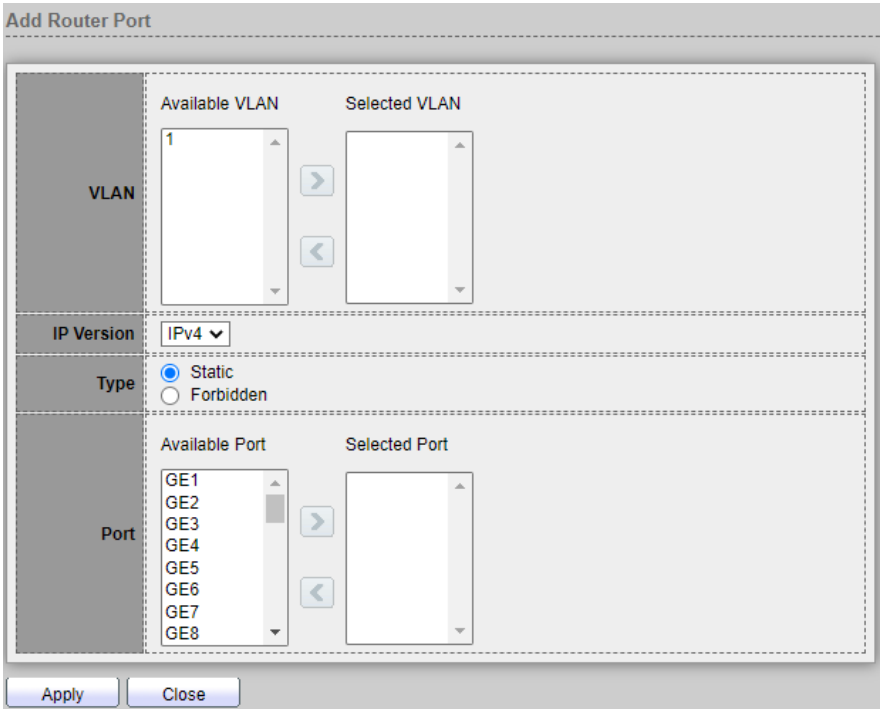
A Multicast Router (MRouter) port is a port that connects to a Multicast router. The switch includes the MRouter port(s) when it forwards Multicast streams and IGMP/ MLD registration messages. It is required in order for all Router(s) can, in turn; forward the Multicast streams and propagate the registration messages to other subnets, Setting **"add"** and **"Edit"** and **"Delete"** function for this management.



➢ **IPV4 Version :** Select the IP Version.

- **IPv4 :** ipv4 multicast router.
- **IPv6 :** ipv6 multicast router.

Field	Description
VLAN	The VLAN ID router entry.
Member	Router Port member (include static and learned port member).
Static Port	Static router port member.
Forbidden Port	Forbidden router port member.
Life(Sec)	The expiry time of the router entry.



- **VLAN :** The VLAN ID of group.
  - **Available VLAN:** Optional VLAN member.
  - **Selected VLAN**: Selected VLAN member.
- **IP Version :**
  - **IPv4 :** IPv4 multicast router.
  - **IPv6 :** IPv6 multicast router.

Type : The router port type:

- **Static :** Static router port.
- **Forbidden :** forbidden router port, can't learn dynamic router port member.

- **Port :** The member ports of Router entry.
  - **Available Port:** Optional router port member.
  - **Selected Port**: Selected router port member.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

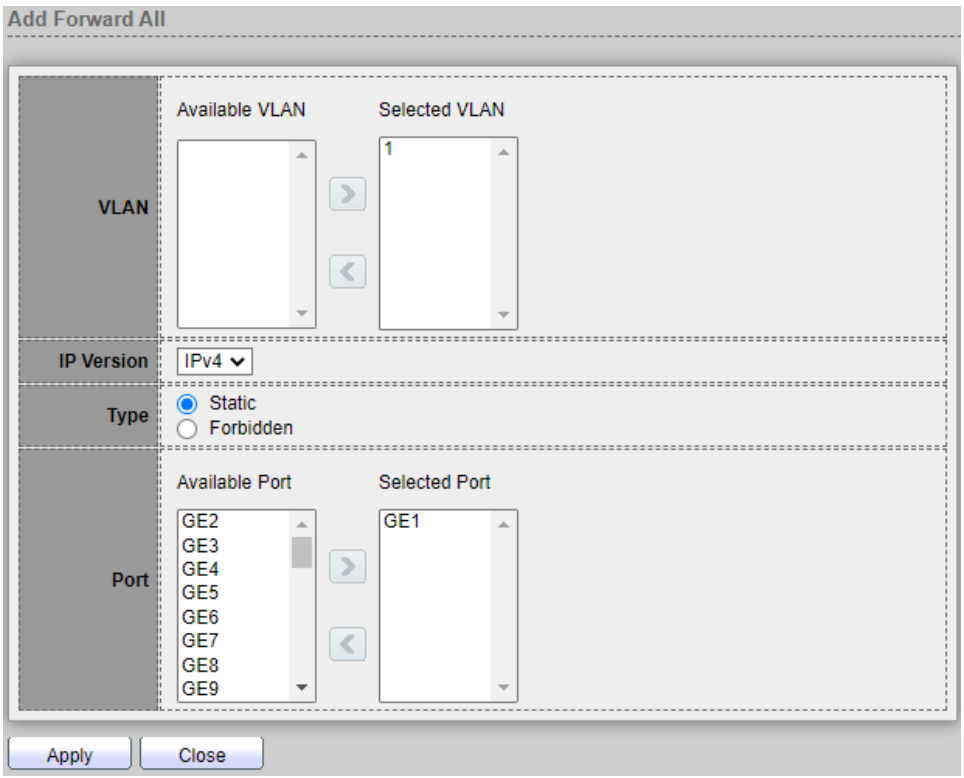
9.1.4 Forward All

Configure ports or LAGs to receive Multicast streams from a specific VLAN. Administrator can statically configure a port to Forward All if the devices connecting to the port do not support IGMP or MLD, Setting **"add"** and **"Edit"** and **"Delete"** function for this management.

Note	The configuration affects only the ports that are members of the selected VLAN.

- **IPV4 Version :** Select the IP Version.
  - **IPv4 :** IPv4 multicast forward all.
  - **IPv6 :** IPv6 multicast forward all.

Field	Description
VLAN	VLAN ID of forward all entry
Static Port	Known multicast group always forward port member
Forbidden Port	Known multicast group always not forward port member

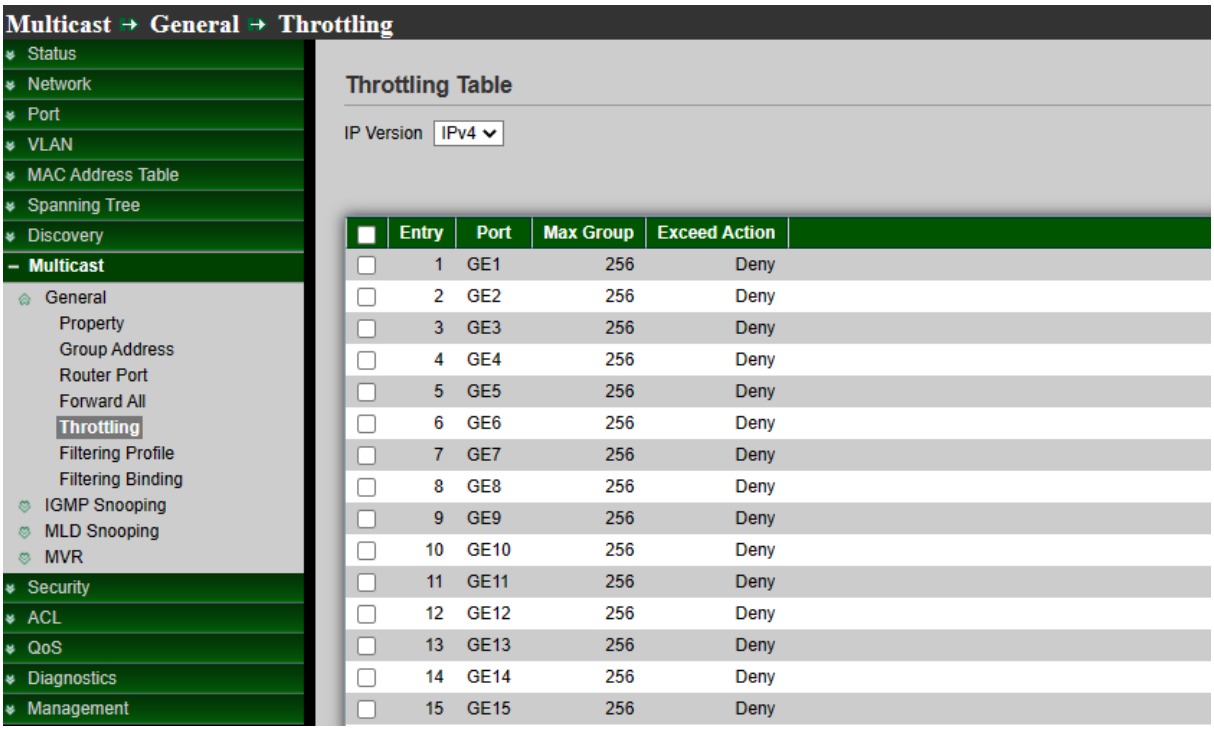


- **VLAN :** The VLAN ID of forward all entry.
  - **Available VLAN:** Optional VLAN member.
  - **Selected VLAN**: Selected VLAN member.
- **IP Version :**
  - **IPv4 :** IPv4 multicast forward all.
  - **IPv6 :** IPv6 multicast forward all.
- **Type :** The forward all port type
  - **Static :** Static forward all port. The port is statically configured as a Multicast router port.
  - **Forbidden :** Forbidden forward all port. This port is not to be configured as a Multicast Router port, even if IGMP or MLD queries are received on this port.
- **Port :** The member ports of forward all.
  - **Available Port:** Optional router port member.
  - **Selected Port**: Selected router port member.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

9.1.5 Throttling

This page allow user to configure port can learned max group number and if port group number arrived max group number action.

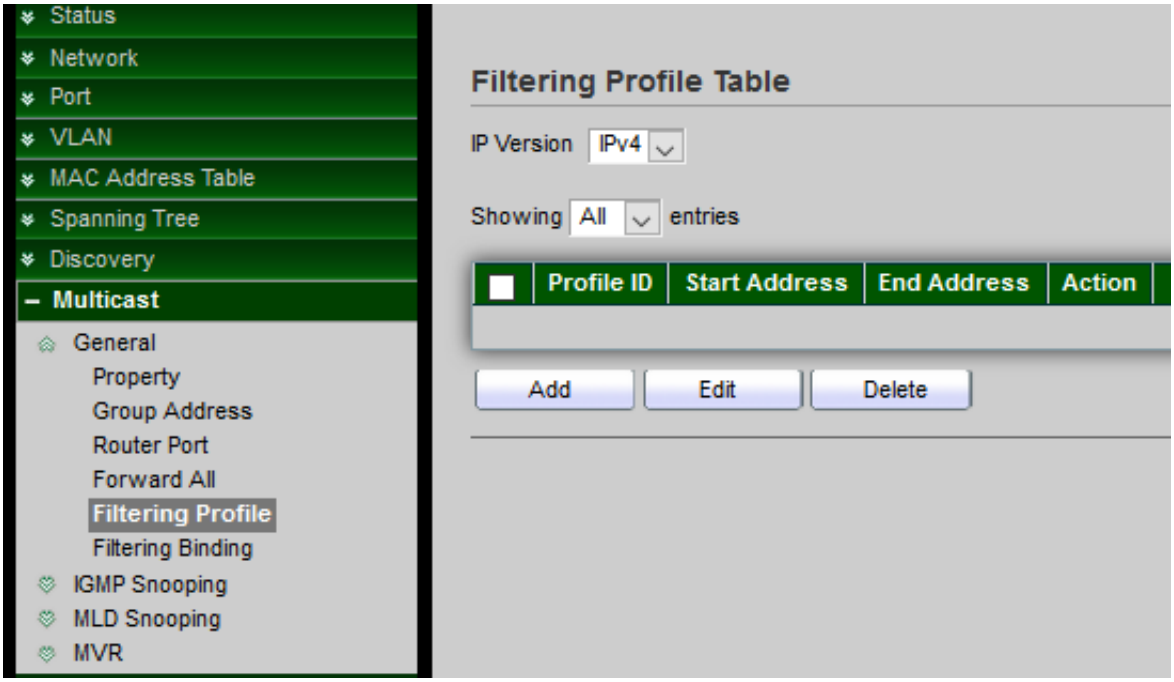


- **IPV4 Version :** Select the IP Version.
  - **IPv4 :** IPv4 for IGMP snooping throttling.
  - **IPv6 :** IPv6 for MLD snooping throttling.

Field	Description
Port	Display the Port Name
Max Group	Display the Max number of group for port
Exceed Action	Display the port exceed max number group learning group action

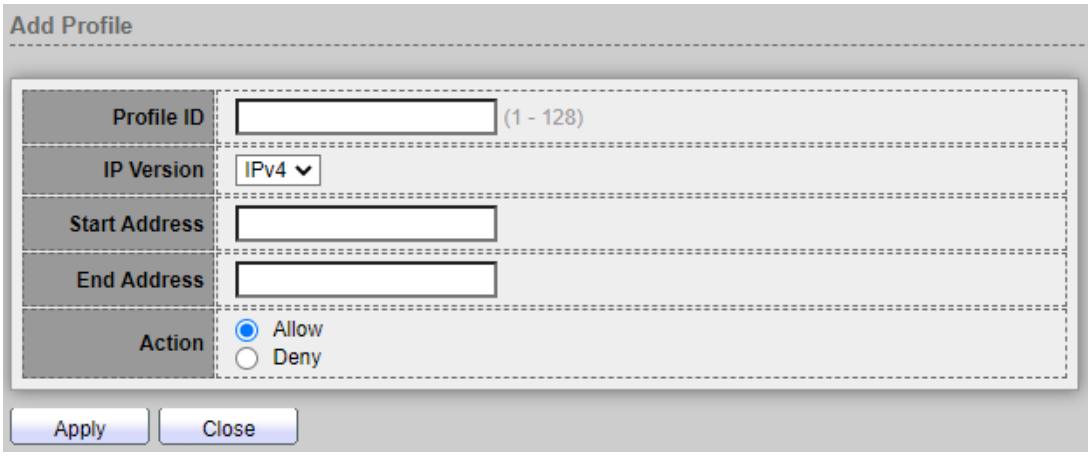
9.1.6 Filtering Profile

Filter profile permits or denies a range of Multicast groups to be learned when the join group matches the filter profile IP group range, Setting **“add”** and **“Edit”** and **“Delete”** function for this management.



- **IPV4 Version :** Select the IP Version.
  - **IPv4 :** IPv4 for IGMP snooping profile.
  - **IPv6 :** IPv6 for MLD snooping profile.

Field	Description
Profile ID	Display profile ID
Start Address	The start group address of profile
End Address	The end group address of profile
Action	Display profile action

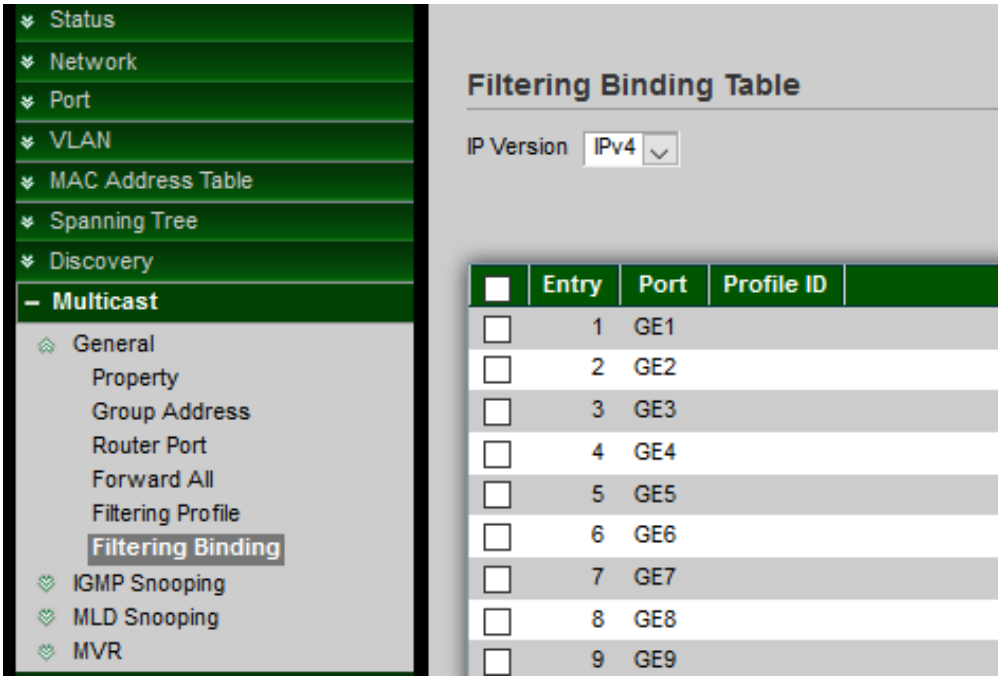


- **Profile ID: Profile ID**.
- **IP Version :** Display the selected IP version
  - **IPv4:** IGMP snooping profile.
  - **IPv6:** MLD snooping profile.
- **Start Address:** The start group address of profile.
- **End Address :** The end group address of profile.
- **Action:** The action of profile:
  - **Allow:** permit all packets that match the profile.
  - **Deny:** deny all packets that match the profile.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

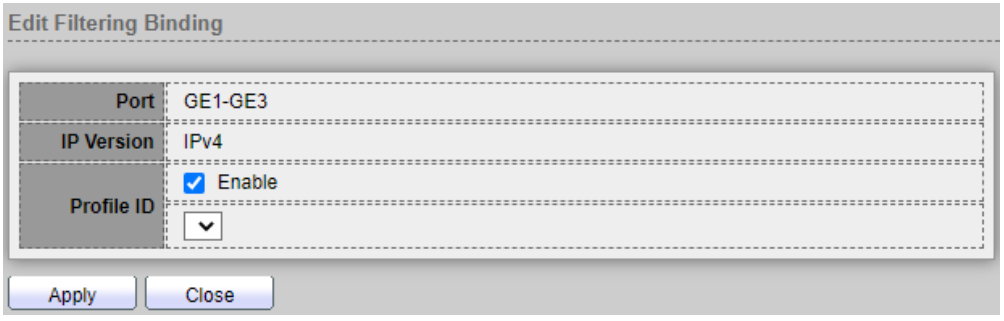
9.1.7 Filtering Binding

When the setting is completed of Filtering Profile, administrator can select ports to set filtering binding.



- **IPV4 Version :** Select the IP Version.
  - **IPv4 :** IPv4 for IGMP snooping throttling.
  - **IPv6 :** IPv6 for MLD snooping throttling.

Field	Description
Entry	Entry of number
Port	Port Name
Profile ID	Port binding Profile ID



- **Port:** Selected Port List.
- **IP Version :** Display Selected Port filtering IP version.
- **Profile ID:** If check Enable, can select or change profile ID, Else it will delete port filter profile *binding.*

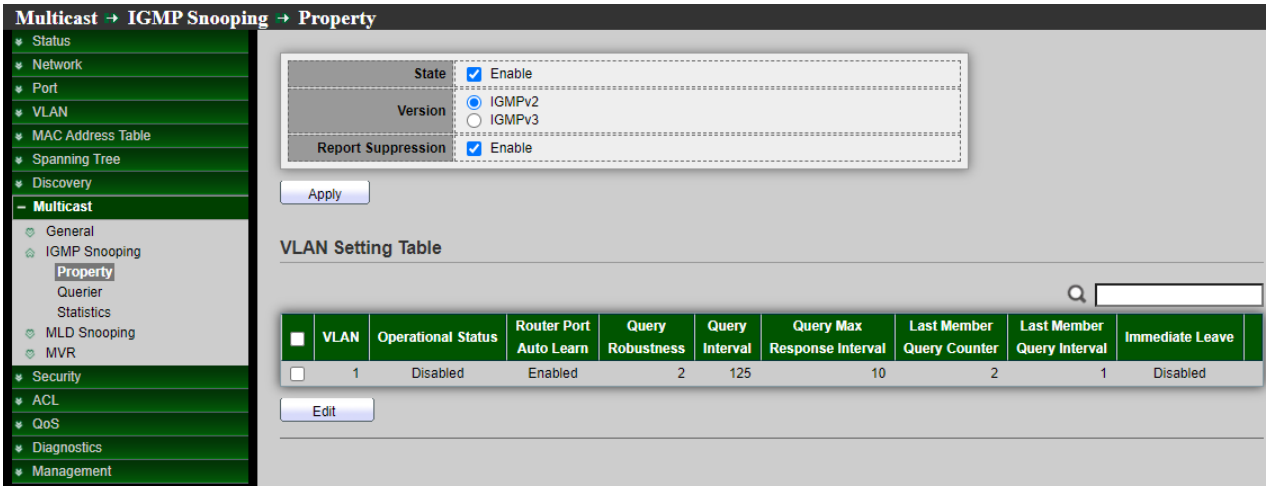
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

9.2 IGMP Snooping

IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic. The IGMP snooping support v2 & v3, administrator can forward or drop Unknown Multicast.

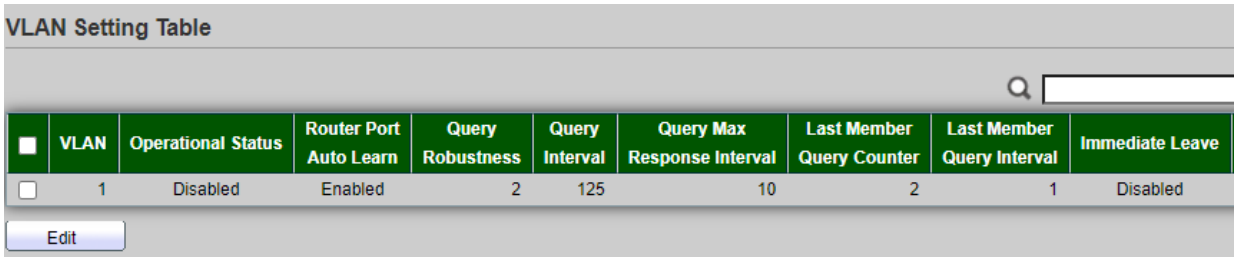
9.2.1 Property

When IGMP Snooping is enabled globally or on a VLAN, all IGMP packets are forwarded to the CPU. The CPU analyzes select of ports are asking to join Multicast groups on VLAN or routers that are generating IGMP queries, or receiving PIM / OSFP / DVMRP / IGMP query protocols incoming packets.

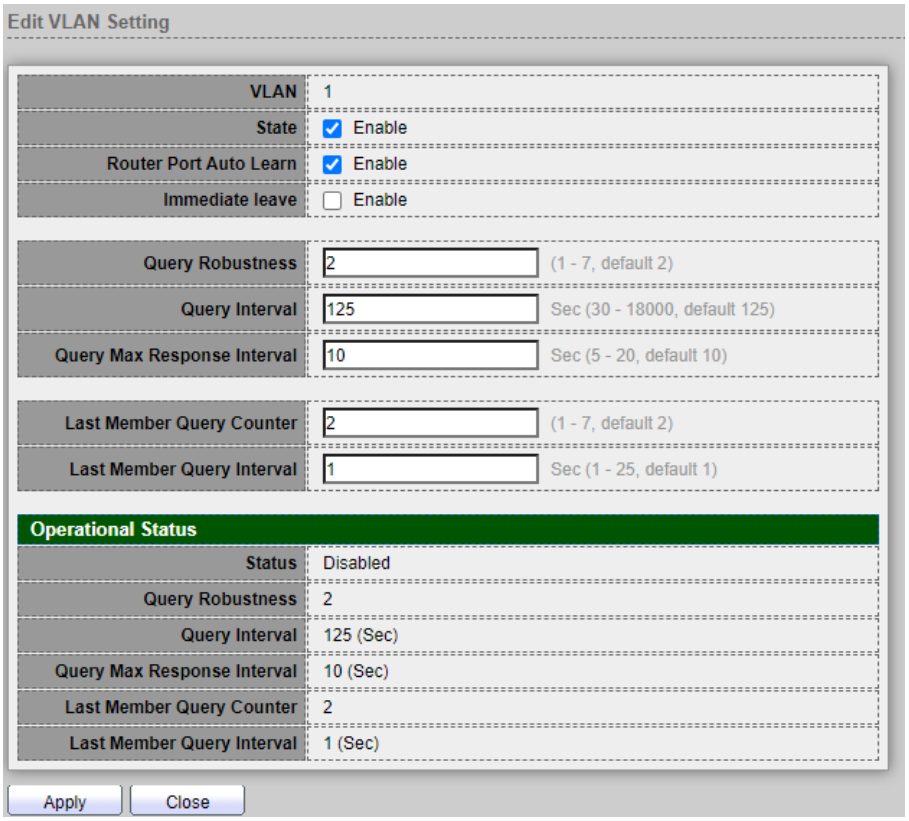


- **State:** Administrator can select Enable or Un-enable, Set the enabling status of IGMP Snooping functionality.
  - **Enable:** If Checked Enable IGMP Snooping, else is Disabled IGMP Snooping.
- **Version:** Select either IGMPv2 or IGMPv3,Set the igmp snooping version.
  - **IGMPv2:** Only support process igmp v2 packet.
  - **IGMPv3:** Support v3 basic and v2.
- **Report Suppression:** Enable or disable IGMP report suppression. If administrator select disabling this feature will forward all IGMP reports to Multicast routers, Set the enabling status of IGMP v2 report suppression.
  - **Enable:** If Checked Enable IGMP Snooping v2 report suppression, else Disable the report suppression function.

*Click the **"Apply"** button to save your changes.*



Field	Description
VLAN	The IGMP entry VLAN ID
Operation Status	The enable status of IGMP snooping VLAN functionality
Router Port Auto Learn	The enabling status of IGMP snooping router port auto learning
Query Robustness	The Query Robustness allows tuning for the expected packet loss on a subnet.
Query Interval	The interval of querier to send general query
Query Max Response Interval	In Membership Query Messages, it specifies the maximum allowed time before sending a responding report in units of 1/10 second.
Last Member Query count	The count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Last Member Query Interval	The interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Immediate leave	The immediate leave status of the group will immediate leave when receive IGMP Leave message.



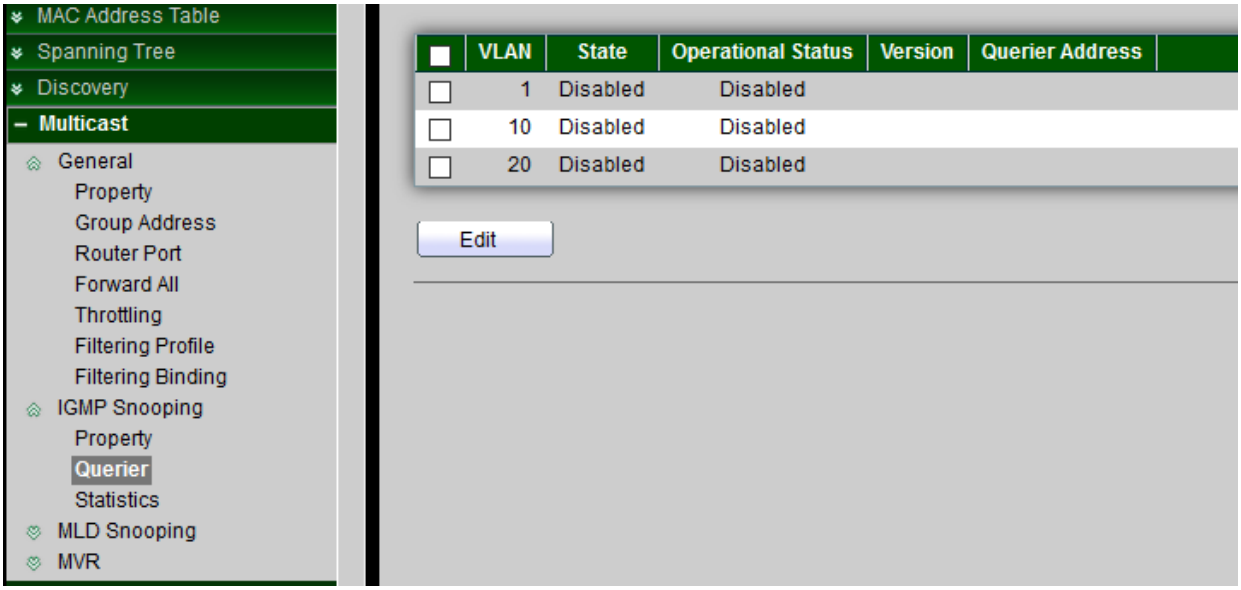
- **VLAN:** The VLAN ID of IGMP Snooping.
- **State:** Set the enabling status of IGMP Snooping VLAN functionality.
  - **Enable: Enable:** If Checked Enable IGMP Snooping VLAN, else is Disabled IGMP Snooping VLAN.
- **Router Port Auto Learn:** Set the enabling status of IGMP Snooping router port learning.
  - **Enable:** If checked Enable learning router port by query and PIM, DVRMP, else Disable the learning router port.
- **Immediate leave:** Immediate Leave the group when receive IGMP Leave message.
  - **Enable:** If checked Enable immediate leave, else disable immediate leave.
- **Query Robustness:** The Admin Query Robustness allows tuning for the expected packet loss on a subnet.
- **Query Interval:** The Admin interval of querier to send general query.
- **Query Max Response Interval:** The Admin query max response interval， In Membership Query Messages, it specifies the maximum allowed time before sending a responding report in units of 1/10 second.
- **Last Member Query Counter:** The Admin last member query count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
- **Last Member Query Interval:** The Admin last member query interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.

- **Operational Status:** Set the enabling status of IGMP Snooping router port learning.
  - **Status:** Operational IGMP snooping status， must both IGMP snooping global and IGMP snooping enable the status will be enable.
  - **Query Robustness:** Operational Query Robustness.
  - **Query Interval:** Operational Query Interval.
  - **Query Max Response Interval:** Operational Query Max Response Interval.
  - **Last Member Query Counter:** Operational Last Member Query Count.
  - **Last Member Query Interval:** Operational Last Member Query Interval.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

9.2.2 Querier

Administrator can choose created VLAN to enable or disable the IGMP Snooping query function. When select checkbox and click "**Edit**" button will be go to set IGMP Snooping version, this function can get IGMP Snooping query device regularly to VLAN local segments in all hosts and routers send IGMP Snooping general query packets, to the query segment which multicast group members.



Field	Description
VLAN	IGMP Snooping querier entry VLAN ID
State	The IGMP Snooping querier Admin State.
Operational Status	The IGMP Snooping querier operational status

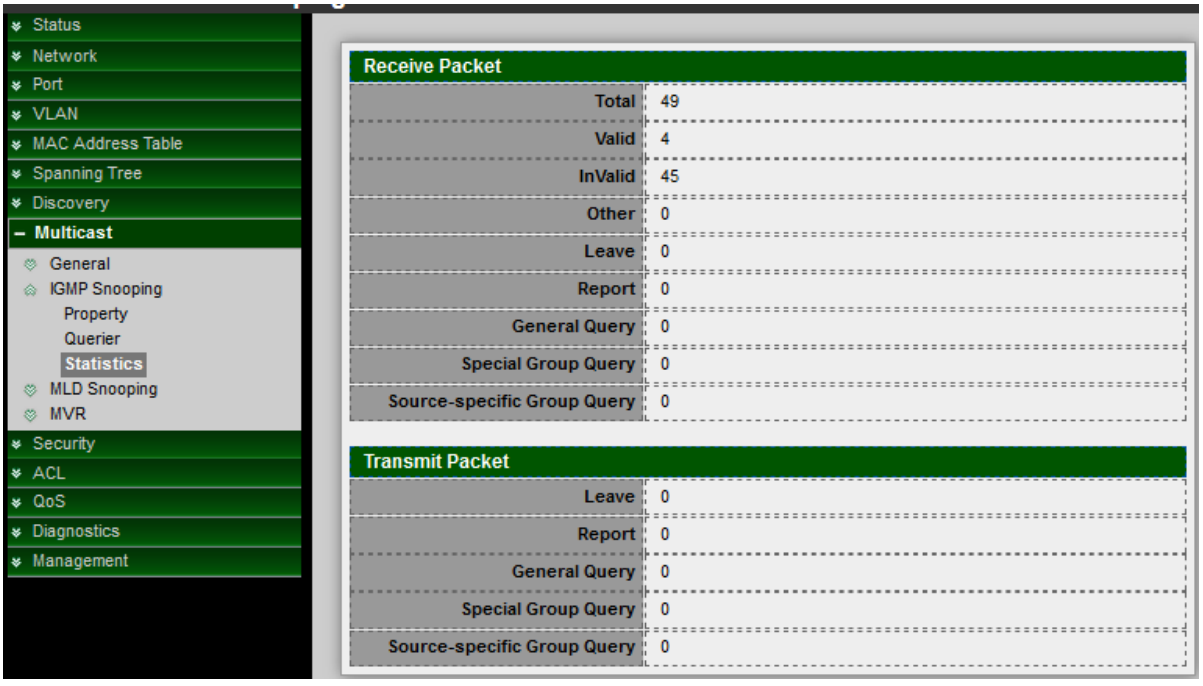
Querier Version	The IGMP Snooping querier operational version.
Querier IP	The operational Querier IP address on the VLAN

- **VLAN:** The Selected Edit IGMP Snooping querier VLAN List.
- **State :** Set the enabling status of IGMP Querier Election on the chose VLANs.
  - **Enabled:** if checked Enable IGMP Querier else Disable IGMP Querier.
- **Version :** Set the query version of IGMP Querier Election on the chose VLANs.
  - **IGMPv2:** Querier version 2.
  - **IGMPv3:** Querier version 3. (IGMP Snooping version should be IGMPv3).

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

9.2.3 Statistics

Display Receive / Transmit Packet information of IGMP snooping.



Field	Description
Receive Packet	● **Total:** Total RX igmp packet, include ipv4 multicast data to CPU. ● **Valid:** The valid igmp snooping process packet. ● **InValid:** The invalid igmp snooping process packet. ● **Other:** The ICMP protocol is not 2, and is not ipv4 multicast data packet. ● **Leave:** IGMP leave packet. ● **Report:** IGMP join and report packet. ● **General Query:** IGMP General Query packet. ● **Special Group Query:** IGMP Special Group General Query packet. ● **Source-specific Group Query:** IGMP Special Source and Group General Query packet.
Transmit Packet	● **Leave:** IGMP leave packet. ● **Report:** IGMP join and report packet. ● **General Query:** IGMP general query packet include querier transmit general query packet ● **Special Group Query:** IGMP special group query packet include querier transmit special group query packet. ● **Source-specific Group Query:** IGMP Special Source and Group General Query packet.

*Click the **"Clear"** button to clear this page or click the **"Refresh"** button to refresh the page .*

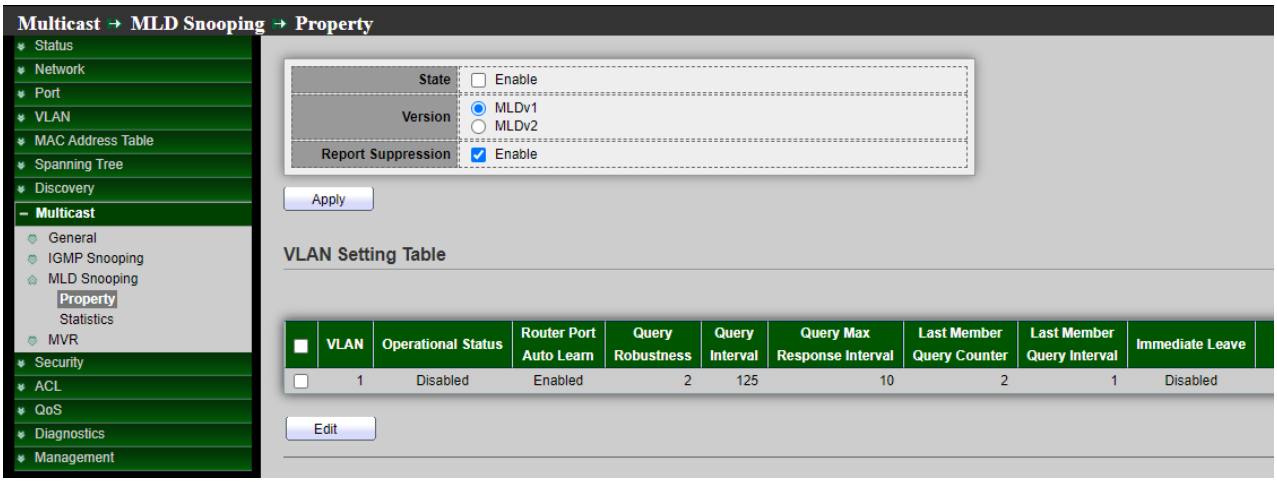
9.3 MLD Snooping

The function support selective Multicast forwarding (IPv6), MLD Snooping must be enabled globally and for each relevant VLAN. The switch supports MLD Snooping on both static and dynamic VLANs. Hosts use the MLD protocol to report their participation in Multicast sessions, and the switch uses MLD Snooping to build Multicast membership lists. It uses these lists to forward Multicast packets only to switch ports where there are host nodes that are members of the Multicast groups. The switch does not support MLD Querier.

9.3.1 Property

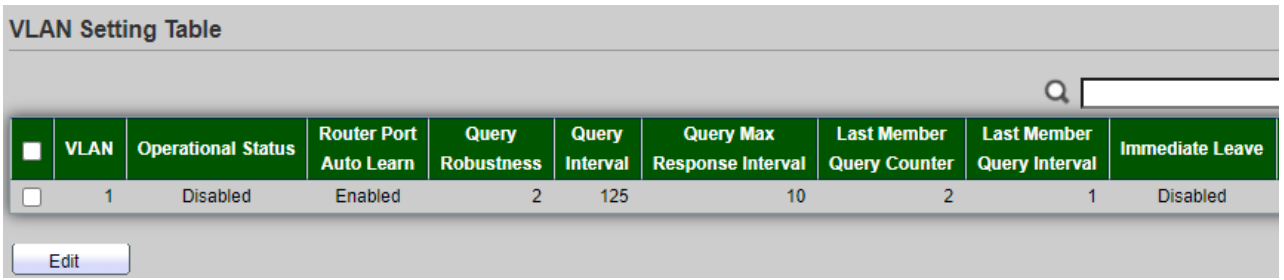
Administrator to enable MLD Snooping in addition to the manually configured Multicast groups, the result is a union of the Multicast groups and port memberships derived from the manual

setup and the dynamic discovery by MLD Snooping. However, only the static definitions are preserved when the switch is rebooted.



- **State:** Administrator can select Enable or Un-enable, Set the enabling status of IGMP Snooping functionality.
  - **Enable:** If Checked Enable IGMP Snooping, else is Disabled IGMP Snooping.
- **Version:** Select either MLDv1 or MLDv2, Set the MLD snooping version.
  - **MLDv1:** Only support process MLD v1 packet.
  - **MLDv2:** Support v2 basic and v1.
- **Report Suppression:** Set the enabling status of MLD v1 report suppression.
  - **Enable:** If Checked Enable MLD Snooping v1 report suppression, else Disable the report suppression function.

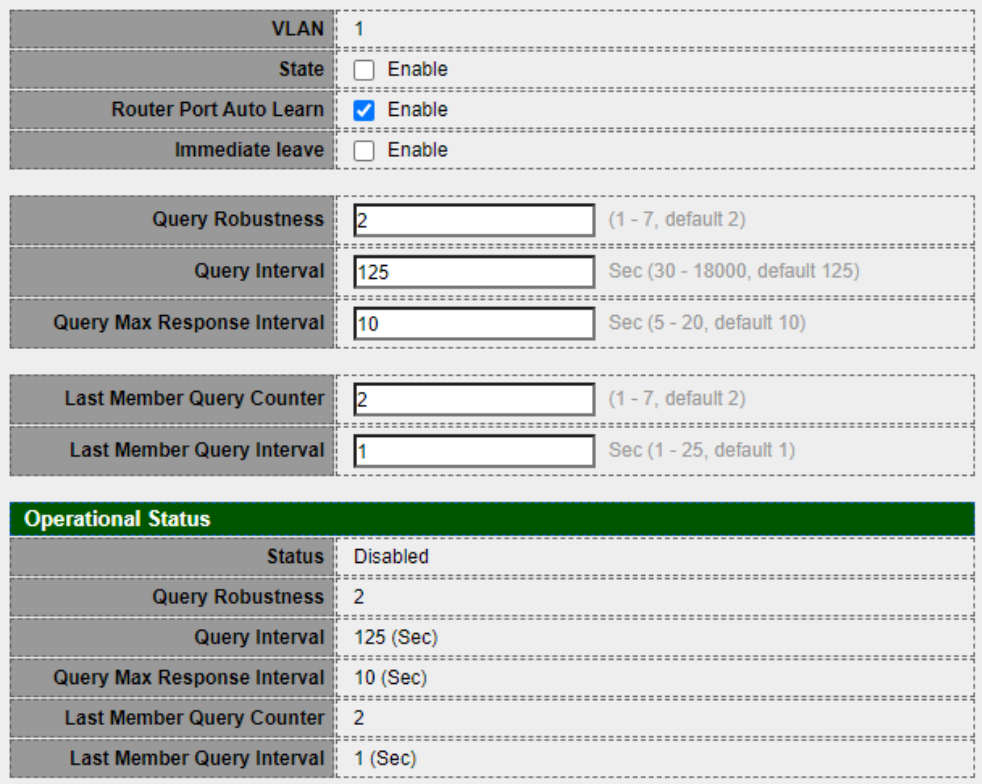
*Click the **"Apply"** button to save your changes.*



Field	Description
VLAN	The MLD entry VLAN ID
Operation Status	The enable status of MLD snooping VLAN functionality

Router Port Auto Learn	The enabling status of MLD snooping router port auto learning
Query Robustness	The Query Robustness allows tuning for the expected packet loss on a subnet.
Query Interval	The interval of querier to send general query
Query Max Response Interval	In Membership Query Messages, it specifies the maximum allowed time before sending a responding report in units of 1/10 second.
Query Max Response Interval	The count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Last Member Query Interval	The interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Immediate leave	The immediate leave status of the group will immediate leave when receive MLD Leave message.

Administrator can select VLAN in checkbox and click Edit button to set MLD Snooping.

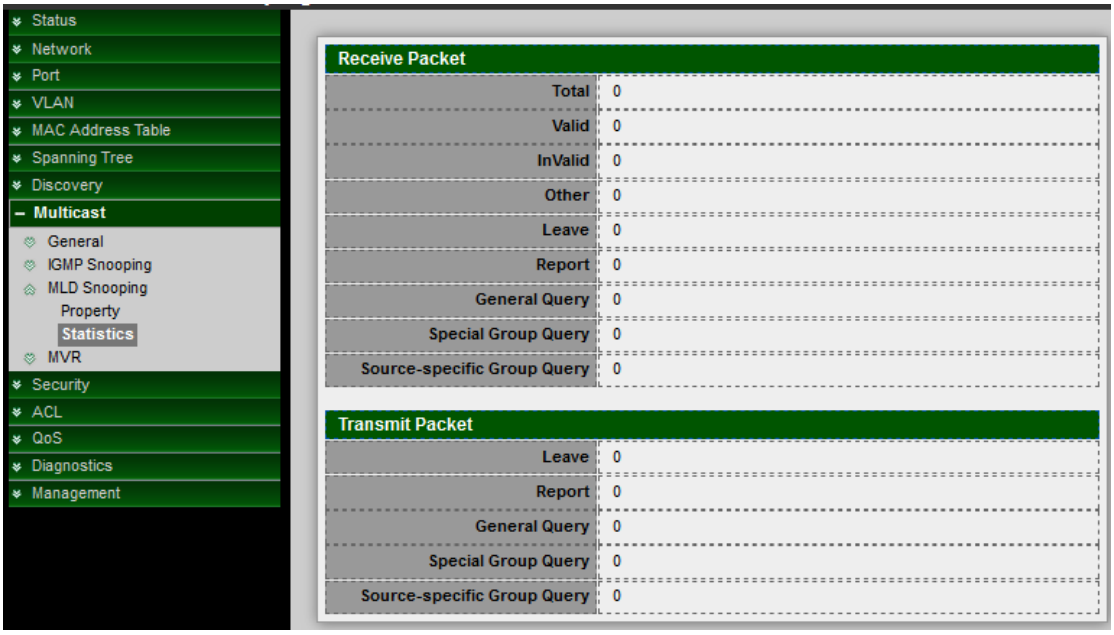


- **VLAN:** The VLAN ID of MLD Snooping.
- **State:** Set the enabling status of MLD Snooping VLAN functionality.
  - **Enable: Enable:** If Checked Enable MLD Snooping VLAN, else is Disabled MLD Snooping VLAN.

- **Router Port Auto Learn:** Set the enabling status of MLD Snooping router port learning.
  - **Enable:** If checked Enable learning router port by query and PIM, DVRMP, else Disable the learning router port.
- **Immediate leave:** Immediate Leave the group when receive MLD Leave message.
  - **Enable:** If checked Enable immediate leave, else disable immediate leave.
- **Query Robustness:** The Admin Query Robustness allows tuning for the expected packet loss on a subnet.
- **Query Interval:** The Admin interval of querier to send general query.
- **Query Max Response Interval:** The Admin query max response interval， In Membership Query Messages, it specifies the maximum allowed time before sending a responding report in units of 1/10 second.
- **Last Member Query Counter:** The Admin last member query count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
- **Last Member Query Interval:** The Admin last member query interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
- **Operational Status:** Set the enabling status of MLD Snooping router port learning.
  - **Status:** Operational MLD snooping status,must both MLD snooping global and MLD snooping enable the status will be enable.
  - **Query Robustness:** Operational Query Robustness.
  - **Query Interval:** Operational Query Interval.
  - **Query Max Response Interval:** Operational Query Max Response Interval.
  - **Last Member Query Counter:** Operational Last Member Query Count.
  - **Last Member Query Interval:** Operational Last Member Query Interval.

9.3.2 Statistics

If administrator to enable MLD snooping, the page will display Receive / Transmit Packet information of MLD Snooping.



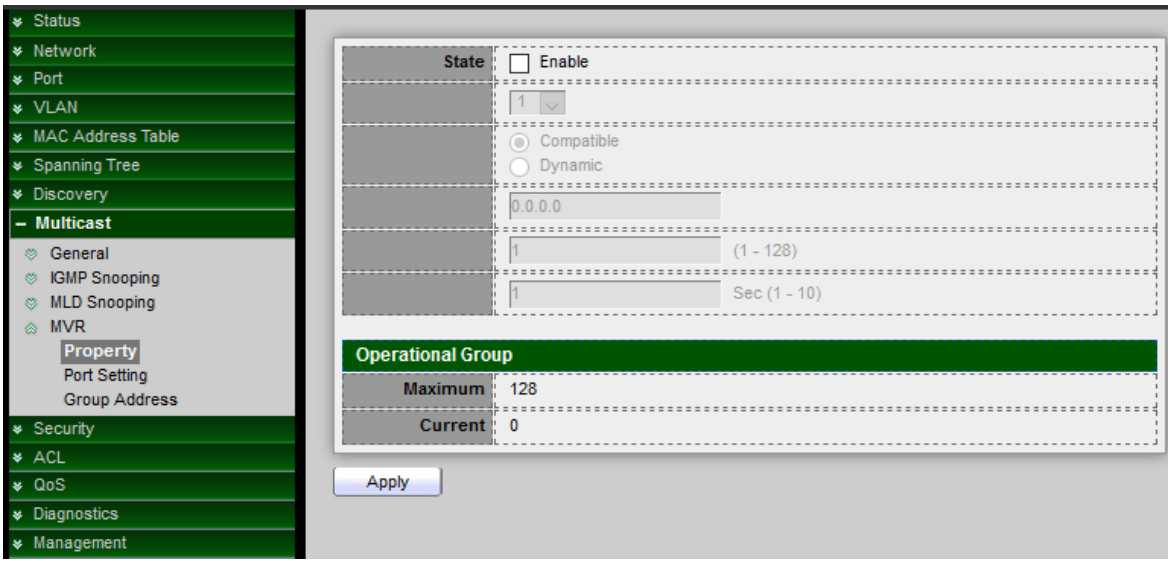
Field	Description
Receive Packet	● **Total:** Total RX MLD packet, include ipv4 multicast data to CPU. ● **Valid:** The valid MLD snooping process packet. ● **InValid:** The invalid MLD snooping process packet. ● **Other:** The ICMPV6 type is not MLD, and is not ipv6 multicast data packet and is not IPV6 router protocol. ● **Leave:** MLD leave packet. ● **Report:** MLD join and report packet. ● **General Query:** MLD General Query packet. ● **Special Group Query:** MLD Special Group General Query packet. ● **Source-specific Group Query:** MLD Special Source and Group General Query packet.
Transmit Packet	● **Leave:** MLD leave packet. ● **Report:** MLD join and report packet. ● **General Query:** MLD general query packet. ● **Special Group Query:** MLD special group query packet. ● **Source-specific Group Query:** MLD Special Source and Group General Query packet.

*Click the **"Clear"** button to clear this page or click the **"Refresh"** button to refresh the page .*

9.4 MVR

MVR (Multicast VLAN Registration) is designed for applications that use wide-scale deployment of multicast traffic across an Ethernet ring-based service-provider network (for example, the broadcast of multiple television channels over a service-provider network). MVR allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on the network-wide multicast VLAN.
It allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs. MVR provides the ability to continuously send multicast streams in the multicast VLAN, but to isolate the streams from the subscriber VLANs for bandwidth and security reasons.

9.4.1 Property



- **State:** Administrator can select Enable or Un-enable, Set the enabling status of MVR functionality.
  - **Enable:** if checked enable the MVR state, else disable the MVR state.
- **VLAN:** Select the MVR VLAN ID.
- **Mode:** Set the MVR mode.
  - **Compatible:** compatible mode.
  - **Dynamic:** dynamic mode, will learn group member on source port.
- **Group Start:** Administrator can set range is 224.0.0.0 to 239.255.255.255,MVR group range start.
- **Group Count:** MVR group continue count, Uses the count parameter to configure a contiguous series of MVR group addresses (the range for count is 1 to 128; the default is 1).
- **Query Time:** MVR query time when receive MVR leave MVR group packet,Administrator can defines the maximum time to wait for IGMP report memberships on a receiver port before removing the port from multicast group membership. The value is in units of second. The range

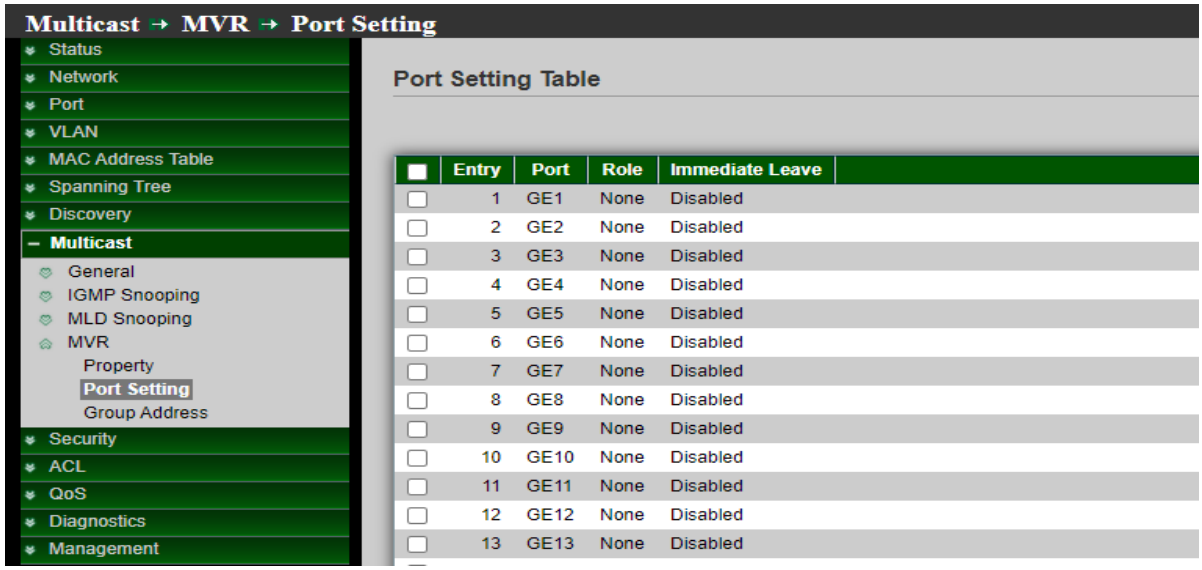
is 1 to 10, and the default is 1 second.

- **Operational Group:**
  - **Maximum:** The max number of MVR group database.
  - **Current:** The learned MVR group current time.

*Click the **"Apply"** button to save your changes settings.*

9.4.2 Port Setting

Administrator can select ports to set role and immediate of MVR.



Field	Description
Port	Port Name
Role	Port Role for MVR, the type is None/Receiver/Source
Immediate Leave	Status of immediate leave

- **Port:** Display the selected port list.
- **Role:** MVR port role.
  - **None:** port role is none.
  - **Receiver:** port role is receiver, Configures a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group, either statically or by using IGMP leave and join messages. Receiver ports cannot belong to the multicast VLAN.
  - **Source:** port role is source, Configures uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports. All source ports on a switch belong to the single multicast VLAN.

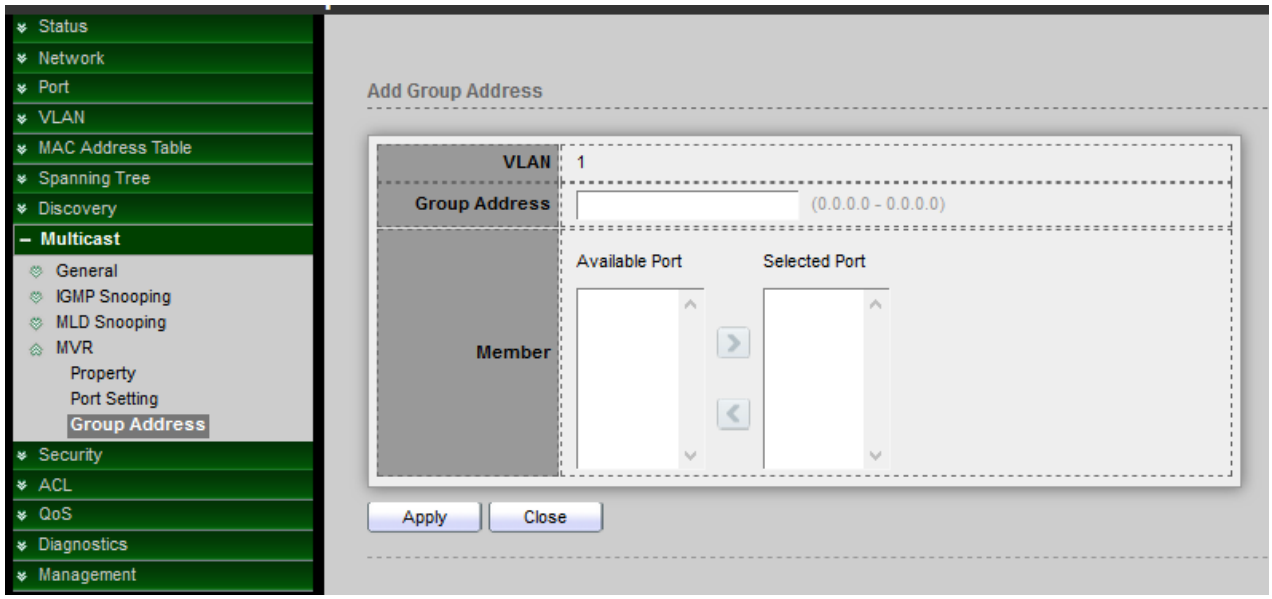
Note	If administrator to set a non-MVR port with MVR characteristics is operation fails. The default configuration is as a non-MVR port.

- **Immediate Leave:** MVR Port immediate leave
  - **Enable:** if checked is enable immediate leave, else disable immediate leave, This function only be enabled on receiver ports to which a single receiver device is connected. When Enables the Immediate Leave feature of MVR on the port. The Immediate Leave feature is disabled by default

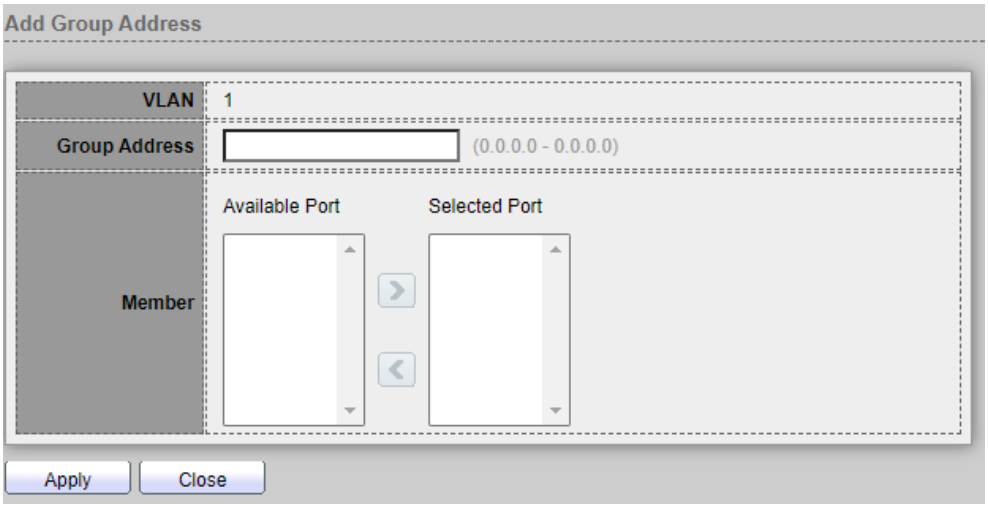
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

9.4.3 Group Address

Setting **"add"** and **"Edit"** and **"Delete"** and **"Refresh"** function for this management.



Field	Description
VLAN	The VLAN ID of MVR group.
Group Address	The MVR group IP address.
Member	The member ports of MVR group.
Type	The type of MVR group. Static or Dynamic.
Life(Sec)	The life time of this dynamic MVR group.



- **VLAN:** The VLAN ID of MVR group.
- **Group Address:** MVR group IP address ,Administrator can set MVR multicast group addresses on the switch.(The address range is 224.0.0.0 to 239.255.255.255)
- **Member:** Select Ports in the MVR Group.
  - **Available Port:** Optional port member, it is only receiver port when MVR mode is compatible, it include source port when mode is dynamic.
  - **Selected Port**: Selected port member.

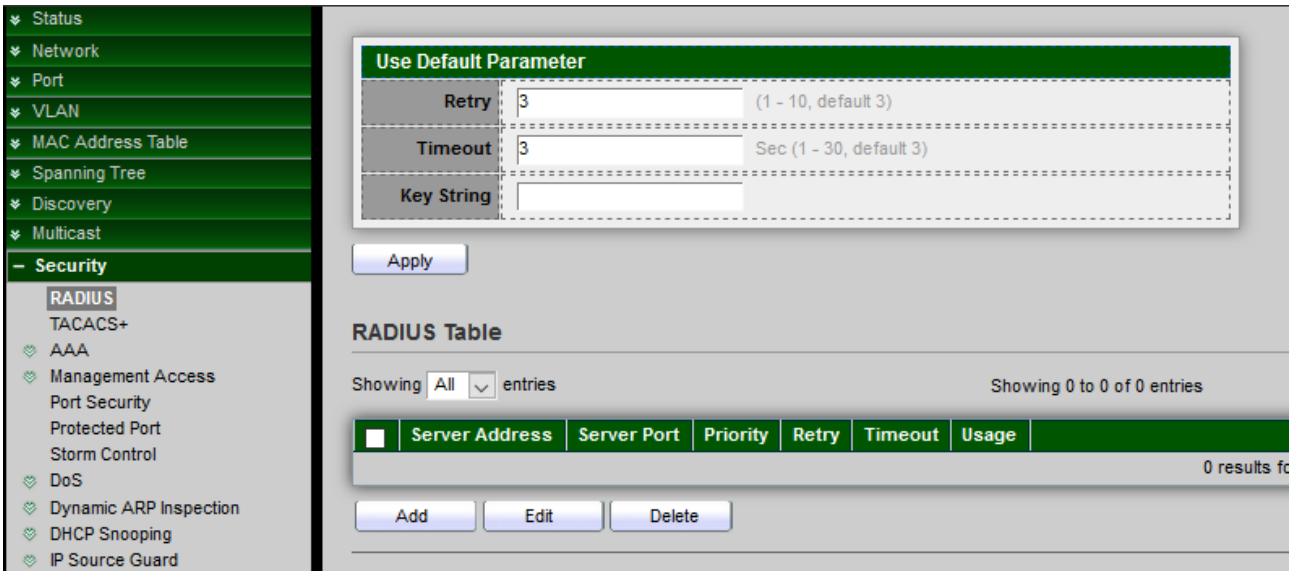
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

10. Security

10.1 RADIUS

Network architecture can establish a Remote Authorization login Service (RADIUS) server to provide a centralized 802.1X or MAC-based network access control for all of its devices. This switch can act as a RADIUS client that uses the RADIUS server to provide centralized security and authorization and user authentication.

Administrator can set account for the switch on the RADIUS server, and configure that RADIUS server along with the other parameters on the RADIUS page.

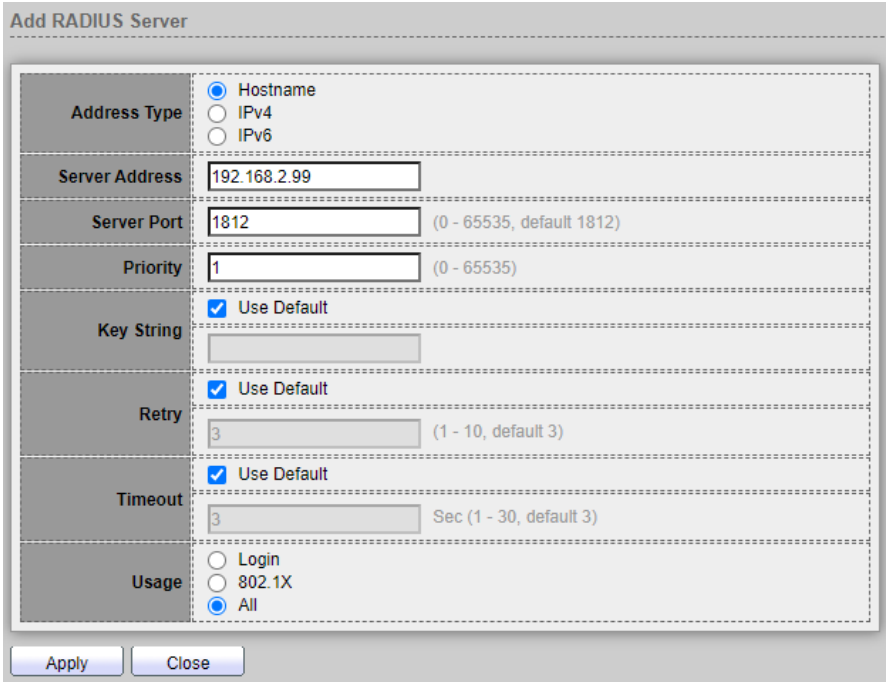


➢ **Use Default Parameters :**

- **Retry:** Set default retry number ,Enter the number of transmitted requests that are sent to the RADIUS server before a failure is considered to have occurred. Default is 3.
- **Timeout:** Set default timeout value ,Enter the number of seconds that the switch waits for an answer from the RADIUS server before retrying the query, or switching to the next server. Default is 3.
- **Key String:** Set default RADIUS key string ,The key string used security communications between the switch and the RADIUS server by MD5.This key must match the key configured on the RADIUS server. If don't have an encrypted key string (from other device), please enter the key string in plaintext form.

*Click the "**Apply**" button to save your changes settings.*

Field	Description
Server Address	RADIUS server address.
Server Port	RADIUS server port.
Priority	RADIUS server priority (smaller value has higher priority). RADIUS session will try to establish with the server setting which has highest priority. If failed, it will try to connect to the server with next higher priority.
Retry	RADIUS server retry value. If it is fail to connect to server, it will keep trying until timeout with retry times.
Timeout	RADIUS server timeout value. If it is fail to connect to server, it will keep trying until timeout.
Usage	RADIUS server usage type • **Login:** For login authentication. • **802.1x:** For 802.1x authentication. • **All:** For alltypes.



- **Address Type:** Select IP Version 4 / 6 or use Hostname typem, In add dialog, user need to specify server Address Type
  - **Hostname:** Use domain name as server address.
  - **IPv4:** Use IPv4 as server address.

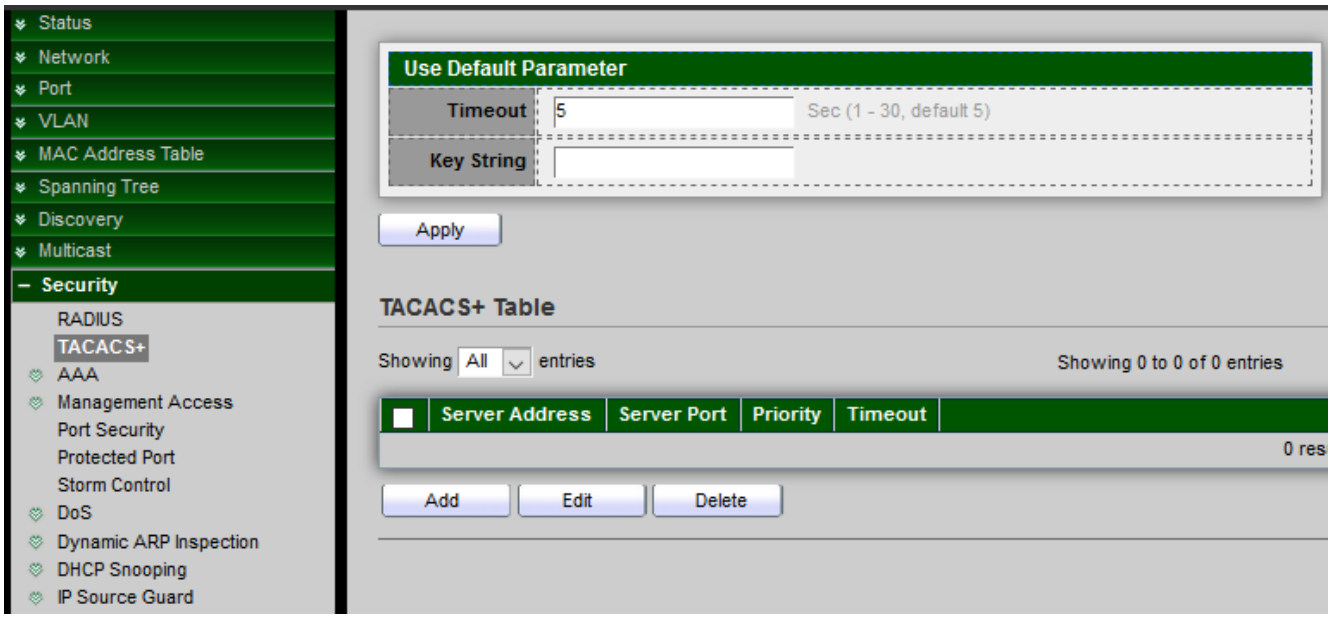
- **IPv6:** Use IPv6 as server address.

- **Server Address:** Please enter the IP address or hostname of the RADIUS server. In add dialog, user need to input server address based on address type. In edit dialog, it shows current edit server address.
- **Server Port:** Set port of RADIUS server.
- **Priority:** Administrator can enter the priority of the server. The priority determines the order that the switch attempts to contact the servers to authenticate users. The switch first starts with the highest priority server. 0 is the high priority, Set RADIUS server priority (smaller value has higher priority). RADIUS session will try to establish with the server setting which has highest priority. If failed, it will try to connect to the server with next higher priority.
- **Key String:** Administrator can select user defined Encrypted or Plaintext to enter the key string form used for authenticating and encrypting the communication between the switch and the RADIUS server. This key must match the key configured on the RADIUS server. If administrator select use default (checked in checkbox) will use the default key string.
- **Retry:** Select User Defined to enter the number of requests that are sent to the RADIUS server before a failure is considered to have occurred, or select Use Default to use the default value.
- **Timeout:** Select User Defined to enter the number of seconds that the switch waits for an answer from the RADIUS server before retrying the query or switching to the next server, or select Use Default to use the default value. Set RADIUS server timeout value. If it is fail to connect to server, it will keep trying until timeout.
- **Usage:** Select the RADIUS server authentication type.
  - **Login:** RADIUS server is used for authenticating users that want to administer the switch.
  - **802.1X:** RADIUS server is used for authentication in 802.1X access control.
  - **All:** RADIUS server is used for authenticating user that wants to administer the switch and for authentication in 802.1X access control.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

10.2 TACACS+

Administrator can be configuration TACACS+ to connection TACACS+ Server to provide authentication and authorization for all devices in the organization.
This page allow user to add, edit or delete TACACS+ server settings and modify default parameter of TACACS+ server.



➢ **Use Default Parameters :**

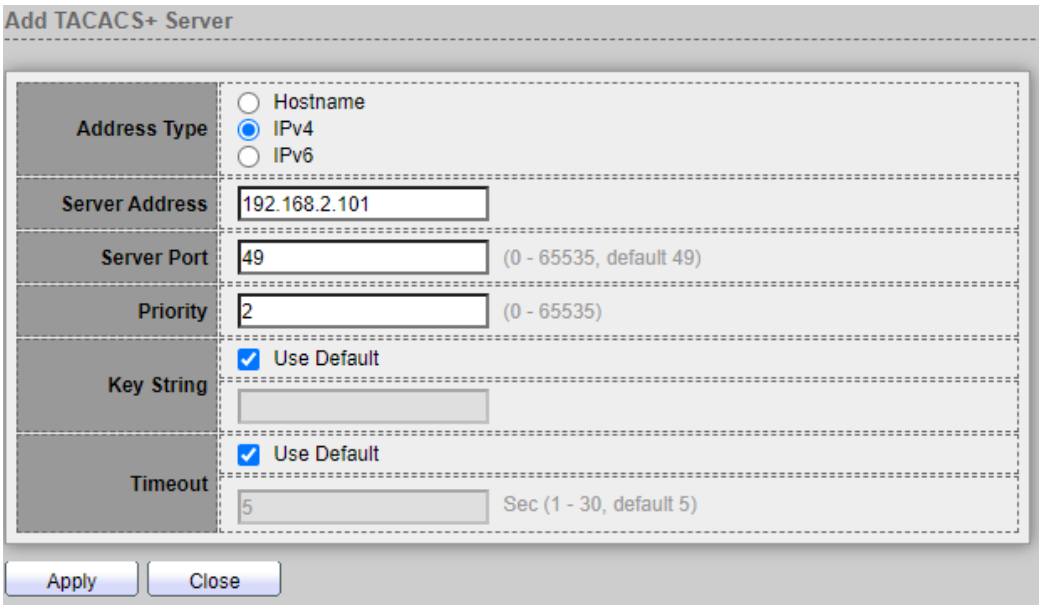
- **Timeout:** Enter the amount of time in seconds that passes before the connection between the switch and the TACACS+ server times out. If a value is not entered for an individual server, the value is taken from this field, default is 5.
- **Key String:** Enter the default key string in encrypted or plaintext form used for communicating with all TACACS+ servers.

Note	If administrator don't enter the default key string here, the key entered on the Add page must match the encryption key used by the TACACS+ server or enter the default key string here and a key string for an individual TACACS+ server, the key string configured for the individual TACACS+ server takes precedence.

*Click the **"Apply"** button to save your changes settings.*

Field	Description
Server Address	TACACS+ server address.
Server Port	TACACS+ server port.
Priority	TACACS+ server priority (smaller value has higher priority). TACACS+ session will try to establish with the server setting which has highest priority. If failed, it will try to connect to the server with next higher priority.
Retry	RADIUS server retry value. If it is fail to connect to server, it will keep trying until timeout with retry times.

Timeout	TACACS+ server timeout value. If it is fail to connect to server, it will keep trying until timeout.



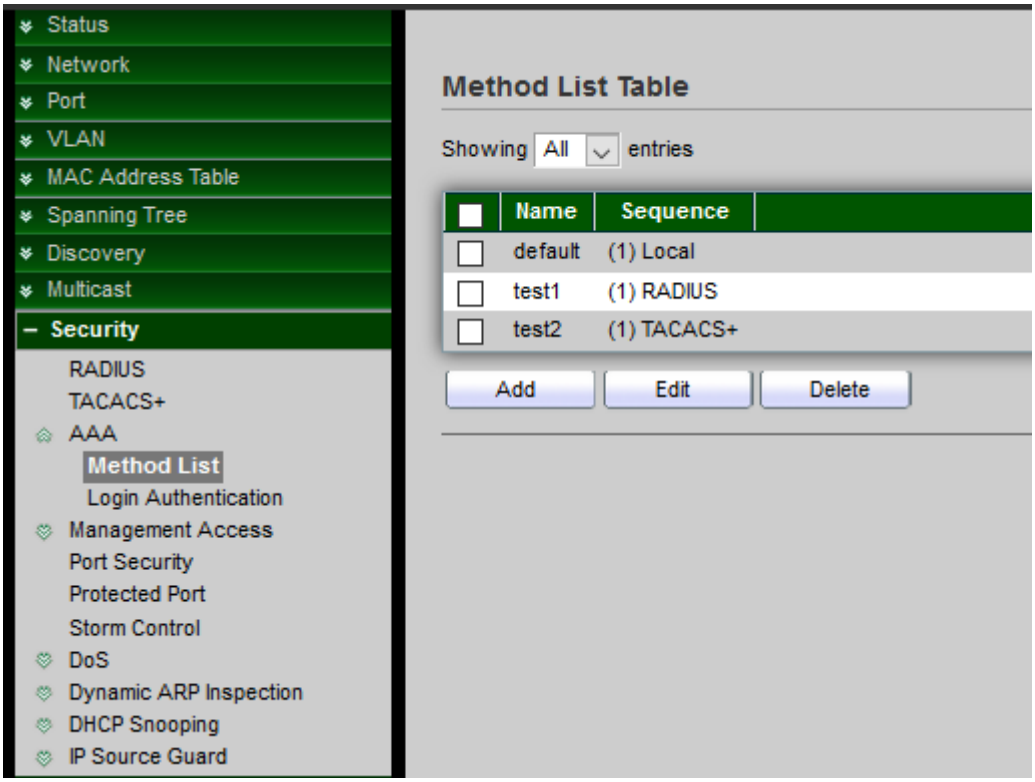
- **Address Type:** Select IP Version 4 / 6 or use Hostname typem, In add dialog, user need to specify server Address Type
  - **Hostname:** Use domain name as server address.
  - **IPv4:** Use IPv4 as server address.
  - **IPv6:** Use IPv6 as server address.
- **Server Address:** In add dialog, user need to input server address based on address type. In edit dialog, it shows current edit server address.
- **Server Port:** Set TACACS+ server port.
- **Priority:** Administrator can enter the priority of the server. The priority determines the order that the switch attempts to contact the servers to authenticate users. The switch first starts with the highest priority server. 0 is the high priority, Set TACACS+ server priority (smaller value has higher priority). TACACS+ session will try to establish with the server setting which has highest priority. If failed, it will try to connect to the server with next higher priority.
- **Key String:** Administrator can select user defined Encrypted or Plaintext to enter the key string form used for authenticating and encrypting the communication between the switch and the TACACS+ server. This key must match the key configured on the TACACS+ server. If administrator select use default (checked in checkbox) will use the default key string.
- **Timeout:** Set TACACS+ server timeout value. If it is fail to connect to server,it will keep trying until timeout.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

10.3 AAA

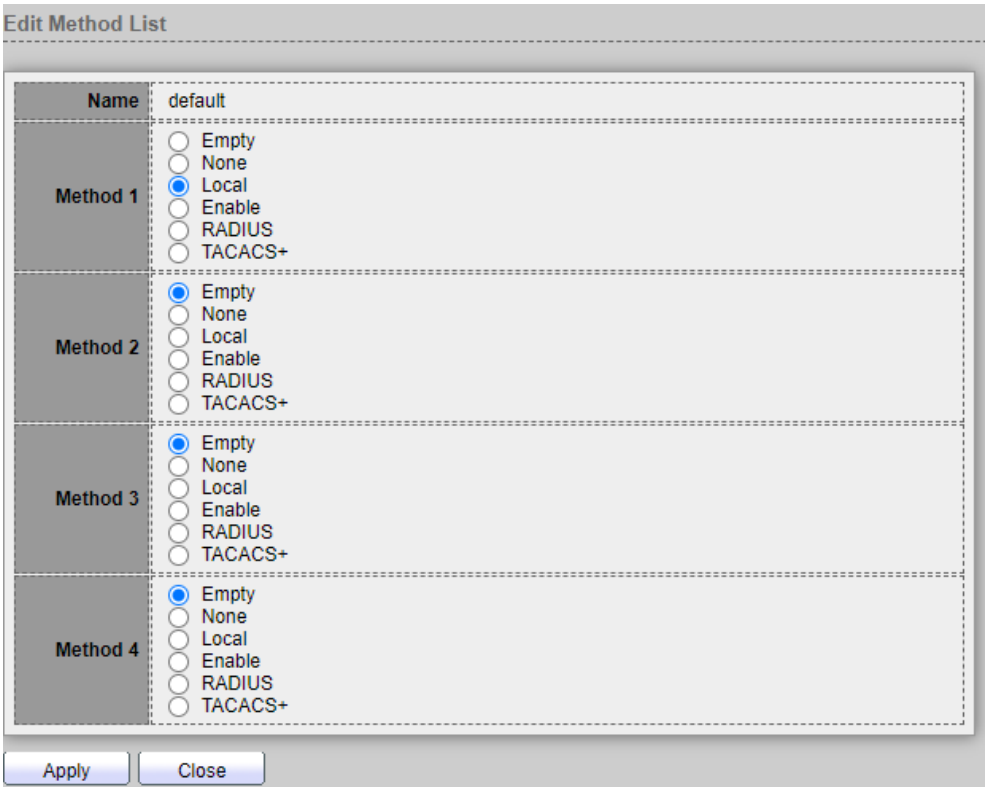
10.3.1 Method List

Administrator can set groups of AAA security, each group have 4 method table, each method can select 1 of 6 type which contains Empty / None / Local / Enable / RADIUS and TACACS+.
This page allow user to add, edit or delete login authentication list settings (The “default” list cannot be deleted.). The line combined to this list will authenticate login user by methods in this list. If the first method is failed, it will try to use the next priority method to authenticate if it exists.With RADIUS and TACACS+ methods, the failed means connecting to server fail. With Local method, the failed means cannot find the user in local database.



Field	Description
Name	Login authentication list name. This name should be different from other existing lists.

Sequence	Priority of login authentication method. • **None:** Authenticated with any condition. • **Local:** Use local accounts database to authenticate • **TACACS+:** Use remote TACACS+ server to authenticate. • **RADIUS:** Use remote Radius server to authenticate. • **Enable:** Use local enable password to authenticate



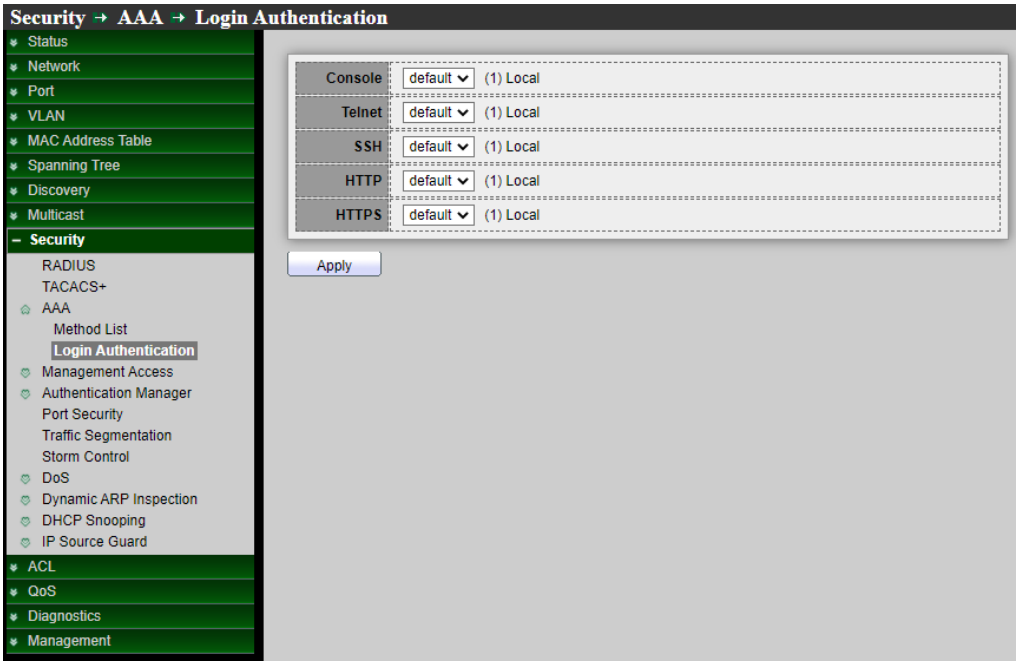
- **Name:** Login authentication list name. This name should be different from other existing lists.
- **Method 1:** Select first priority of login authentication method.
  - **None:** Authenticated with any condition.
  - **Local:** Use local accounts database to authenticate TACACS+: Use remote TACACS+ server to authenticate.
  - **RADIUS:** Use remote Radius server to authenticate.
  - **Enable:** Use local enable password to authenticate.
- **Method 2:** Select first priority of login authentication method.
  - **None:** Authenticated with any condition.
  - **Local:** Use local accounts database to authenticate TACACS+: Use remote TACACS+ server to authenticate.
  - **RADIUS:** Use remote Radius server to authenticate.
  - **Enable:** Use local enable password to authenticate.

- **Method 3:** Select first priority of login authentication method.
  - **None:** Authenticated with any condition.
  - **Local:** Use local accounts database to authenticate TACACS+: Use remote TACACS+ server to authenticate.
  - **RADIUS:** Use remote Radius server to authenticate.
  - **Enable:** Use local enable password to authenticate.
- **Method 4:** Select first priority of login authentication method.
  - **None:** Authenticated with any condition.
  - **Local:** Use local accounts database to authenticate TACACS+: Use remote TACACS+ server to authenticate.
  - **RADIUS:** Use remote Radius server to authenticate.
  - **Enable:** Use local enable password to authenticate.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

10.3.2 Login Authentication

When administrator has created security groups in "AAA➔method" then administrator can select different security group in service port.



Field	Description
Console	Specify login authentication list combined on console

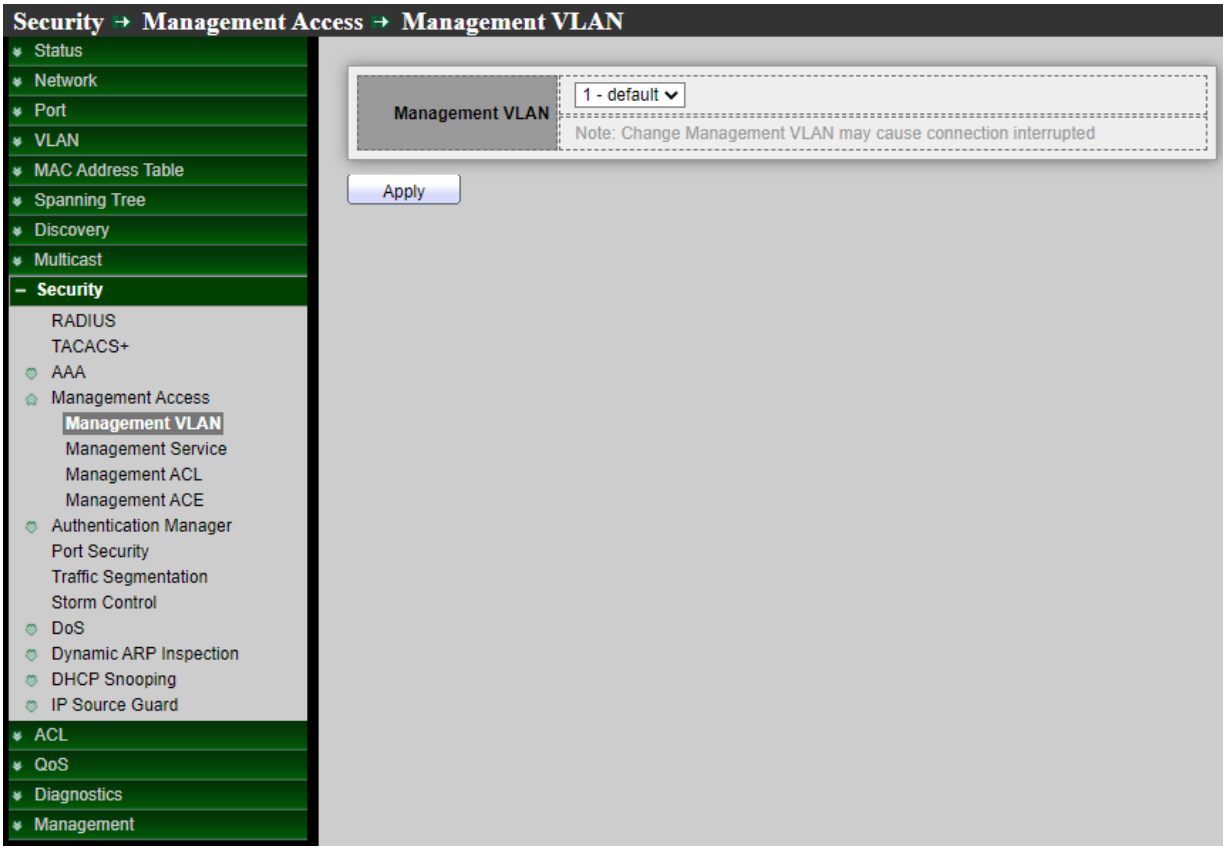
Telnet	Specify login authentication list combined on Telnet
SSH	Specify login authentication list combined on SSH
HTTPS	Specify login authentication list combined on HTTPS

*Click the **"Apply"** button to save your changes settings.*

10.4 Management Access

10.4.1 Management VLAN

When created VLAN function then administrator can select a specific VLAN, only allow this VLAN can to enter the UI management page.

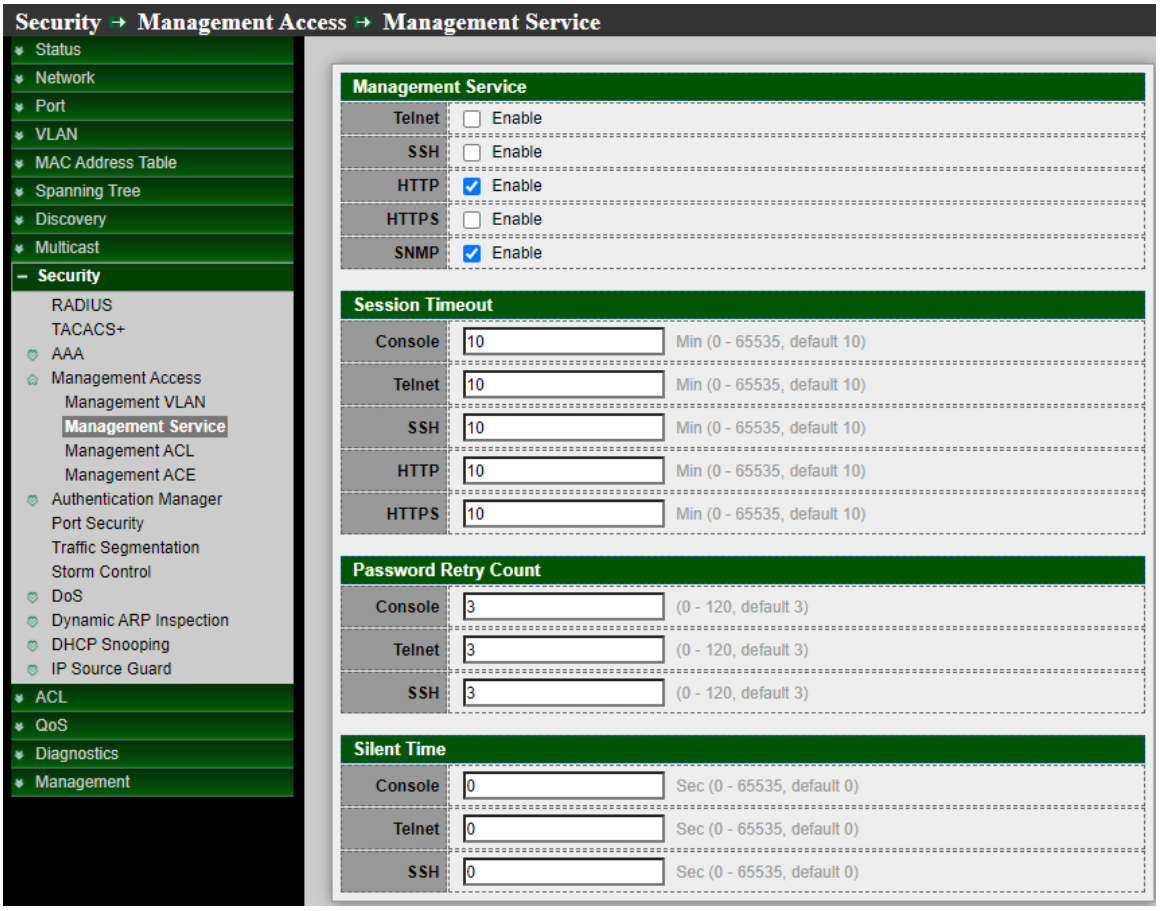


- **Management VLAN:** Select the Management VLAN ID.

*Click the "**Apply**" button to save your changes settings.*

10.4.2 Management Service

Administrator can select enable Telnet / SSH / HTTP / HTTPS / SNMP by different protocol to login service and configuration login timeout limit and password error retry count limit.



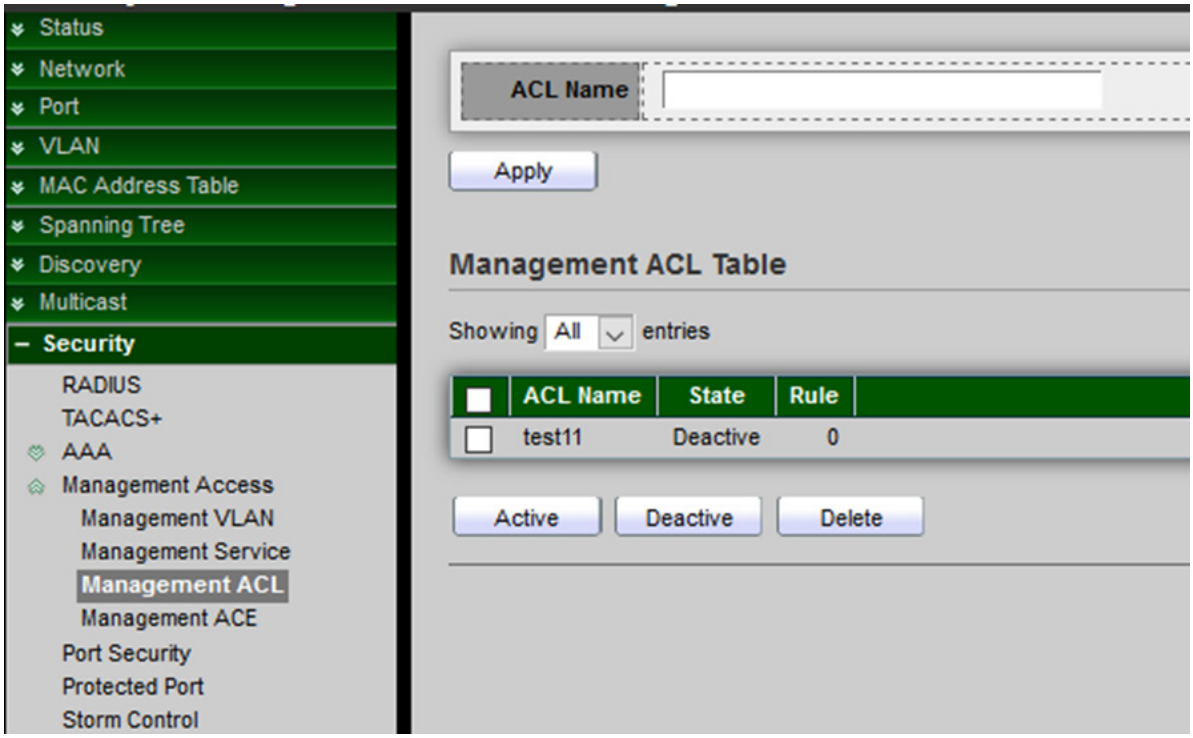
- **Management Service:** Management service admin state.
  - **Telnet:** Connect CLI through telnet.
  - **SSH:** Connect CLI through SSH.
  - **HTTP:** Connect WEBUI through HTTP.
  - **HTTPS:** Connect WEBUI through HTTPS.
  - **SNMP:** Manage switch trough SNMP.
- **Session Timeout:** Set session timeout minutes for user access to user interface. 0 minutes means never timeout, After login management page, in the set time if not session then system will auto timeout, administrator need re-login.
  - **Console:** Set console for session timeout 0~65535 minutes.
  - **Telnet:** Set Telnet for session timeout 0~65535 minutes.
  - **SSH:** Set SSH for session timeout 0~65535 minutes.
  - **HTTP:** Set HTTP for session timeout 0~65535 minutes.
  - **HTTPS:** Set HTTPS for session timeout 0~65535 minutes.

- **Password Retry Count:** Retry count is the number which CLI password input error tolerance count. After input error password exceeds this count, the CLI will freeze after silent time, If login error reaches the set value then login page will be kicked out, administrator need reopen the login page.
  - **Console:** Set console for password Retry count of 0~120 .
  - **Telnet:** Set Telnet for password Retry count of 0~120 .
  - **SSH:** Set SSH for password Retry count of 0~120 .
- **Silent Time:** This function to be matched "Password Retry Count" function, if login error reaches the set value within then set value of silent time will can't be reopen login page until the set time end ,After input error password exceeds password retry count, the CLI will freeze after silent time.
  - **Console:** Set console for Silent Time of 0~65535 minutes .
  - **Telnet:** Set Telnet for Silent Time of 0~65535 minutes .
  - **SSH:** Set SSH for for Silent Time of 0~65535 minutes .

10.4.3 Management ACL

Administrator can create ACL and set Active or Deactive the rules.
If administrator set "Active" will be apply "Management ACE" rules. ACL can set which ports is Permit or Deny connection to which services of the switch management interface.

Note	If only create one ACL Profile and click Active then these all ports and services will are all denied.



- **ACL Name:** Input MAC ACL name.

*Click the "**Apply**" button to save your changes settings.*

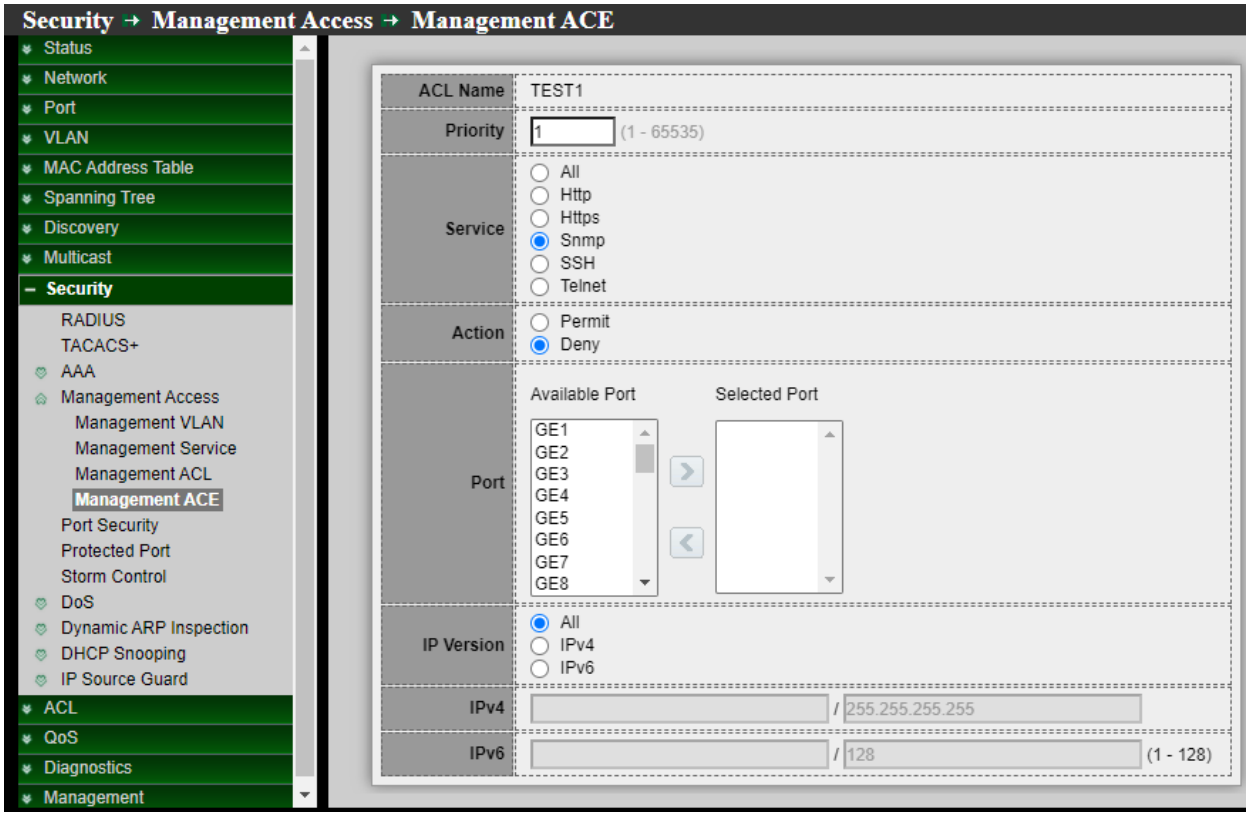
Field	Description
ACL Name	Display Management ACL name
State	Display Management ACL whether active.
Rule	Display the number Management ACE rule of ACL

*Set the **"Active"** and **"Deactive"** and **"Delete"** for this table management.*

10.4.4 Management ACE

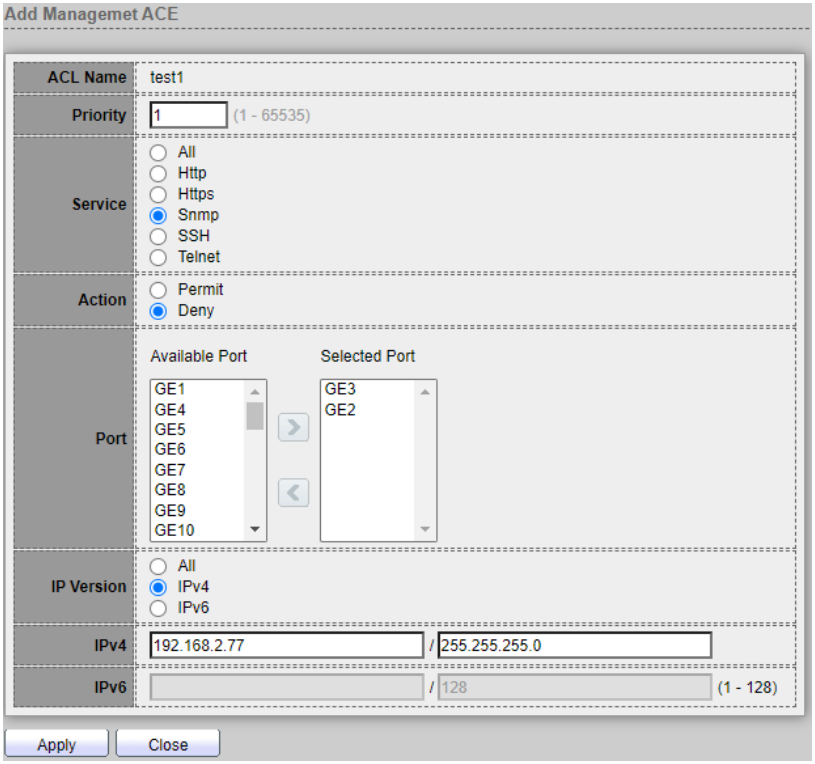
This management ACE page is to create an ACL profile rule. Administrator can select an created ACL profile to set security rule. If set the ACE only use Telnet a single rule. After confirmation the rule will apply to ACL profile.

Administrator can go to "management ACL" page click "Active" button to enable the rule. After active the rule, this management page will can't operating only use Telnet protocol to management, Setting **"add"** and **"Edit"** and **"Delete"** function for this management.



- **ACL Name:** Select the ACL name to which an ACE is being added.

Field	Description
Priority	Display the priority of ACE.
Action	Display the action of ACE
Service	Display the service ACE.
Port	Display the port list of ACE.
Address / Mask	Display the source IP address and mask of ACE.



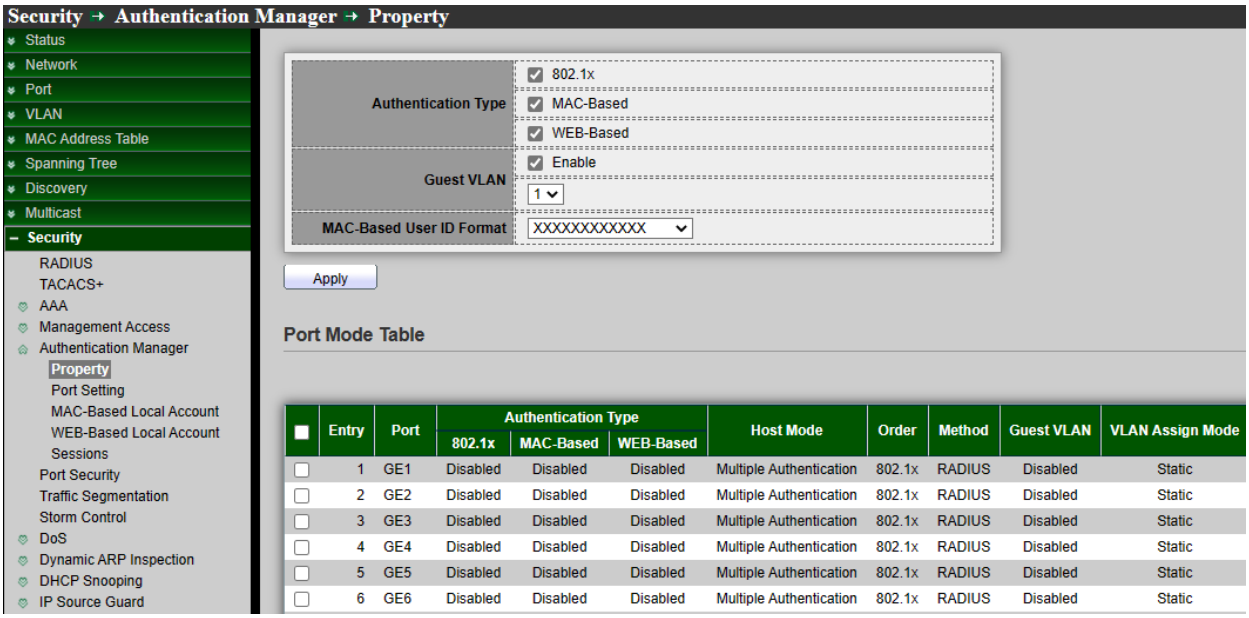
- **ACL Name**: Display the ACL name to which an ACE is being added.
- **Priority**: Set this rule priority, Specify the priority of the ACE. ACEs with higher sequence are processed first (1 is the highest priority). Only available on Add Dialog.
- **Service:** Select the type service of rule.
  - **All**: All services .
  - **HTTP**: Only HTTP service .
  - **HTTPs**: Only HTTPs service.
  - **SNMP**: Only SNMP service.
  - **SSH:** Only SSH service.
  - **Telnet**: Only Telnet service
- **Action:** Select the action after ACE match packet.
  - **Permit**: Forward packets that meet the ACE criteria.
  - **Deny**: Drop packets that meet the ACE criteria.
- **Port:** Select ports which will be matched.
- **IP Version:** Select the type of source IP address.
  - **All**: All IP addresses can access.
  - **IPv4**: Specify IPv4 address ca access.
  - **IPv6**: Specify IPv6 address ca access
- **IPv4:** Enter the source IPv4 address value and mask to which will be matched.
- **IPv6:** Enter the source IPv6 address value and mask to which will be matched.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

10.5 Authentication Manager

10.5.1 Property

This page allow user to edit authentication global settings and some port mods' configurations, Administrator can edit authentication global settings and some port mods' configurations.



- **Authentication Type :** Set checkbox to enable/disable following authentication types
  - 802.1x: Use IEEE 802.1x to do authentication
  - MAC-Based: Use MAC address to do authentication
  - WEB-Based: Prompt authentication web page for user to do authentication
- **Guest VLAN :** Set checkbox to enable/disable guest VLAN, if guest VLAN is enabled, you need to select one available VLAN ID to be guest VID.
- **MAC-Based User ID Format :** Select mac-based authentication RADIUS username/password ID format.
  - XXXXXXXXXXX
  - xxxxxxxxxxx
  - XX:XX:XX:XX:XX:XX
  - xx:xx:xx:xx:xx:xx
  - XX-XX-XX-XX-XX-XX
  - xx-xx-xx-xx-xx-xx
  - XX.XX.XX.XX.XX.XX
  - xx.xx.xx.xx.xx.xx
  - XXXX:XXXX:XXXX
  - xxxx:xxxx:xxxx

- XXXX-XXXX-XXXX
- xxxx-xxxx-xxxx
- XXXX.XXXX.XXXX
- xxxx.xxxx.xxxx
- XXXXXX:XXXXXX
- xxxxxx:xxxxxx
- XXXXXX-XXXXX
- xxxxxx-xxxxxx

*Click the **"Apply"** button to save your changes settings.*

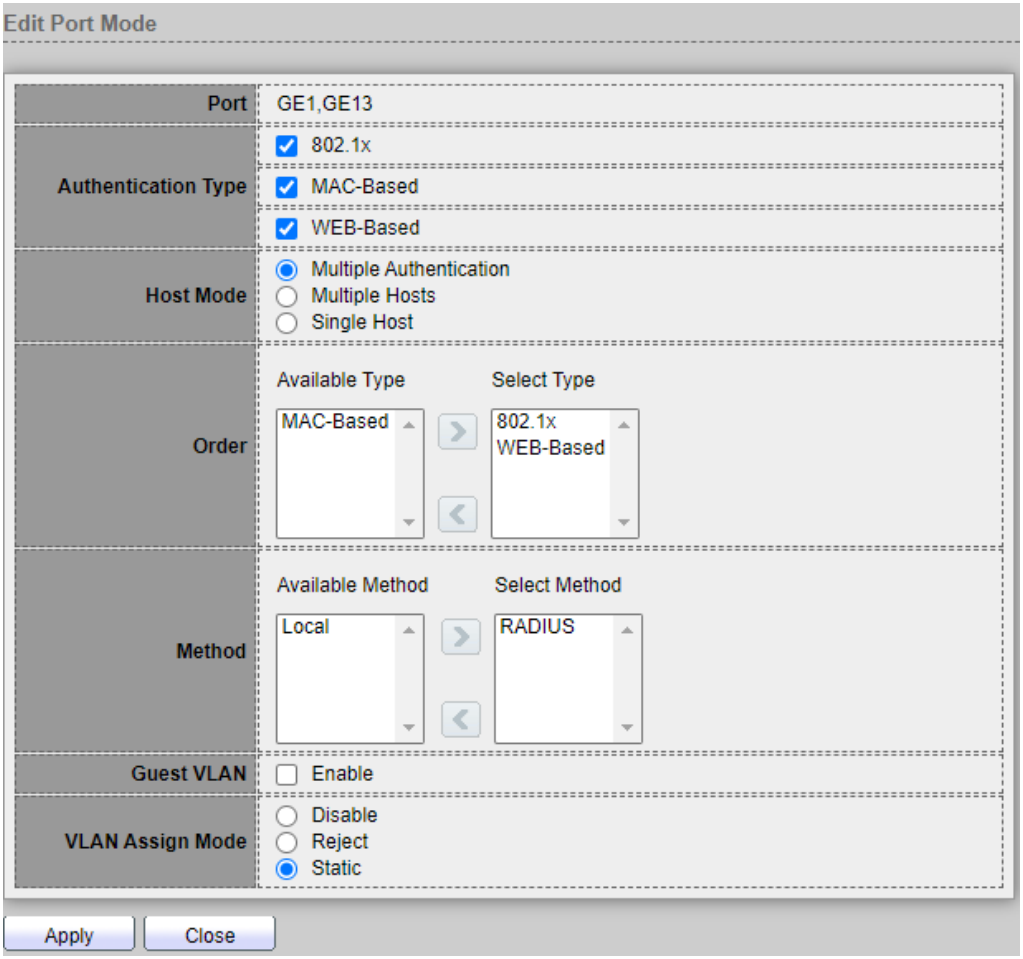
Port Mode Table

Entry	Port	Authentication Type			Host Mode	Order	Method	Guest VLAN	VLAN Assign Mode
		802.1x	MAC-Based	WEB-Based					
1	GE1	Enabled	Enabled	Enabled	Multiple Authentication	802.1x , WEB-Based	RADIUS , Local	Enabled	Disable
2	GE2	Enabled	Enabled	Enabled	Multiple Authentication	802.1x , WEB-Based	RADIUS , Local	Enabled	Disable
3	GE3	Enabled	Enabled	Enabled	Multiple Authentication	802.1x , WEB-Based	RADIUS , Local	Enabled	Disable
4	GE4	Enabled	Enabled	Enabled	Multiple Authentication	802.1x , WEB-Based	RADIUS , Local	Enabled	Disable
5	GE5	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
6	GE6	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
7	GE7	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
8	GE8	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
9	GE9	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static

Field	Description
Port	Port name
Authentication Type (802.1X)	802.1 X authentication type state • **Enabled:** 802.1X is enabled • **Disabled:** 802.1X is disabled
Authentication Type (MAC-Based)	MAC-Based authentication type state • **Enabled:** MAC-Based authentication is enabled • **Disabled:** MAC-Based authentication is disabled
Authentication Type (WEB-Based)	WEB-Based authentication type state • **Enabled:** WEB-Based authentication is enabled • **Disabled:** WEB-Based authentication is disabled
Host Mode	Authenticating host mode • **Multiple Authentication:** In this mode, every client need to pass authenticate procedure individually.

	• **Multiple Hosts:** In this mode, only one client need to be authenticated and other clients will get the same access accessibility. Web-auth cannot be enabled in this mode. • **Single Host:** In this mode, only one host is allowed to be authenticated. It is the same as Multi-auth mode with max hosts number configure to be 1.
Order	Support following authentication type order combinations. Web Authentication should always be the last type. The authentication manager will go to next type if current type is not enabled or authenticated fail. • **802.1x** • **MAC-Based** • **WEB-Based** • **802.1x MAC-Based** • **802.1x WEB-Based** • **MAC-Based 802.1x** • **WEB-Based 802.1x** • **802.1x MAC-Based WEB-Based** • **802.1x WEB-Based MAC-Based**
Method	Support following authentication method order combinations. These orders only available on MAC-Based authentication and WEB-Based authentication. 802.1x only support Radius method. • **Local:** Use DUT's local database to do authentication • **Radius:** Use remote RADIUS server to do authentication • **Local Radius** • **Radius Local**
Guest VLAN	Port guest VLAN enable state • **Enabled:** Guest VLAN is enabled on port • **Disabled:** Guest VLAN is disabled on port
VLAN Assign Mode	Support following VLAN assign mode and only apply when source is RADIUS • **Disable:** Ignore the VLAN authorization result and keep original VLAN of host. • **Reject:** If get VLAN authorized information, just use it. However, if there is no VLAN authorized information, reject the host and make it unauthorized.

- **Static:** If get VLAN authorized information, just use it. If there is no VLAN authorized information, keep original VLAN of host.



- **Port :** Display selected Port number.
- **Authentication Type :** Set checkbox to enable/disable authentication types.
  - **802.1x :** Use IEEE 802.1x to do authentication
  - **MAC-Based :** Use MAC address to do authentication
  - **WEB-Based :** Prompt authentication web page for user to do authentication
- **Host Mode :** Select authenticating host mode.
  - **Multiple Authentication :** In this mode, every client need to pass authenticate procedure individually
  - **Multiple Hosts :** In this mode, only one client need to be authenticated and other clients will get the same access accessibility. Web-auth cannot be enabled in this mode.

- **Single Host :** In this mode, only one host is allowed to be authenticated. It is the same as Multi-auth mode with max hosts number configure to be 1.

➢ **Order :** Support following authentication type order combinations. Web Authentication should always be the last type. The authentication manager will go to next type if current type is not enabled or authenticated fail.

- 802.1x
- MAC-Based
- WEB-Based
- 802.1x MAC-Based
- 802.1x WEB-Based
- MAC-Based 802.1x
- WEB-Based 802.1x
- 802.1x MAC-Based WEB-Based
- 802.1x WEB-Based MAC-Based

➢ **Method :** Support following authentication method order combinations.These orders only available on MAC-Based authentication and WEB-Based authentication. 802.1x only support Radius method.

- **Local :** Use DUT's local database to do authentication
- **Radius :** Use remote RADIUS server to do authentication

➢ **Guest VLAN :** Set checkbox to enable/disable guest VLAN.

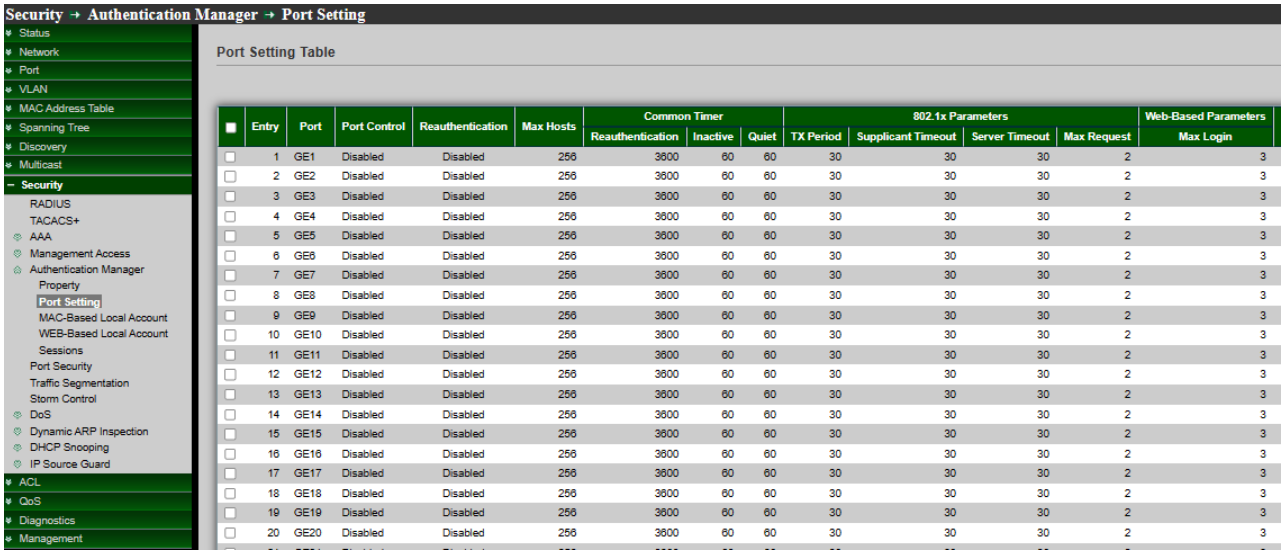
➢ **VLAN Assign Mode :** Support following VLAN assign mode and only apply when source is RADIUS.

- **Disable**: Ignore the VLAN authorization result and keep original VLAN of host.
- **Reject**: If get VLAN authorized information, just use it. However, if there is no VLAN authorized information, reject the host and make it unauthorized.Local Radius.
- **Static**: If get VLAN authorized information, just use it. If there is no VLAN authorized information, keep original VLAN of host.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

10.5.2 Port Setting

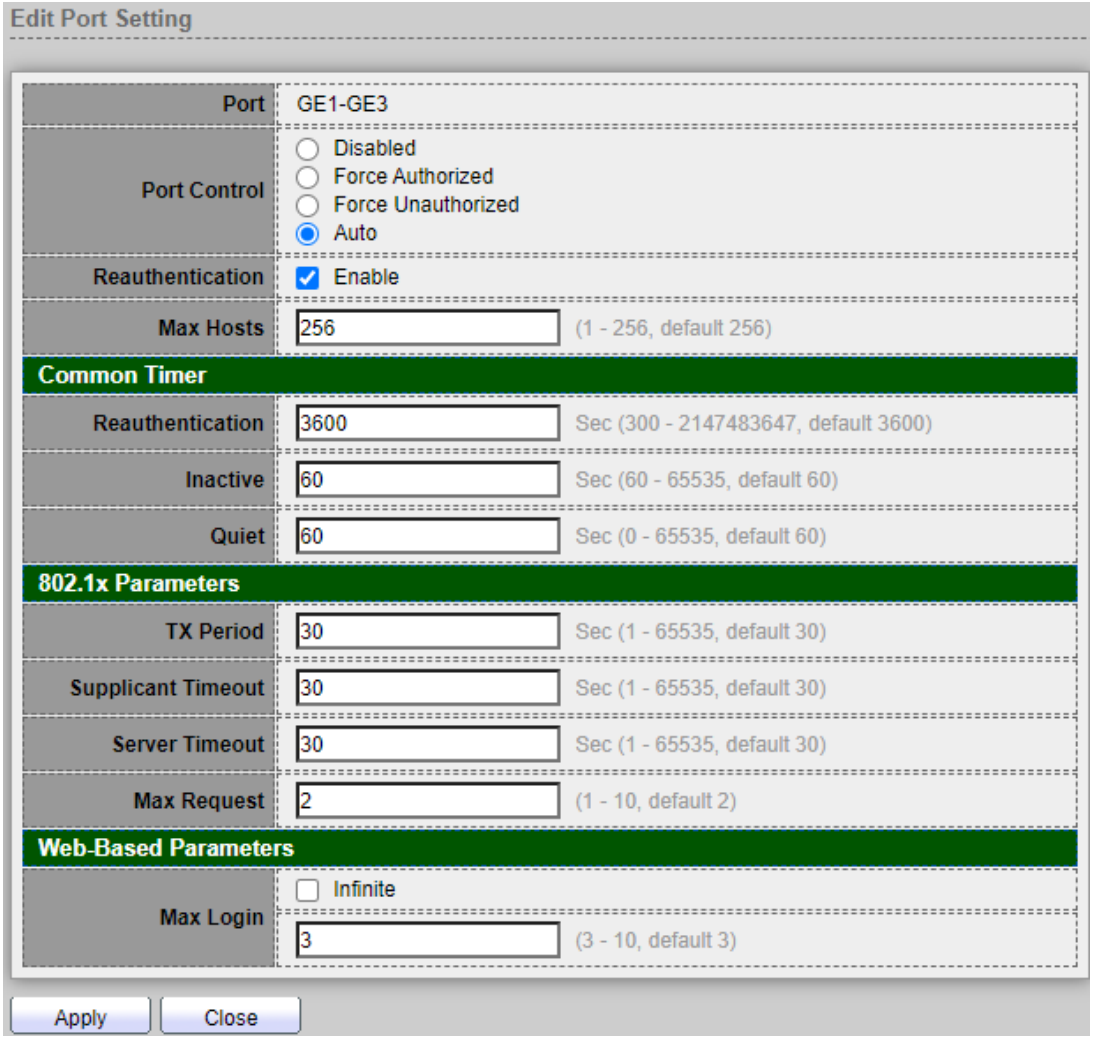
Administrator can configure authentication manger port settings,This page allow user to configure authentication manger port settings



Entry	Port	Port Control	Reauthentication	Max Hosts	Common Timer			802.1x Parameters				Web-Based Parameters
					Reauthentication	Inactive	Quiet	TX Period	Supplicant Timeout	Server Timeout	Max Request	Max Login
1	GE1	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
2	GE2	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
3	GE3	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
4	GE4	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
5	GE5	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
6	GE6	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
7	GE7	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
8	GE8	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
9	GE9	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
10	GE10	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
11	GE11	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
12	GE12	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
13	GE13	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
14	GE14	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
15	GE15	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
16	GE16	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
17	GE17	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
18	GE18	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
19	GE19	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
20	GE20	Disabled	Disabled	256	3600	60	60	30	30	30	2	3

Field	Description
Port	Port name
Port Control	Support following authentication port control types. • **Disable:** Disable authentication function and all clients have network accessibility. • **Force Authorized:** Port is force authorized and all clients have network accessibility. • **Force Unauthorized:** Port is force unauthorized and all clients have no network accessibility. • **Auto:** Need passing authentication procedure to get network accessibility.
Reauthentication	Reautheticate state • **Enabled:** Host will be reauthenticated after reauthentication period • **Disabled:** Host will not be reauthenticated after reauthentication period.
Max Hosts	In Multiple Authentication mode, total host number cannot not exceed max hosts number
Common Timer	• **Reauthentication:** After re-authenticate period, host will return to initial state and need to pass authentication procedure again. • **Inactive:** If no packet from the authenticated host, the inactive timer will increase. After inactive timeout, the host will be

	unauthorized and corresponding session will be deleted. In multi-host mode, the packet is counting on the authorized host only and not all packets on the port. • **Quiet:** When port is in Locked state after authenticating fail several times, the host will be locked in quiet period. After this quiet period, the host is allowed to authenticate again.
802.1X Params	• **TX Period:** Number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the supplicant (client) before resending the request. • **Supplicant Timeout:** The maximum number of EAP requests that can be sent. If a response is not received after the defined period (supplicant timeout), the authentication process is restarted. • **Server Timeout:** Number of seconds that lapses before EAP requests are resent to the supplicant. • **Max Request:** Number of seconds that lapses before the device resends a request to the authentication server
Web-Based Param (Max Login)	Allow user login fail number. After login fail number exceed, the host will enter Lock state and is not able to authenticate until quiet period exceed.



- **Port :** Display selected Port number.
- **Port Control :** Support following authentication port control types.
  - **Disable :** Disable authentication function and all clients have network accessibility.
  - **Force Authorized :** Port is force authorized and all clients have network accessibility.
  - **Force Unauthorized :** Port is force unauthorized and all clients have no network accessibility.
  - **Auto :** Need passing authentication procedure to get network accessibility.
- **Reauthentication :** Set checkbox to enable/disable reuauthentication.
- **Max Hosts :** In Multiple Authentication mode, total host number cannot not exceed max hosts number.
- **Common Timer:**
  - **Reauthentication :** After re-authenticate period, host will return to initial state and need to pass authentication procedure again.

- **Inactive :** If no packet from the authenticated host, the inactive timer will increase. After inactive timeout, the host will be unauthorized and corresponding session will be deleted. In multi-host mode, the packet is counting on the authorized host only and not all packets on the port.
- **Quiet :** When port is in Locked state after authenticating fail several times, the host will be locked in quiet period. After this quiet period, the host is allowed to authenticate again.
- **Auto :** Need passing authentication procedure to get network accessibility.

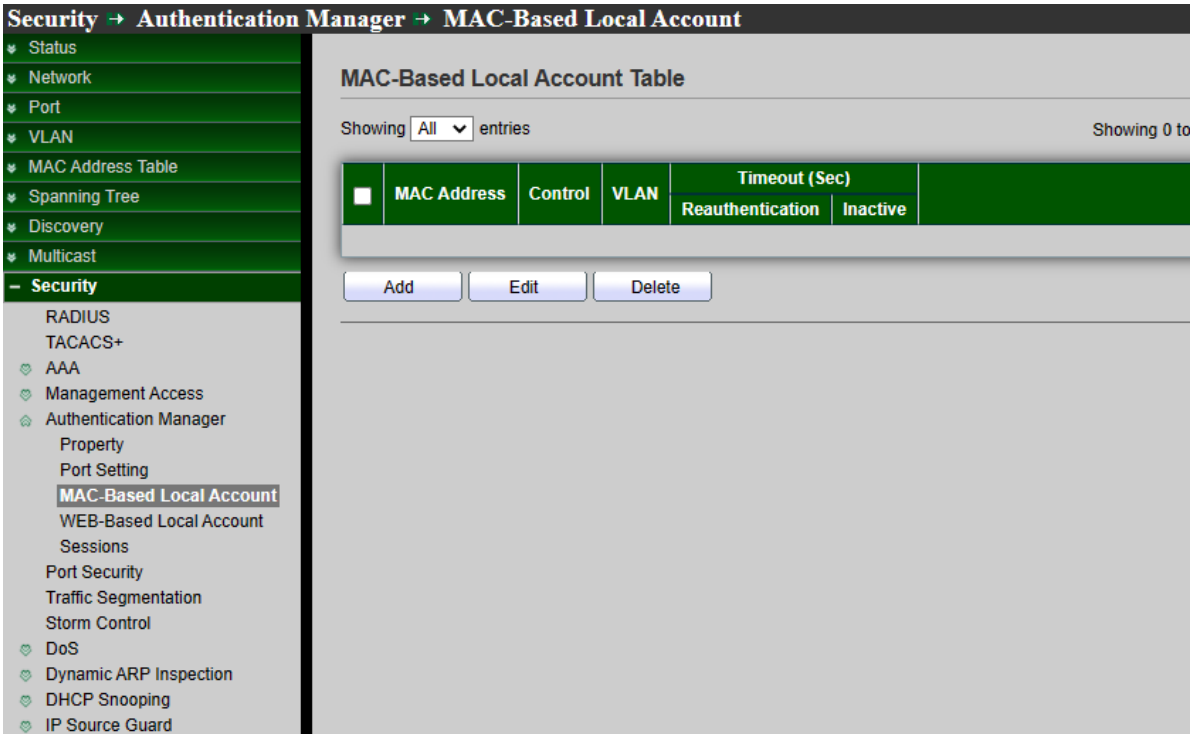
➢ **802.1X Params :**

- **TX Period :** Number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the supplicant (client) before resending the request.
- **Supplicant Timeout :** The maximum number of EAP requests that can be sent. If a response is not received after the defined period (supplicant timeout), the authentication process is restarted.
- **Server Timeout:** Number of seconds that lapses before EAP requests are resent to the supplicant.
- **Max Request :** Number of seconds that lapses before the device resends a request to the authentication server.
- **Max Login :** Set checkbox to set max login number to be infinite or specify max login number.

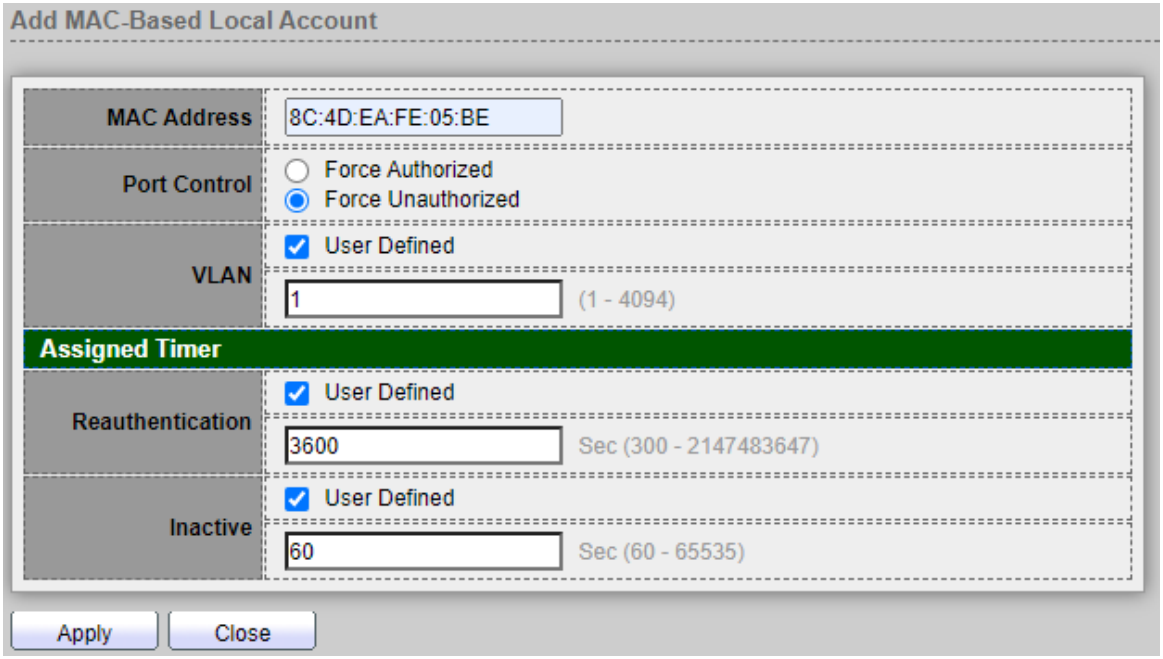
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

10.5.3 MAC-Based Local Account

Administrator can allow to add/edit/delete MAC-Based authentication local accounts, Setting **“add”** and **“Edit”** and **“Delete”** function for this management.



Field	Description
MAC Address	Authenticated host MAC address, and each MAC allow only one entry in local database.
Control	Control Type • **Force Authorized:** Host will be force authorized. • **Force Unauthorized:** Host will be force unauthorized.
VLAN	Assigned VLAN ID for the authenticated host.
Timeout	• **Reauthentication:** Assigned reauthentication period for the authenticated host. • **Inactive:** Assigned inactive timeout for the authenticated host.

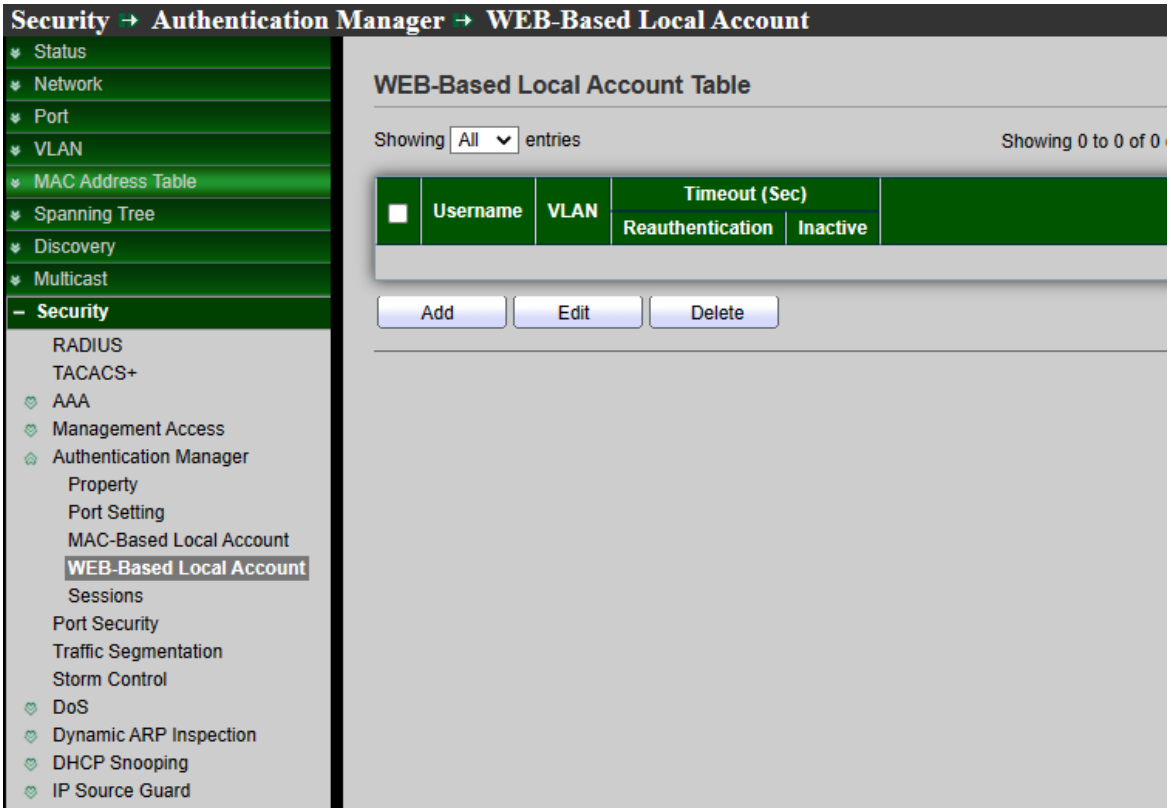


- **MAC Address :** Authenticated host MAC address, and each MAC allow only one entry in local database.
- **Port Control :** Support following authentication port control types.
  - **Force Authorized:** Host will be force authorized.
  - **Force Authorized :** Host will be force unauthorized.
- **VLAN :** Assigned VLAN ID for the authenticated host.
- **Assigned Timer:**
  - **Timeout (Reauthentication) :** Assigned reauthentication period for the authenticated host.
  - **Timeout (Inactive) :** Assigned inactive timeout for the authenticated host.

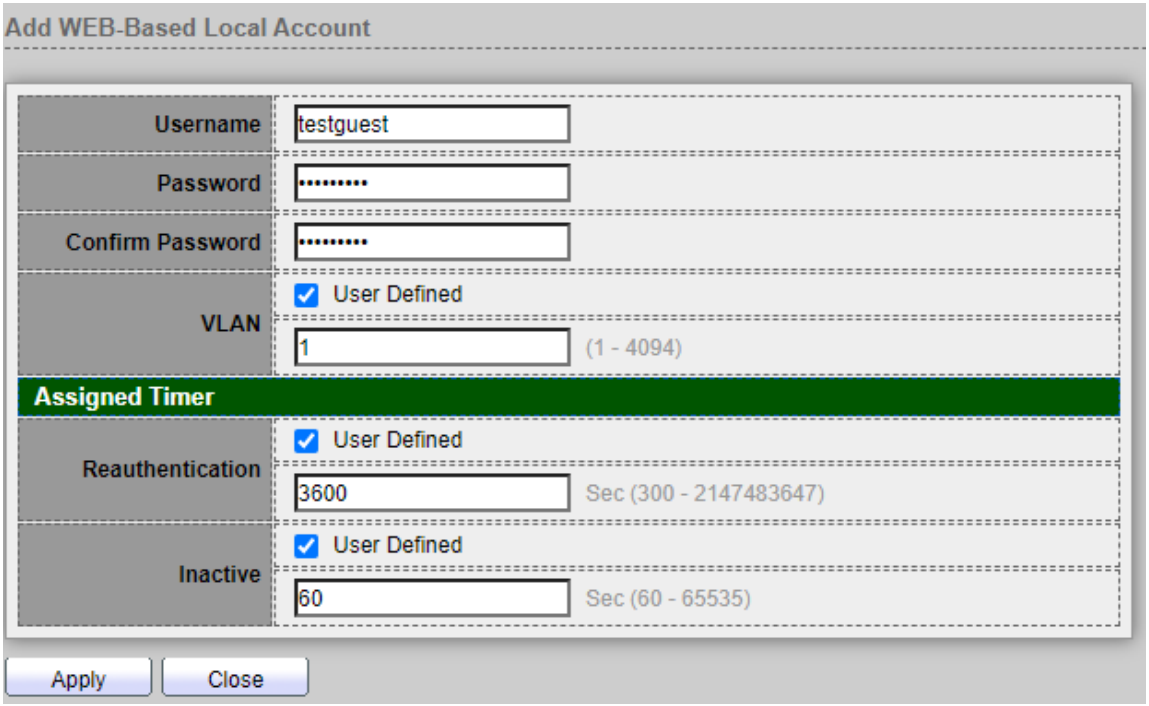
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

10.5.4 WEB-Based Local Account

Administrator can allow to add/edit/delete WEB-Based authentication local accounts, Setting **“add”** and **“Edit”** and **“Delete”** function for this management.



Field	Description
Username	Authenticating account user name
VLAN	Assigned VLAN ID for the authenticated host.
Timeout(Sec)	• **Reauthentication:** Assigned reauthentication period for the authenticated host. • **Inactive:** Assigned inactive timeout for the authenticated host.

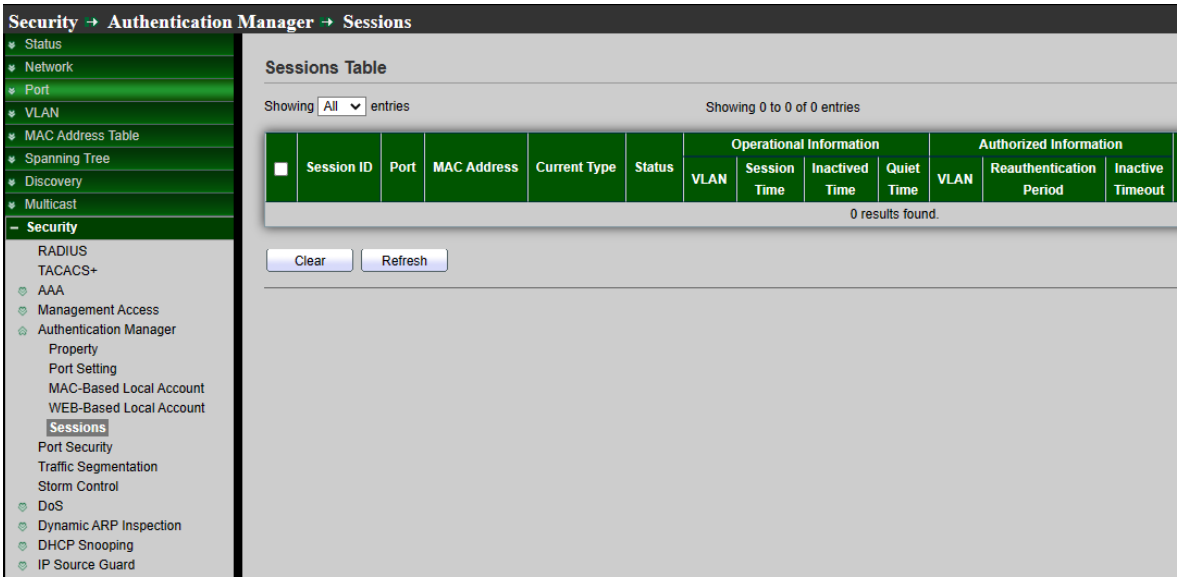


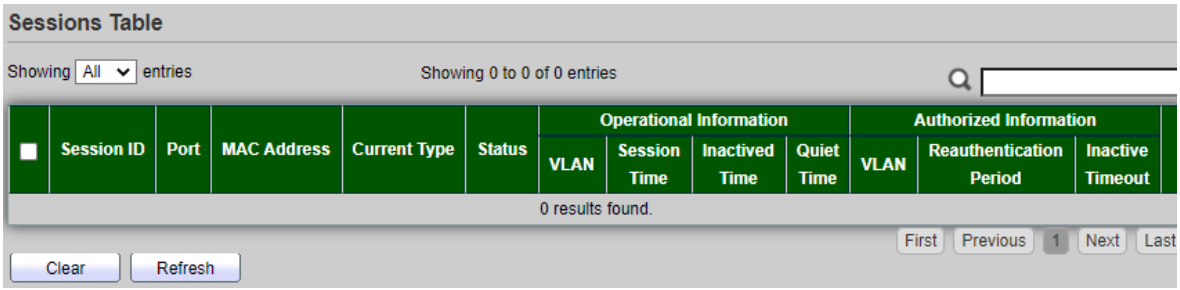
- **Username :** Authenticating account user name.
- **Password :** Authenticating account password.
- **Confirm Password :** Confirm authenticating account password.
- **VLAN :** Assigned VLAN ID for the authenticated host.
- **Assigned Timer:**
  - **Timeout (Reauthentication) :** Assigned reauthentication period for the authenticated host.
  - **Timeout (Inactive) :** Assigned inactive timeout for the authenticated host.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

10.5.5 Sessions

Administrator can check all detail information of authentication sessions and allow user to select specific session to delete by clicking **"Clear "** button.





Field	Description
Session ID	Session ID is unique of each session
Port	Port name which the host located
MAC Address	Host MAC address
Current Type	Show current authenticating type • **802.1x:** Use IEEE 802.1X to do authenticating • **MAC-Based:** Use MAC-Based authentication to do authenticating • **WEB-Based:** Use WEB-Based authentication to do authenticating

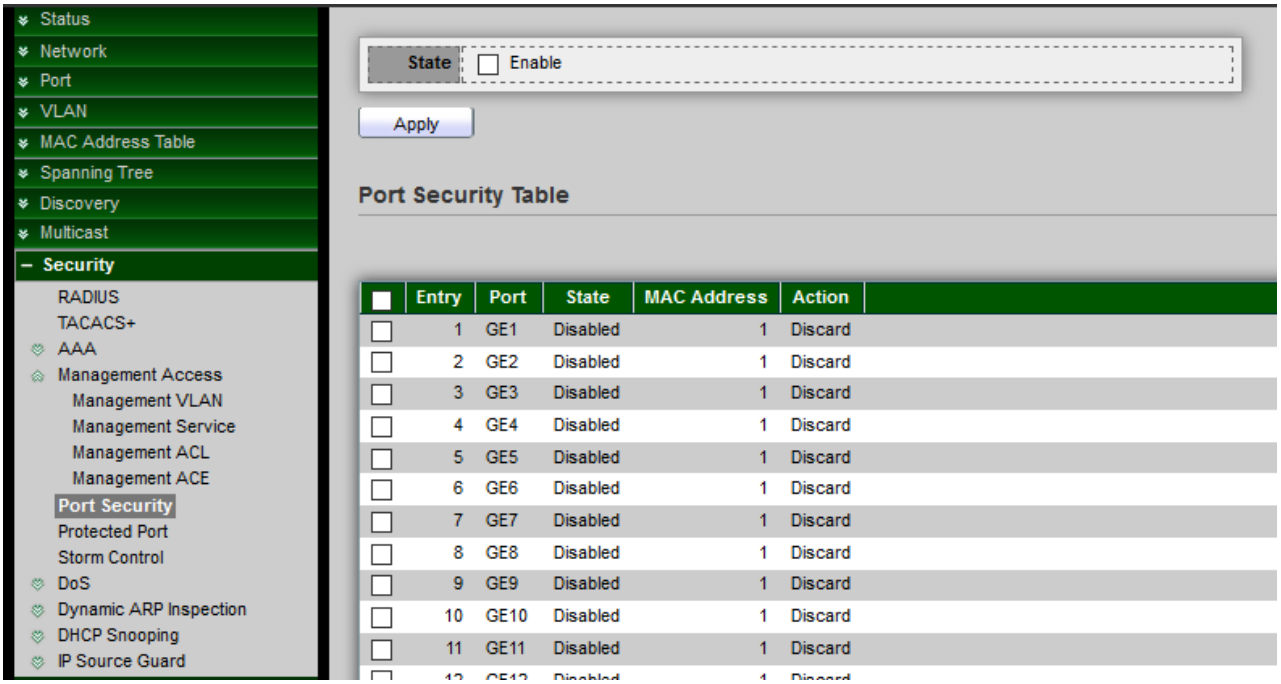
Status	Show host authentication session status • **Disable:** This session is ready to be deleted • **Running:** Authentication process is running • **Authorized:** Authentication is passed and getting network accessibility. • **UnAuthorized:** Authentication is not passed and not getting network accessibility. • **Locked:** Host is locked and do not allow to do authenticating until quiet period. • **Guest:** Host is in the guest VLAN.
Operationl	• **VLAN:** Shows host operational VLAN ID. • **Session Time:** In "Authorized" state, it shows total time after authorized. • **Inactived:** In "Authorized" state, it shows how long the host do not send any packet. • **Quiet Time:** In "Locked" state, it shows total time after locked. • **Locked:** Host is locked and do not allow to do authenticating until quiet period.
Authorized	• **VLAN:** Shows VLAN ID given from authorized procedure. • **Reauthentication Period:** Shows reauthentication period given from authorized procedure. • **Inactive Timeouts:** Shows inactive timeout given from authorized procedure.

*Click the **"Clear"** button to clear this page or click the **"Refresh"** button to refresh the page .*

10.6 Port Security

Port security examines all traffic received by secure ports to detect violations or to recognize and secure new MAC addresses. When the shutdown violation mode is configured, traffic cannot enter the secure port after a violation has been detected, which removes the possibility that violations might cause excessive CPU load.

Port security monitors received packets. Access to locked ports is limited to users with specific MAC addresses, This page allow user to configure port security settings for each interface. When port security is enabled on interface, action will be perform once MAC address over.

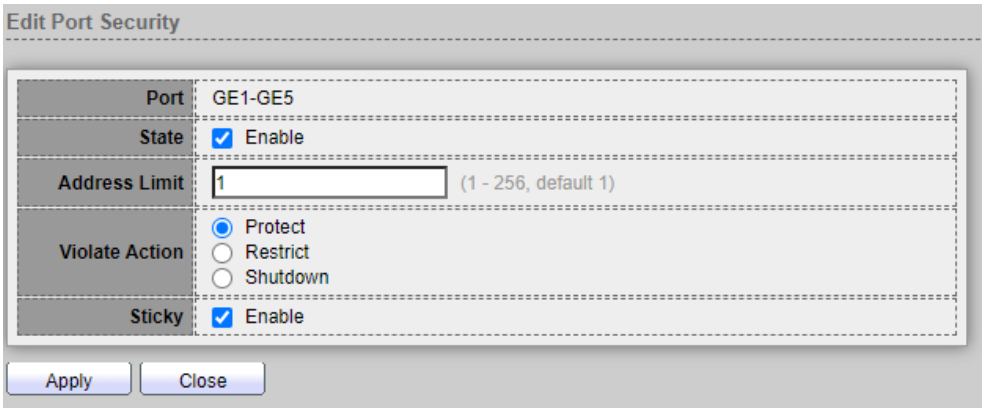


- **State:** Select the status of port security
  - **Disable:** Disable port security function.
  - **Enable:** Enable port security function.
- **Rate Limit :** Set rate limit of 1-600 packets per second.

Note	When the protect or restrict violation modes are configured, port security continues to process traffic after a violation occurs, which might cause excessive CPU load. Configure the port security rate limiter to protect the CPU against excessive load when the protect or restrict violation modes are configured.

*Click the **"Apply"** button to save your changes settings.*

Field	Description
Port	Port name which the port security.
State	Display port security of Enable or Disable state.
Addres Limie	Displays the maximum number of port security of MAC addresses that can be configured on the port.
Total	Displays the number of all port security total MAC addresses on the port.
Configured	Displays the number of all port security MAC addresses configured on the port.
Violate Active	Displays the operational state that the interface applies to packets arriving on the locked interface. • **Protect.** • **Restrict.** • **Shutdown.**
Sticky	Display port security sticky of Enable or Disable.



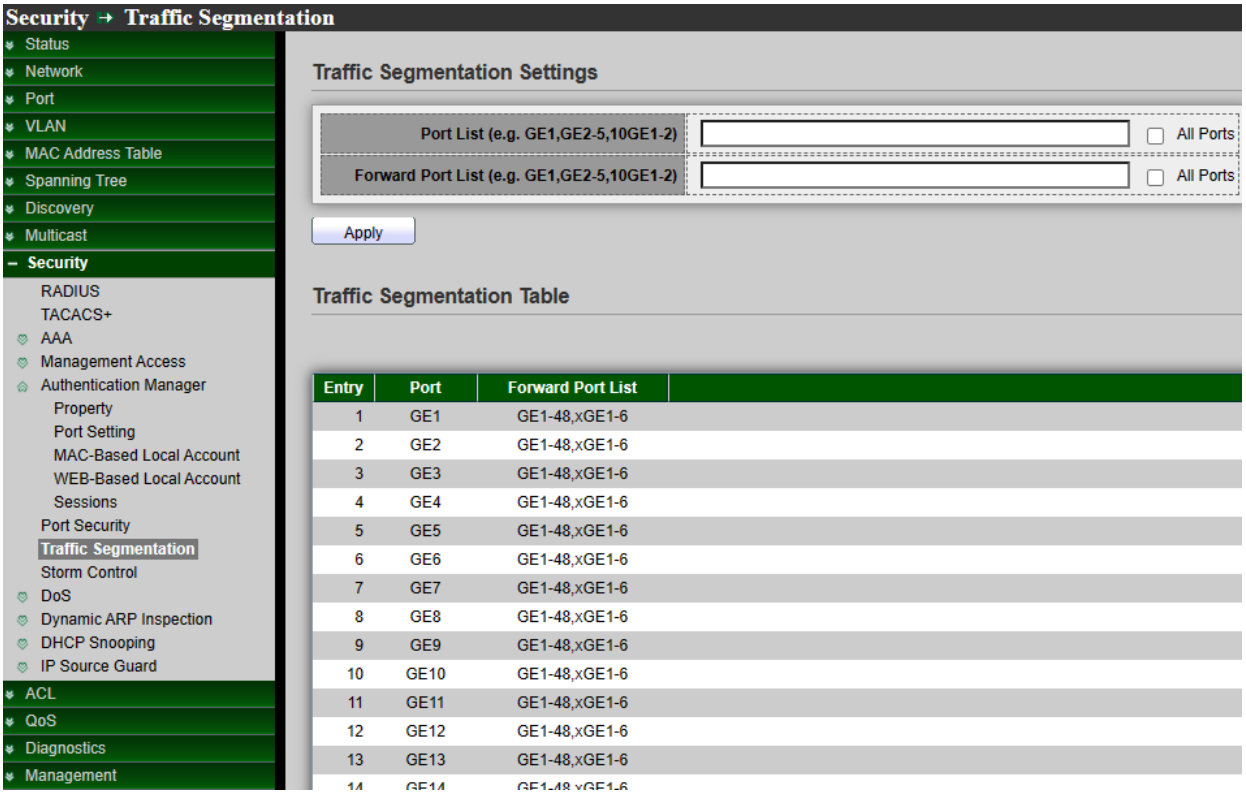
- **Port:** Display selected Port number.
- **State:** Enable or Un-Enable the port security.
- **Address Limit:** When configuring port security, the maximum number of secure MAC addresses that can be configured in the switch, A secure port has a default of one MAC address. The default can be changed to any value between 1 and 256. The upper limit of 256 guarantees one MAC address per port.
- **Violate Action:** Select the action if learned mac addresses, If Interface Status is locked, select an action to be applied to packets arriving on a locked interface.
  - **Protect:** Drop packets with invalid MAC address.
  - **Restrict:** Drop packets with invalid MAC address and log the event.

- **Shutdown:** Drop packets with invalid MAC address and shut down the interface of port, and log the event.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

10.7 Traffic Segmentation

Segmentation works by controlling how traffic flows among the parts. You could choose to stop all traffic in one part from reaching another, or you can limit the flow by traffic type, source, destination, and many other options. How you decide to segment your network is called a segmentation policy.



Traffic Segmentation Setting

- **Port List:** Set port List (e.g. GE1,GE2-5,10GE1-2).
- **Forward Port List:** Set forward Port List (e.g. GE1,GE2-5,10GE1-2).

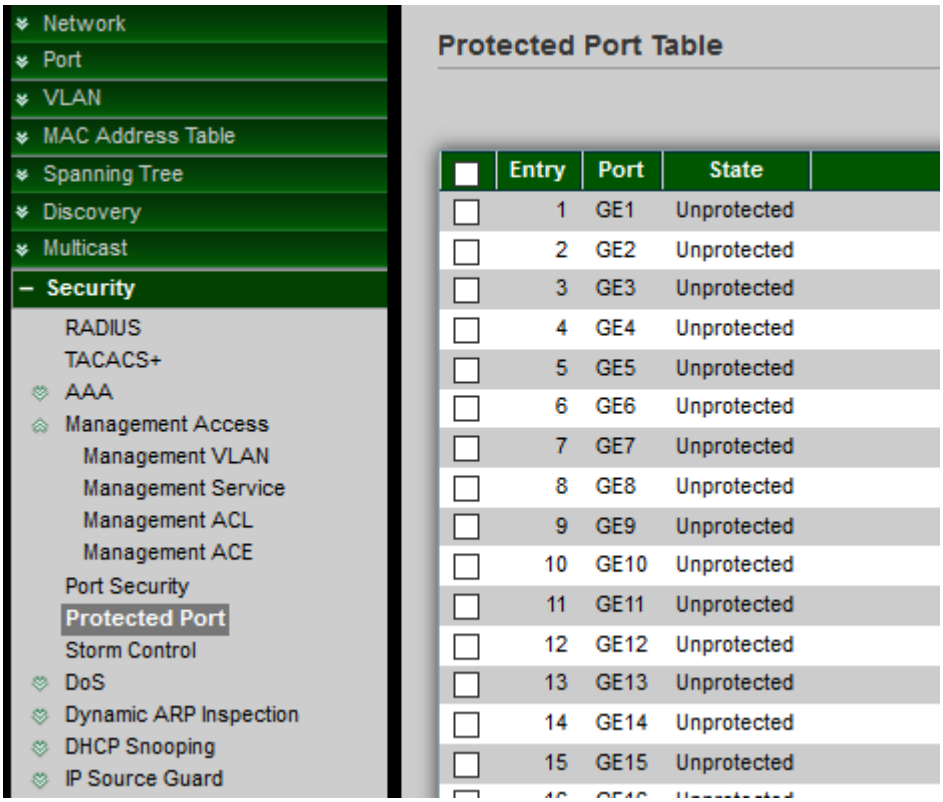
*Click the **"Apply"** button to save your changes settings.*

Field	Description

Port	Port Name
Forward Port List	Disaplay forward port list

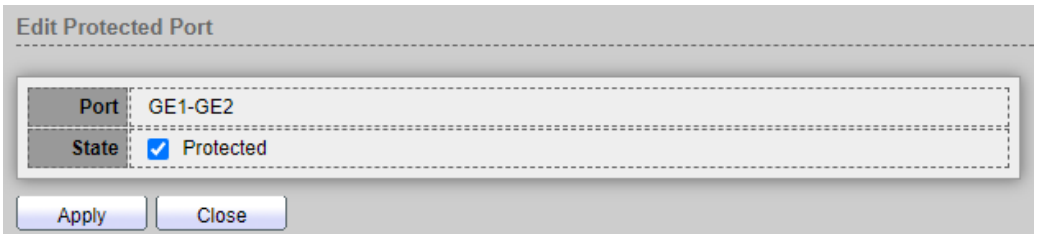
10.8 Protected Port

This page allow user to configure protected port setting to prevent the selected ports from communication with each other. Protected port is only allowed to communicate with unprotected port. In other words, protected port is not allowed to communicate with another protected port. If administrators check enable to make this a protected port. A protected port is also referred as a Private VLAN Edge. It's provide Layer 2 isolation between interfaces (Ethernet ports and Link Aggregation Groups) that share the same Broadcast domain (VLAN).After enable protected port, packets received from protected ports can be forwarded only to unprotected egress ports and unrestricted by VLAN members.



Field	Description
Port	Port Name

State	Port protected admin state. • **Protected:** Port is protected. • **Unprotected:** Port is unprotected

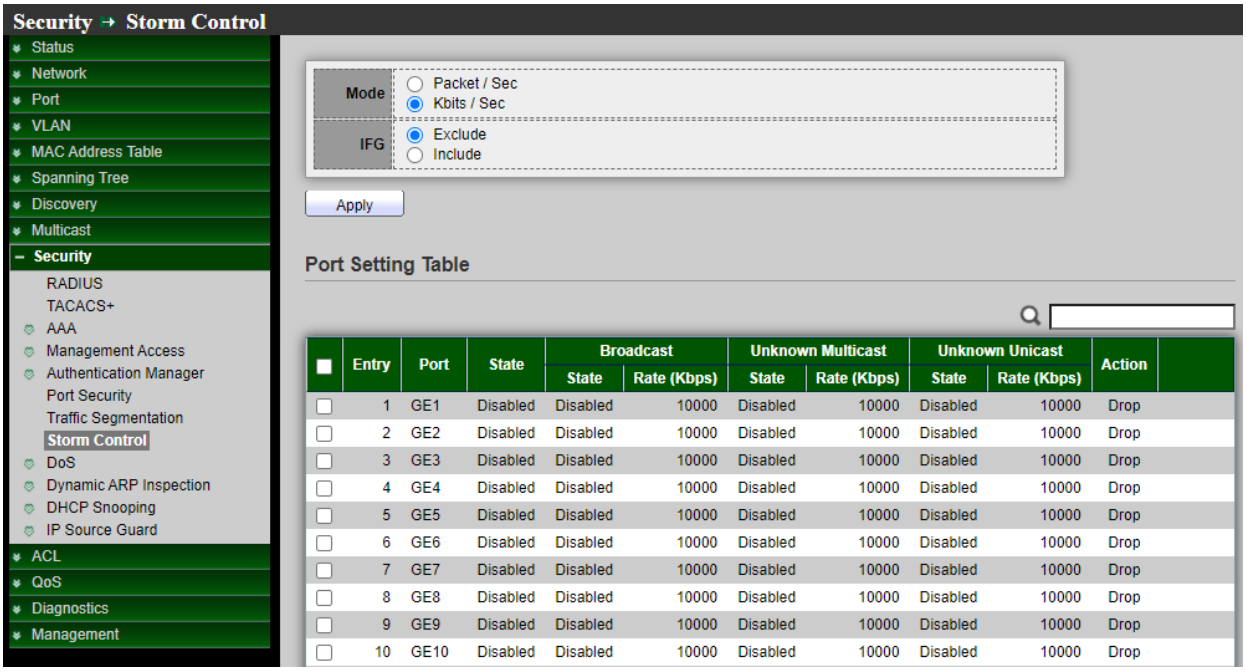


- **Port:** Display selected Port number.
- **State:** Port protected admin state.
  - **Protected:** Enable protecting function.
  - **Unprotected (deselect):** Disable protecting function

*Click the **"Apply"** button to save your changes or "**Close**" the button to close settings.*

10.9 Storm Control

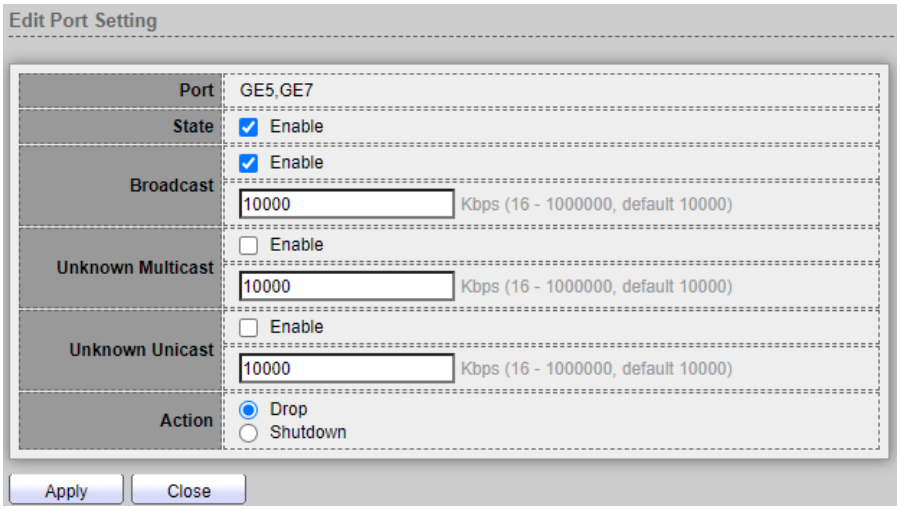
When the rate of Broadcast / unknown Multicast or unknown Unicast frames is higher than the user-defined threshold, this function can to limit the number of frames entering the switch and to define the types of frames that are counted towards this limit. Will be the frames received beyond the threshold are discarded or the interface shuts down.



- **Mode:** Select the unit of storm control.
  - **Packets/sec:** Select by Packets/second of the rate threshold.
  - **Kbits/sec:** Select by Kbits/second of the rate threshold.
- **IFG:** Select the rate calculates w/o preamble & IFG (20 bytes).
  - **Excluded:** exclude preamble & IFG (20 bytes) when count ingress storm control rate.
  - **Include:** include preamble & IFG (20 bytes) when count ingress storm control rate.

*Click the **"Apply"** button to save your changes settings.*

Field	Description
Port	Port name which the host located.
State	Display enable or disable the storm control function.
Broadcast	Show the storm control for the Broadcast packets. • **State:** Display enable or disable the storm control for broadcast packets. • **Rate(Kpps):** Displays the bandwidth threshold for broadcast packets.
Unknown Multicast	Show the storm control for the unknown Multicast packets. • **State:** Display enable or disable the storm control for unknown Multicast packets . • **Rate(Kpps):** Displays the bandwidth threshold for unknown Multicast packets.
Unknown Unicast	Show the storm control for the unknown Unicast packets. • **State:** Display enable or disable the storm control for unknown Unicast packets . • **Rate(Kpps):** Displays the bandwidth threshold for unknown Unicast packets.
Action	• **Drop:** Shows will Broadcast / unknown Multicast or unknown Unicast frames is higher than the user-defined threshold. • **Shutdown:** will Broadcast / unknown Multicast or unknown Unicast frames is higher than the user-defined threshold.



- **Port:** Display selected Port number.
- **State:** Select the state of setting.
  - **Enable:** Enable the storm control function.
- **Broadcast:** If enable storm control for Broadcast traffic will count Broadcast traffic towards the bandwidth threshold.
  - **Enable:** Enable the storm control function of Broadcast packet, Value of storm control rate, Unit: Kbps (Kbits per-second, range16 - 1000000) depends on global mode setting.
- **Unknown Multicast:** If enable storm control for unknown Multicast will count unknown Multicast traffic towards the bandwidth threshold.
  - **Enable:** Enable the storm control function of Unknown Multicast packet, Value of storm control rate, Unit: Kbps (Kbits per-second, range16 - 1000000) depends on global mode setting.
- **Unknown Unicast:** If enable storm control for unknown Unicast will count unknown Unicast traffic towards the bandwidth threshold.
  - **Enable:** Enable the storm control function of Unknown Unicast packet, Value of storm control rate, Unit: Kbps (Kbits per-second, range16 - 1000000) depends on global mode setting.
- **Action:** Administrator can select Drop or Shutdown will Broadcast / unknown Multicast or unknown Unicast frames is higher than the user-defined threshold.
  - **Drop:** Received beyond the threshold will discard the frames, Packets exceed storm control rate will be dropped
  - **Shutdown:** Received beyond the threshold will shut down the port, Port will be shutdown when packets exceed storm control rate.

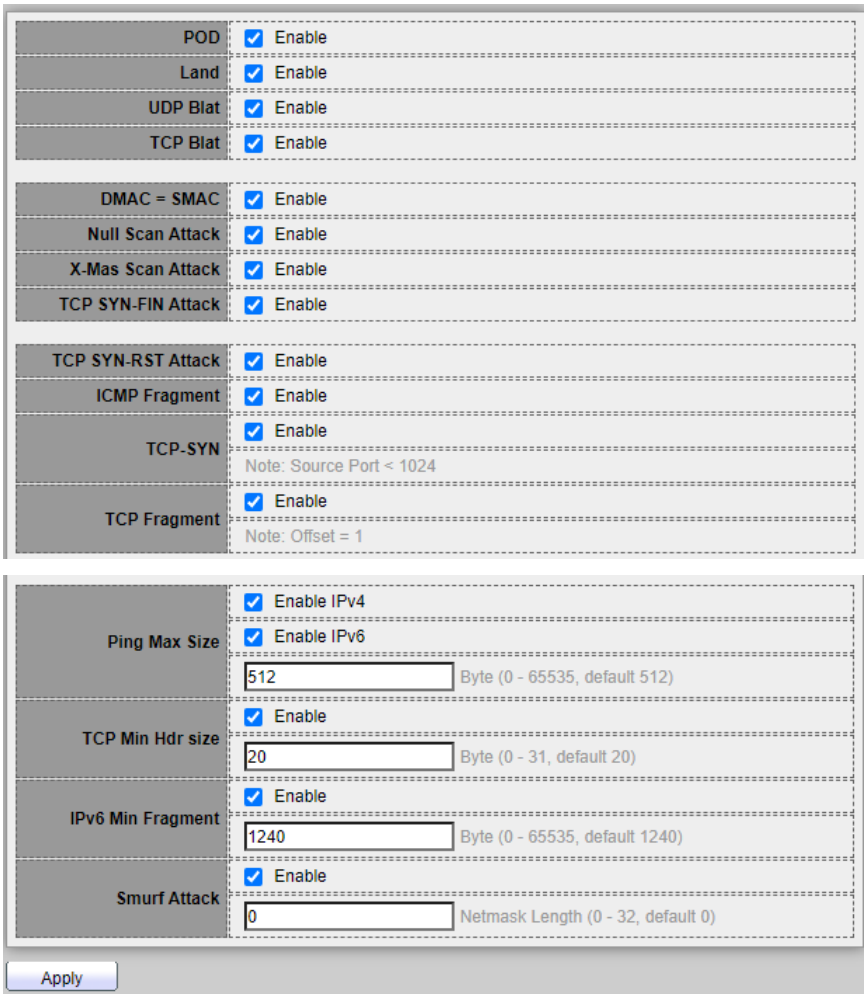
*Click the **"Apply"** button to save your changes or "**Close**" the button to close settings.*

10.10 DoS

DoS attack (denial-of-service) is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

10.10.1 Property

This default is enabled all DoS protection feature and SYN-FIN / SYN-RST protections. The default threshold is 60 SYN packets per second. The default period of port recovery is 60 seconds.



- **POD:**
  - **Enable:** Enable the Dos attack of avoids ping of death attack function.
- **Land:**
  - **Enable:** Enable the Dos attack of drops the packets if the source IP address is equal to the

destination IP address function.

- **UDP Blat:**
  - **Enable:** Enable the Dos attack of drops the packets if the UDP source port equals to the UDP destination port function.
- **TCP Blat:**
  - **Enable:** Enable the Dos attack of drops the packages if the TCP source port is equal to the TCP destination port function.
- **DMAC = SMAC:**
  - **Enable:** Enable the Dos attack of drops the packets if the destination MAC address is equal to the source MAC address function.
- **Null Scan Attach:**
  - **Enable:** Enable the Dos attack of drops the packets with NULL scan function.
- **X-Mas Scan Attack:**
  - **Enable:** Enable the Dos attack of drops the packets if the sequence number is zero, and the FIN, URG and PSH bits are set function.
- **TCP SYN-FIN Attack:**
  - **Enable:** Enable the Dos attack of drops the packets with SYN and FIN bits set function.
- **TCP SYN-RST Attack:**
  - **Enable:** Enable the Dos attack of drops the packets with SYN and RST bits set function.
- **ICMP Flagment:**
  - **Drop:** Enable the Dos attack of drops the fragmented ICMP packets function.
- **TCP- SYN (SPORT<1024):**
  - **Enable:** Enable the Dos attack of drops SYN packets with sport less than 1024 function.
- **TCP Fragment (Offset = 1):**
  - **Enable:** Enable the Dos attack of drops the TCP fragment packets with offset equals to one function.
- **Ping Max Size:**
  - **Enable:** Enable the Dos attack of specify the maximum size of the ICMPv4/ICMPv6 ping packets. The valid range is from 0 to 65535 bytes, and the default value is 512 bytes.
- **IPv4 Ping Max Size:**
  - **Enable:** Enable the Dos attack of checks the maximum size of ICMP ping packets, and drops the packets larger than the maximum packet size function.
- **IPv6 Ping Max Size:**
  - **Enable:** Enable the Dos attack of checks the maximum size of ICMPv6 ping packets, and drops the packets larger than the maximum packet size function.
- **TCP Min Hdr Size:**
  - **Enable:** Enable the Dos attack of checks the minimum TCP header and drops the TCP

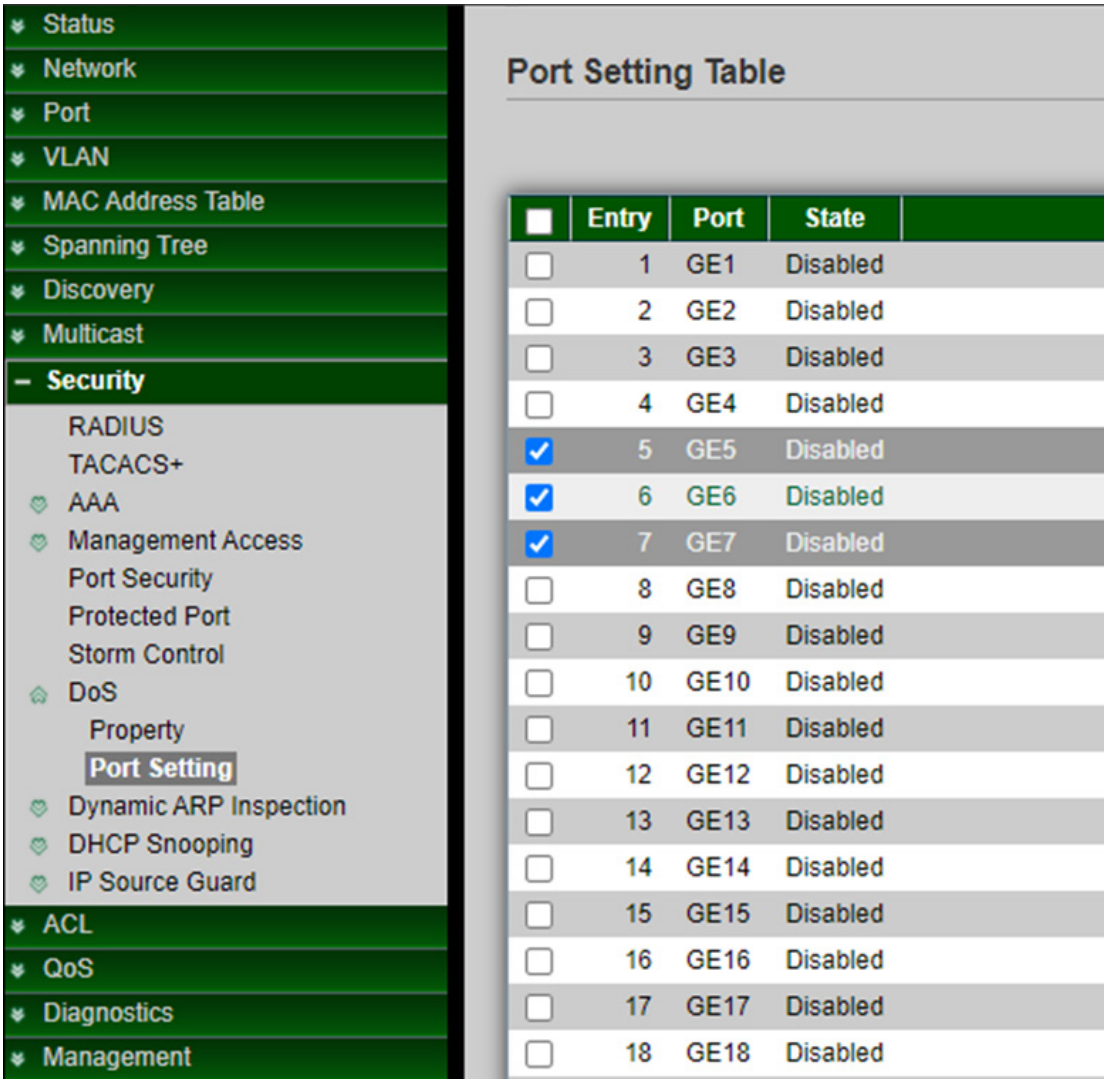
packets with the header smaller than the minimum size. The length range is from 0 to 31 bytes, and default length is 20 bytes function.

- **IPv6 Min Flagment:**
  - **Enable:** Enable the Dos attack of checks the minimum size of IPv6 fragments, and drops the packets smaller than the minimum size. The valid range is from 0 to 65535 bytes, and default value is 1240 bytes function.
- **Smurf Attack:**
  - **Enable:** Enable the Dos attack of avoids smurf attack. The length range of the netmask is from 0 to 323 bytes, and default length is 0 bytes function.

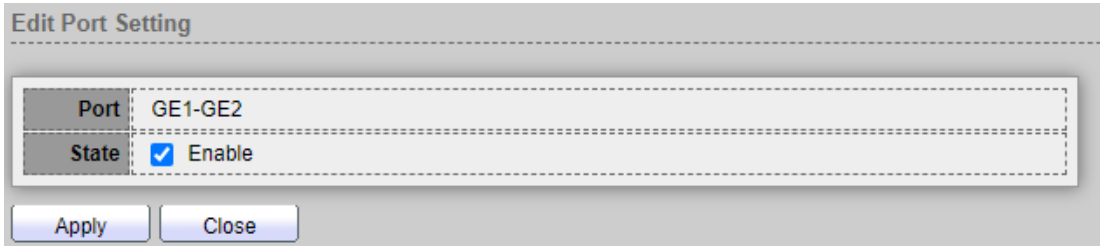
*Click the **"Apply"** button to save your changes settings*

10.10.2 Port Setting

Administrator can choose protected ports.



Field	Description
Port	Interface of port number.
State	Display Enable/Disable the DoS protection on the interface.



- **Port:** Display selected Port number.
- **State:** Select the state of setting.
  - **Enable:** Enable the DoS protection function.

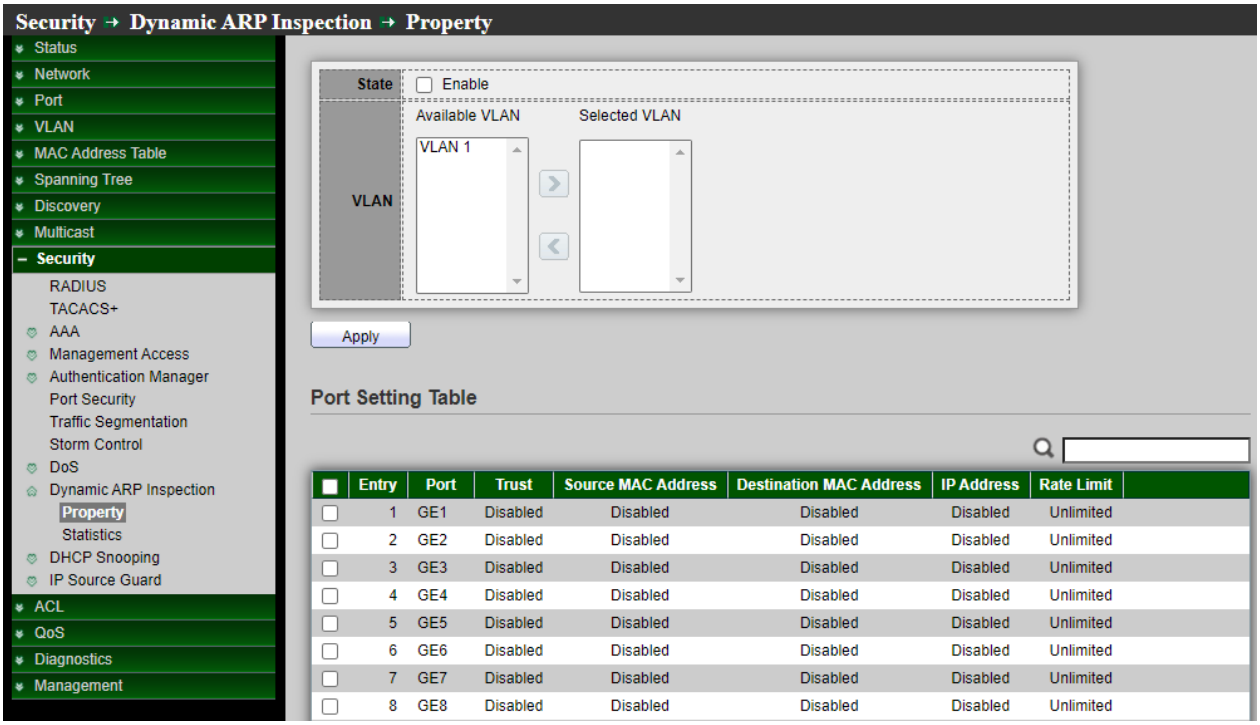
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

10.11 Dynamic ARP Inspection

Dynamic Address Resolution Protocol (ARP) is a TCP/IP protocol for translating IP addresses into MAC addresses. Use the Dynamic ARP Inspection pages to configure settings of Dynamic ARP Inspection.

10.11.1 Property

This page allow user to configure global and per interface settings of Dynamic ARP Inspection.

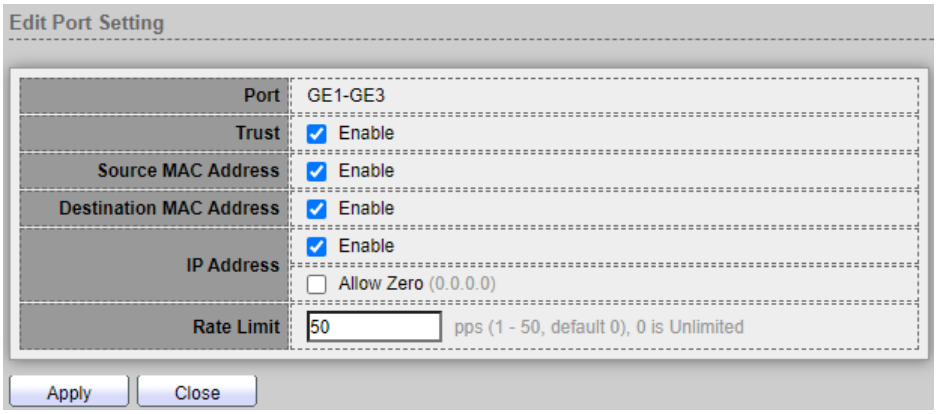


- **State:** Administrator can enable or disable this Dynamic ARP Inspection. Set checkbox to enable/disable Dynamic ARP Inspection function.
- **VLAN:** In the Enabled VLAN table, users assign static ARP Inspection lists to enabled VLANs. When a packet passes through an untrusted interface that is enabled for ARP Inspection switch will performs the checks, Select VLANs in left box then move to right to enable Dynamic ARP Inspection. Or select VLANs in right box then move to left to disable Dynamic ARP Inspection.

*Click the **"Apply"** button to save your changes settings*

Field	Description
Port	Port the port ID.
Trust	Display enable/disabled trust attribute of interface.
Source MAC Address	Display enable/disabled source mac address validation attribute of interface.
Destination MAC Address	Display enable/disabled destination mac address validation attribute of interface.

IP Address	Display enable/disabled IP address validation attribute of interface, Allow zero which means allow 0.0.0.0 IP address.
Rate Limit	Display rate limitation value of interface.

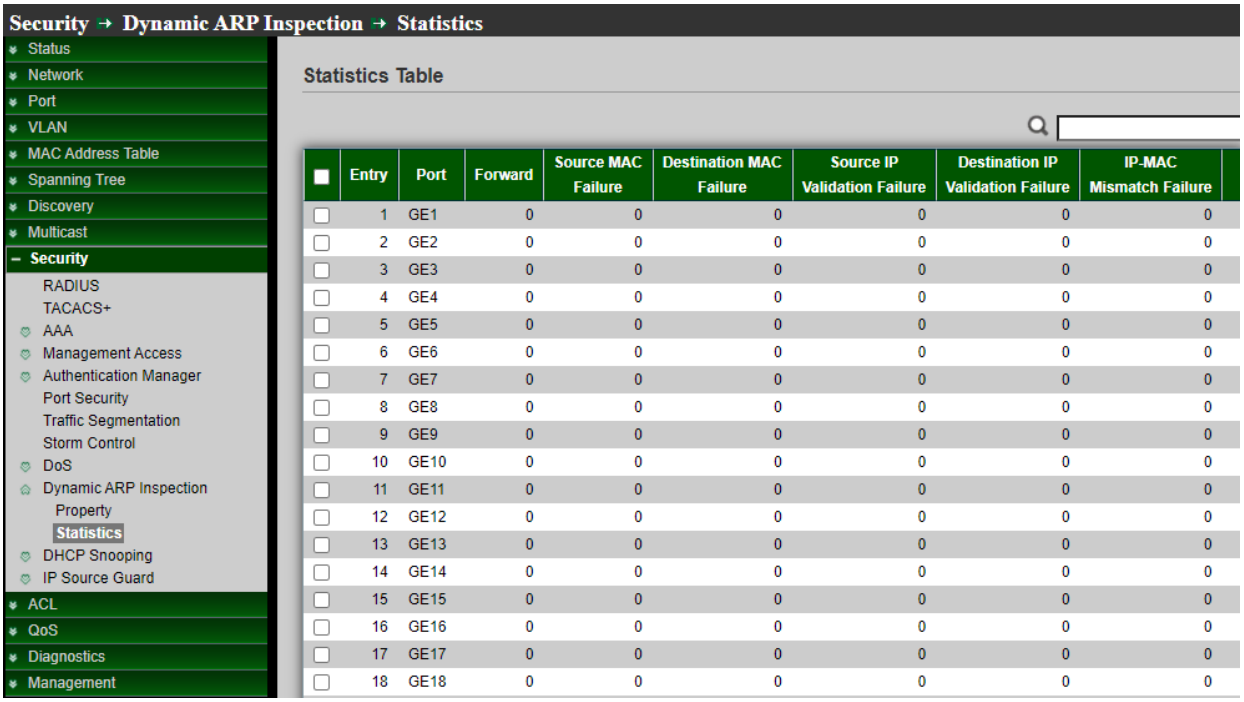


- **Port:** Display selected Port number.
- **Trust:** If enabled, the port or LAG is a trusted interface, and ARP inspection is not performed on the ARP requests or replies sent to or from the interface. If Un-Enable, the port or LAG is not a trusted interface, and ARP inspection is performed on the ARP requests or replies sent to or from the interface. By default, it is disabled.
- **Source MAC Address:** Check Enable to validate the source MAC addresses in ARP requests and replies, Set checkbox to enable or disable source mac address validation of interface. All ARP packets will be checked whether sender mac is same as source mac in Ethernet header if enable source mac address validation. Default is disabled.
- **Destination MAC Address:** Check Enable to validate the destination MAC addresses in ARP replies, Set checkbox to enable or disable destination mac address validation of interface. All ARP packets will be checked whether target mac is same as destination mac in Ethernet header if enable destination mac address validation. Default is disabled.
- **IP Address:** Set checkbox to enable or disable IP address validation of interface. All ARP packets will be checked whether IP address is 0.0.0.0,255.255.255.255 or multicast address. Default is disabled.
  - **Allow all-zeros IP:** If IP address validation is enabled, check Enable to allow 0.0.0.0 the IP address.
- **Rate Limit:** Enter the maximum rate that is allowed on the interface. The range is 1 to 50pps and the default is 0 Unlimited.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

10.11.2 Statistics

The Statistics page will displays the statistical information for ARP Inspection.



Entry	Port	Forward	Source MAC Failure	Destination MAC Failure	Source IP Validation Failure	Destination IP Validation Failure	IP-MAC Mismatch Failure
1	GE1	0	0	0	0	0	0
2	GE2	0	0	0	0	0	0
3	GE3	0	0	0	0	0	0
4	GE4	0	0	0	0	0	0
5	GE5	0	0	0	0	0	0
6	GE6	0	0	0	0	0	0
7	GE7	0	0	0	0	0	0
8	GE8	0	0	0	0	0	0
9	GE9	0	0	0	0	0	0
10	GE10	0	0	0	0	0	0
11	GE11	0	0	0	0	0	0
12	GE12	0	0	0	0	0	0
13	GE13	0	0	0	0	0	0
14	GE14	0	0	0	0	0	0
15	GE15	0	0	0	0	0	0
16	GE16	0	0	0	0	0	0
17	GE17	0	0	0	0	0	0
18	GE18	0	0	0	0	0	0

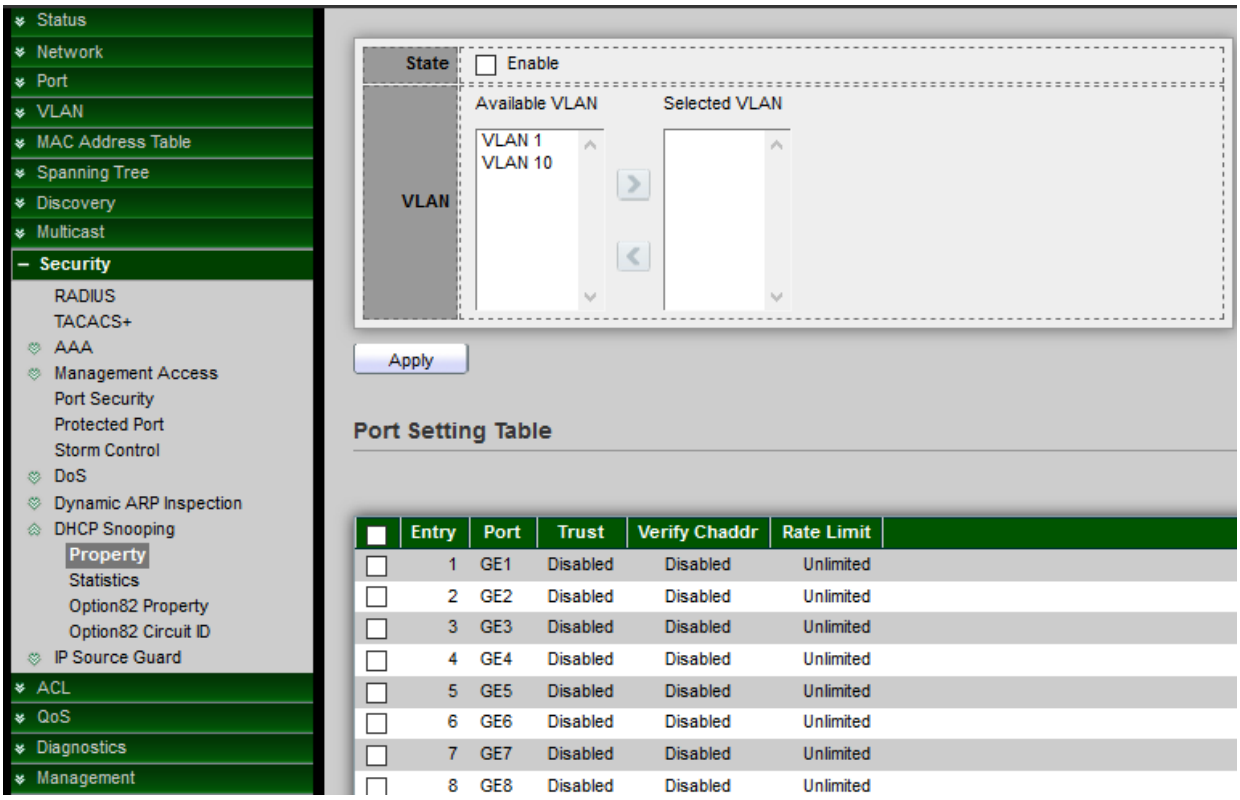
Field	Description
Port	Interface of port number.
Forward	Display how many packets forwarded normally.
Source MAC Failure	Display how many packets dropped by source MAC validation.
Destination MAC Failure	Display how many packets dropped by destination MAC validation.
Source IP Address Validation Failures	Display how many packets dropped by source IP validation.
Destination IP Address Validation Failures	Display how many packets dropped by destination IP validation.
IP-MAC Mismatch Failures	Display how many packets dropped by IP-MAC doesn't match in IP Source Guard binding table.

10.12 DHCP Snooping

Administrator can use DHCP snooping to help avoid the Denial of Service attacks that result from unauthorized users adding a DHCP server to the network that then provides invalid configuration data to other DHCP clients on the network. DHCP packets received on other switch ports are inspected before being forwarded. Packets from untrusted sources are dropped.

10.12.1 Property

This page allow user to configure global and per interface settings of DHCP Snooping.

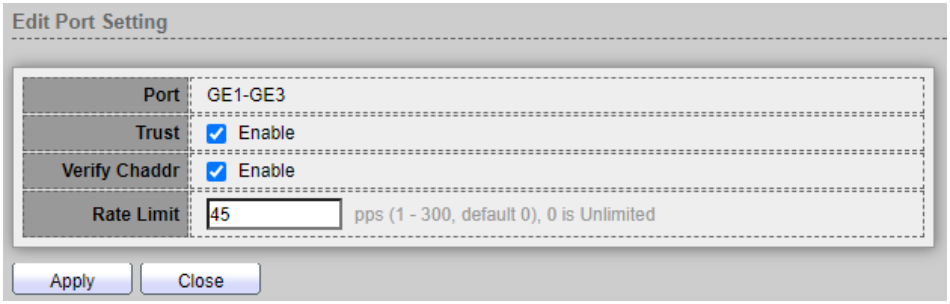


- **State:** Administrator can enable or Un-Enable DHCP Snooping, Set checkbox to enable/disable DHCP Snooping function.
- **VLAN:** Administrator can to enable DHCP Snooping on a VLAN, ensure that DHCP Snooping is globally enabled on the switch, Select VLANs in left box then move to right to enable DHCP Snooping. Or select VLANs in right box then move to left to disable DHCP Snooping.

*Click the **"Apply"** button to save your changes settings.*

Field	Description
Port	Interface of port number.

Trust	Display enable/disabled trust attribute of interface.
Verify Chaddr	Display enable/disabled chaddr validation attribute of interface.
Rate Limit	Display rate limitation value of interface.

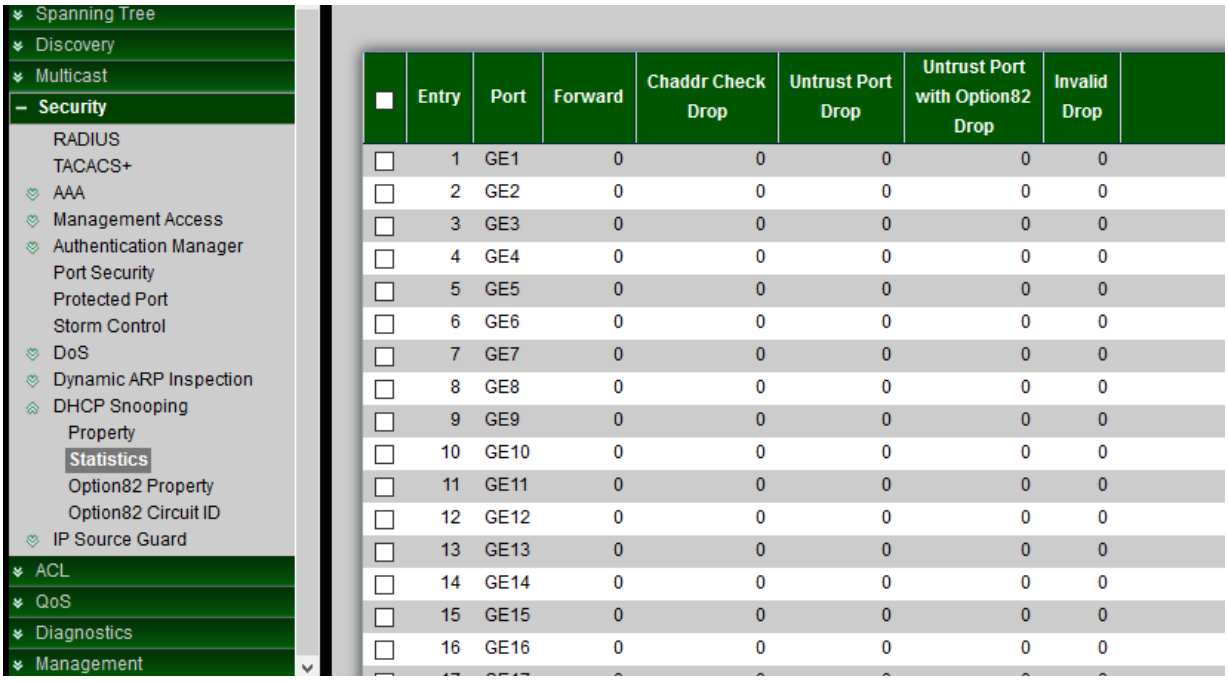


- **Port:** Display selected Port number.
- **Trust:** If check Enable will connected to a DHCP server or to other switches or routers as trusted ports, Set checkbox to enable/disabled trust of interface. All DHCP packet will be forward directly if enable trust. Default is disabled
- **Verify Chaddr:** Set checkbox to enable or disable chaddr validation of interface. All DHCP packets will be checked whether client hardware mac address is same as source mac in Ethernet header if enable chaddr validation. Default is disabled.
- **Rate Limit:** Enter the maximum rate that is allowed on the interface. The range is 1 to 300pps and the default is 0 Unlimited.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

10.12.2 Statistics

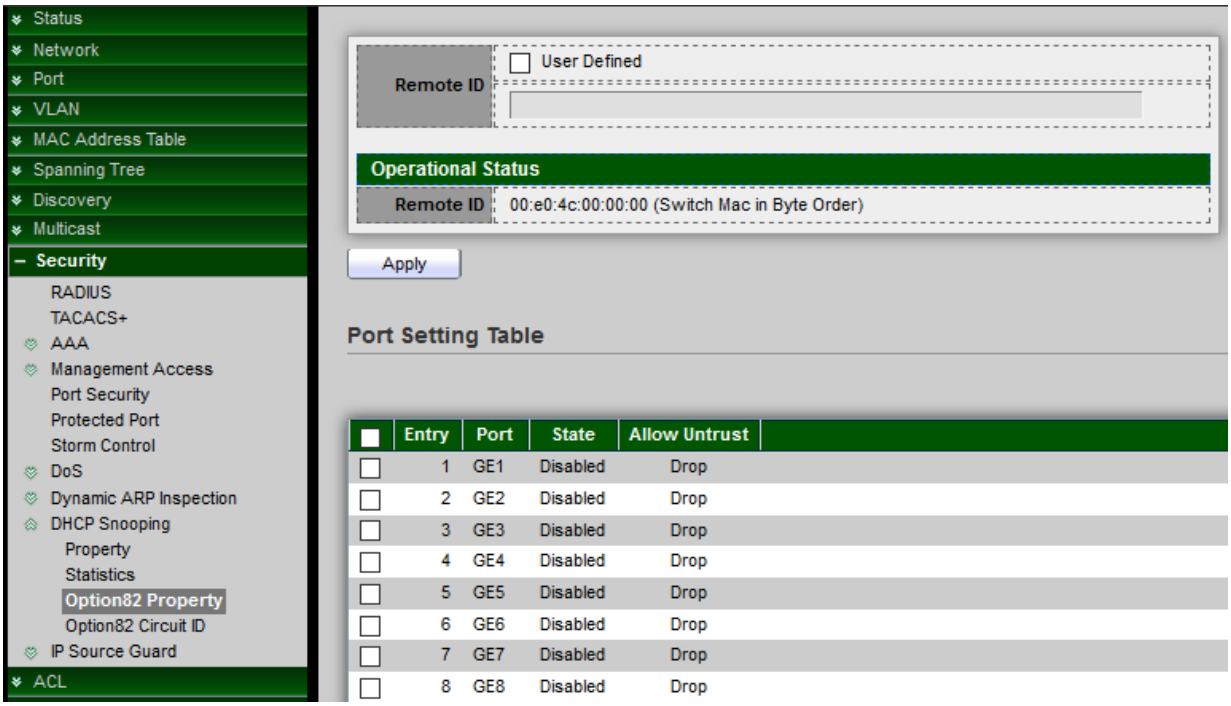
This page allow user to browse all statistics that recorded by DHCP snooping function.



Field	Description
Port	Interface of port number.
Forward	Display how many packets forwarded normally.
Chaddr Check Drop	Display how many packets dropped by chaddr validation.
Untrusted Port Drop	Display how many DHCP server packets that are received by untrusted port dropped.
Untrusted Port with Option82 Drop	Display how many packets dropped by untrusted port with option82 checking.
Invalid Drop	Display how many packets dropped by invalid checking.

10.12.3 Option82 Property

This page allow user to set string of DHCP option82 remote ID filed. The string will attach in option82 if option inserted.



- **Remote ID:** If Option 82 is enabled, select User Defined to manually enter the format remote ID, Set checkbox to enable user-defined remote-ID. By default, remote ID is switch mac in byte order.
  Input user-defined remote ID. Only available when enable user-define remote ID.

Field	Description
Operational Status	Display remote ID information.

*Click the **"Apply"** button to save your changes settings.*

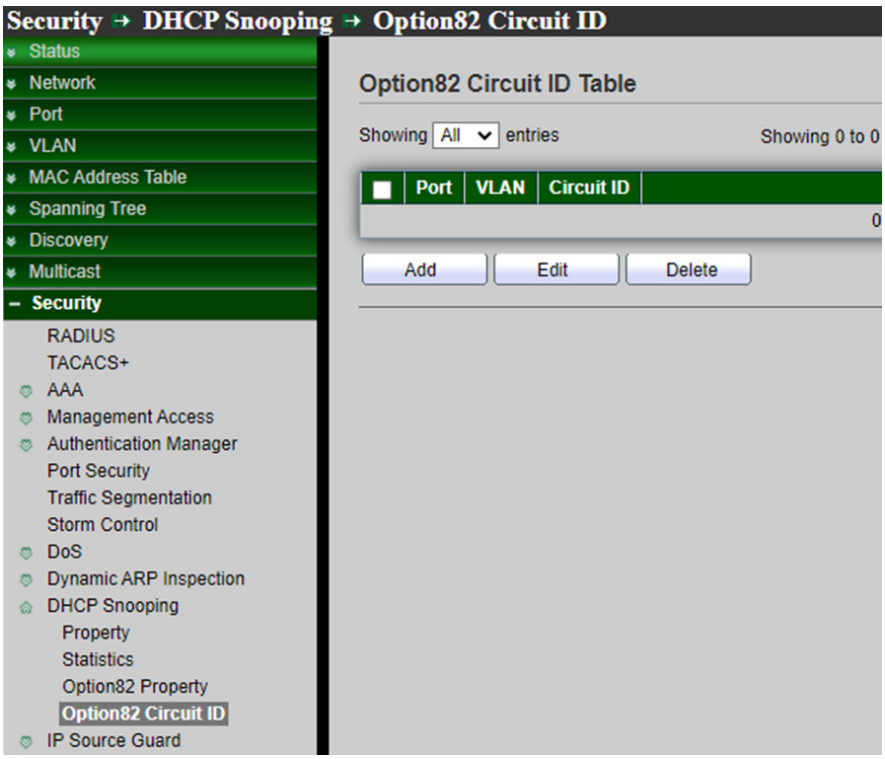
Field	Description
Port	Interface of port number.
State	Set checkbox to enable/disable option82 function of interface.
Allow untrusted	Display allow untrusted action of interface.

- **Port:** Display selected Port number.
- **State:** Check Enable or Un-Enable, Display option82 enable/disable status of interface.
- **Allow untrusted:** Select the action perform when untrusted port receive DHCP packet has option82 filed. Default is drop.
  - **Keep:** Keep original option82 content.
  - **Drop:** Drop packets with option82.
  - **Replace:** Replace option82 content by switch setting.

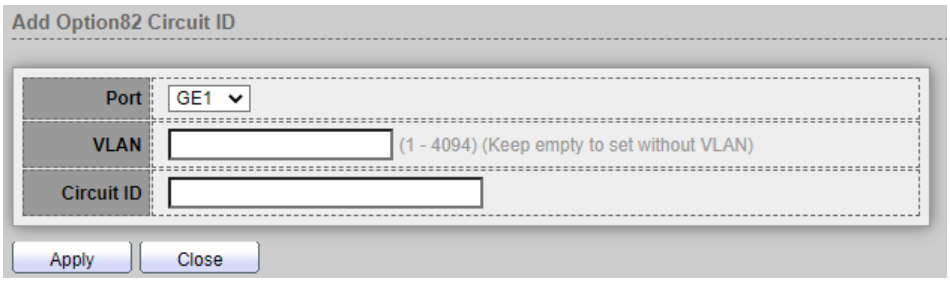
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

10.12.4 Option82 Circuit ID

Administrator can use the Option82 Port CID Settings page to configure the Option 82 circuit-ID Setting **"add"** and "Edit" and **"Delete"** function management, This page allow user to set string of DHCP option82 circuit ID filed. The string will attach in option82 if option inserted.



Field	Description
Port	Display port ID of entry.
VLAN	Display associate VLAN of entry.
Circuit ID	Display circuit ID string of entry.



- **Port:** Select port from list to associate to CID entry. Only available on Add dialog.
- **VLAN:** Input VLAN ID to associate to circuit ID entry. VLAN ID is not mandatory. Only available on Add dialog.
- **Dircuit ID:** Input String as circuit ID. Packets match port and VLAN will be inserted circuit ID.

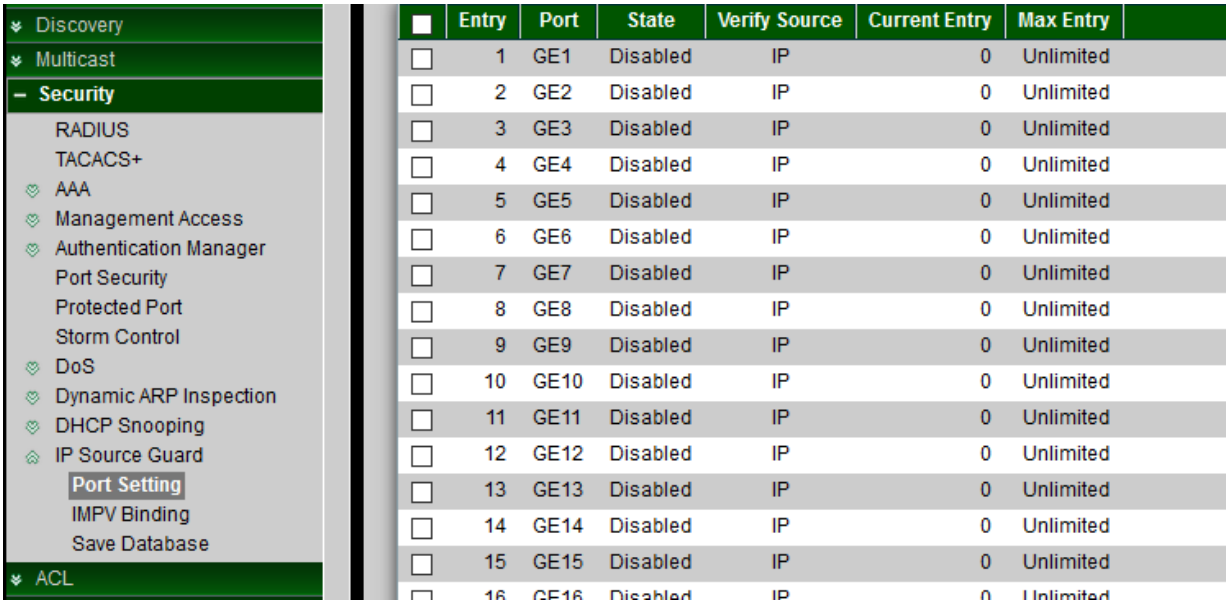
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

10.13 IP Source Guard

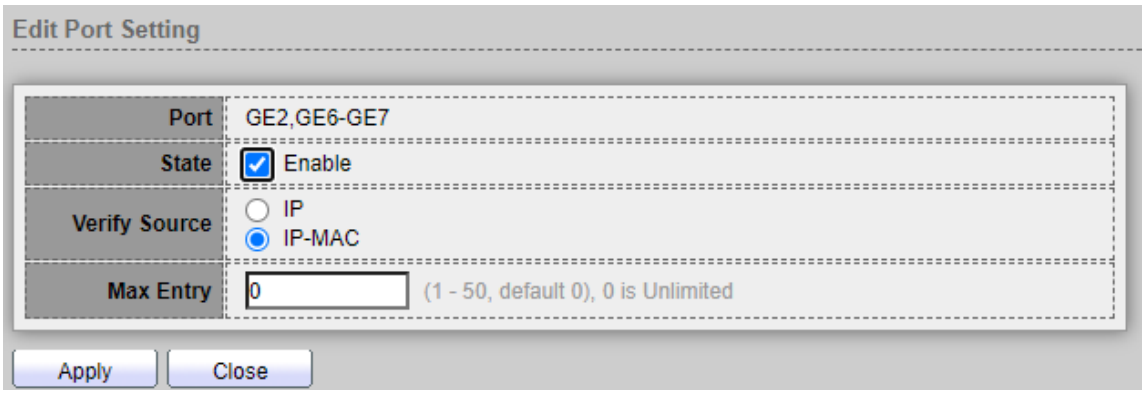
IP Source Guard restricts the client IP traffic to those source IP addresses configured in the IP Source binding database, mainly can prevent traffic attacks caused when a host tries to use the IP address of its neighbor.

10.13.1 Port Setting

This page allow user to configure per port settings of IP Source Guard.



Field	Description
Port	Interface of port number.
State	Display IP Source Guard enable/disable status of interface.
Verify Source	Display mode of IP Source Guard verification.
Current Binding Entry	Display current binding entries of a interface.
Max Binding Entry	Display the number of maximum binding entry of interface.



- **Port:** Display selected Port number.
- **State:** Check Enable or Un-Enable this IP Source Guard. Mainly restricts the client IP traffic to those source IP addresses configured Check Enable to enable IP Source Guard on the

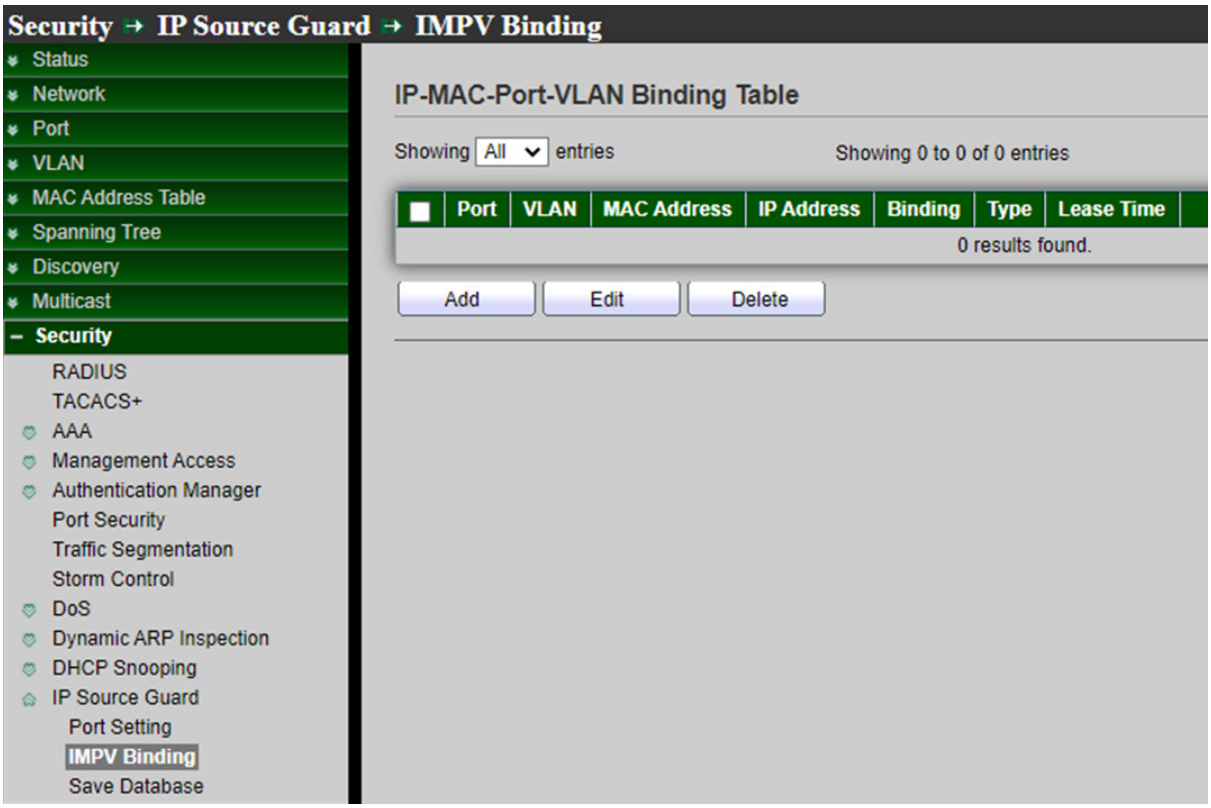
interface. Administrator can disable this feature, Default is disabled.

- **Verify Source:** Administrator can select IP only or MAC and IP type of source traffic to be verified.
  - **IP:** Only verify source IP address of packet.
  - **IP-MAC:** Verify source IP and source MAC address of packet
- **Max Entry:** Administrator need enter the maximum number of IP source binding rules. The range is 0 to 50, and 0 is Unlimited.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

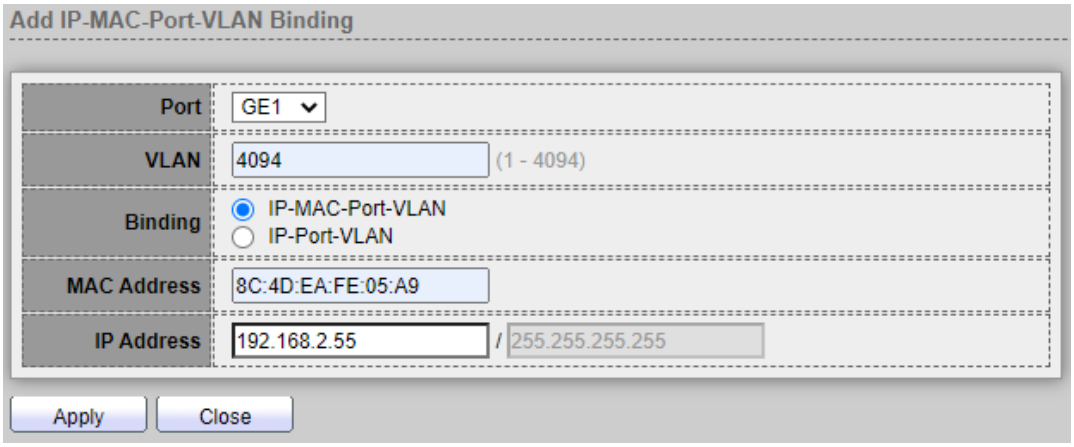
10.13.2 IMPV Binding

Use the Binding to query and view information about inactive addresses recorded in the IP Source Guard database, This page allow user to add static IP source guard entry and browse all IP source guard entries that learned by DHCP snooping or statically create by user, Setting **"add"** and "Edit" and **"Delete"** for this function management.



Field	Description
Port	Display port ID of entry.

VLAN	Display VLAN ID of entry.
MAC Address	Display MAC address of entry. Only available of IP-MAC binding entry.
IP Address	Display IP address of entry. Mask always to be 255.255.255.255 for IP-MAC binding. IP binding entry display user input
Binding	Display binding type of entry.
Status	Type of existing binding entry: • **Static :** Entry added by user manually configured. • **Dynamic :** Entry learned by DHCP snooping.
Lease Time	Lease time of DHCP Snooping learned entry. After lease time entry will be deleted. Only available of dynamic entry.

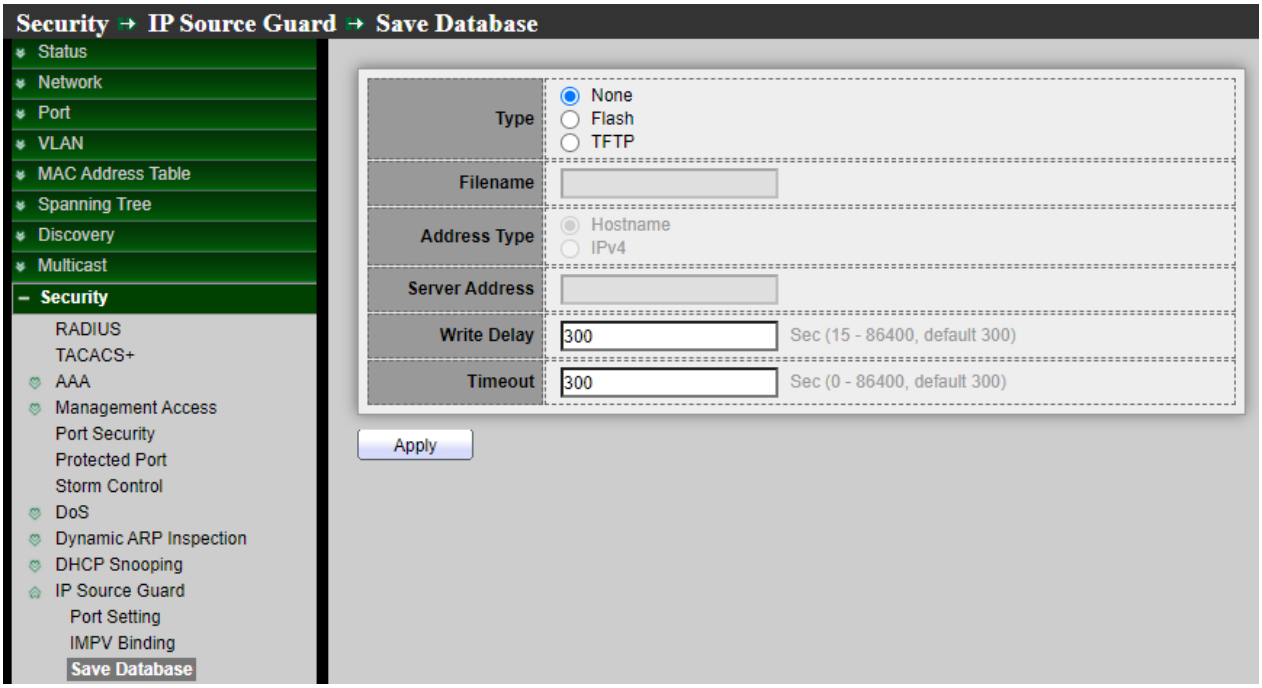


- **Port:** Administrator can select port from list of a binding entry.
- **VLAN:** Specify a VLAN ID of a binding entry.
- **Binding:** Administrator can select matching mode of binding entry.
  - **IP-MAC-Port-VLAN:** packet must match IP address 、 MAC address、Port and VLAN ID.
  - **IP-Port-VLAN:** packet must match IP address or subnet 、Port and VLAN ID.
- **MAC Address:** Input MAC address. Only available on IP-MAC-Port-VLAN mode.
- **IP Address:** Input IP address and mask. Mask only available on IP-MAC-Port mode.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

10.13.3 Save Databases

This page allow user to configure DHCP snooping database which can backup and restore dynamic DHCP snooping entries



- **Type:** Administrator can select the type of database agent.
  - **None:** Disable database agent service.
  - **Flash:** Save DHCP dynamic binding entries to flash.
  - **TFTP:** Save DHCP dynamic binding entries to remote TFTP server.
- **Filename:** Set file name of TFTP server, Input filename for backup file. Only available when selecting type “flash” and “TFTP”.
- **Address Type:** Select use Host name or IP address to connection TFTP server.
  - **Hostname:** TFTP server address is hostname.
  - **IPv4:** TFTP server address is IPv4 address.
- **Server Address:** Input remote TFTP server hostname or IP address. Only availablewhen selecting type “TFTP.
- **Write Delay:** Input delay timer for doing backup after change happened. Default is 300 seconds.
- **Timeout:** Input aborts timeout for doing backup failure. Default is 300 seconds.

*Click the **“Apply”** button to save your changes settings.*

11. ACL

ACL (Access Control List) is an ordered list of classification filters and actions. Each single classification rule, together with its action, is called an Access Control Element (ACE). Each ACE is made up of filters that distinguish traffic groups and associated actions. A single ACL may contain one or more ACEs, which are matched against the contents of incoming frames. Either a DENY or PERMIT action is applied to frames whose contents match the filter.

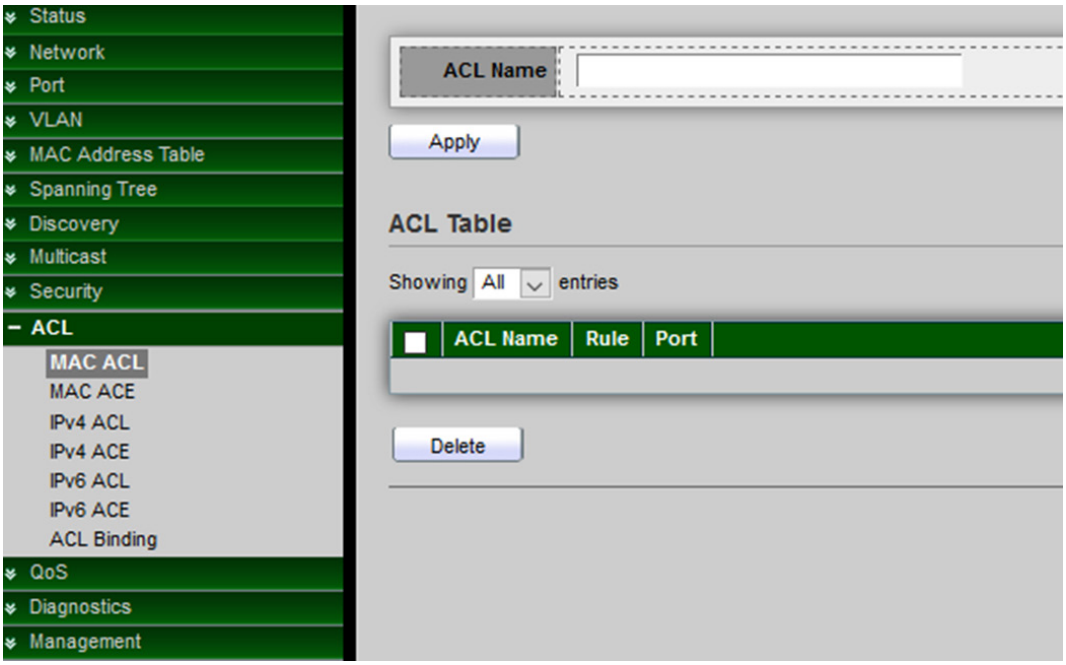
Note	When a packet matches an ACE filter, the ACE action is taken and that ACL processing is stopped. If the packet does not match the ACE filter, the next ACE is processed. If all ACEs of an ACL have been processed without finding a match, and if another ACL exists, it is processed in a similar manner. If no match is found to any ACE in all relevant ACLs then ACL default action will dropped the packet.

11.1 MAC ACL

This page mainly creates MAC ACLs profile. The MAC ACLs are used to filter traffic based on Layer 2 fields and defined on the MAC ACE page.

This page allow user to add or delete ACL rule. A rule cannot be deleted if under binding.

Note	A port can be either secured with ACLs or configured with advanced QoS policy, but not both.



- **ACL Name:** Create a name of ACL.

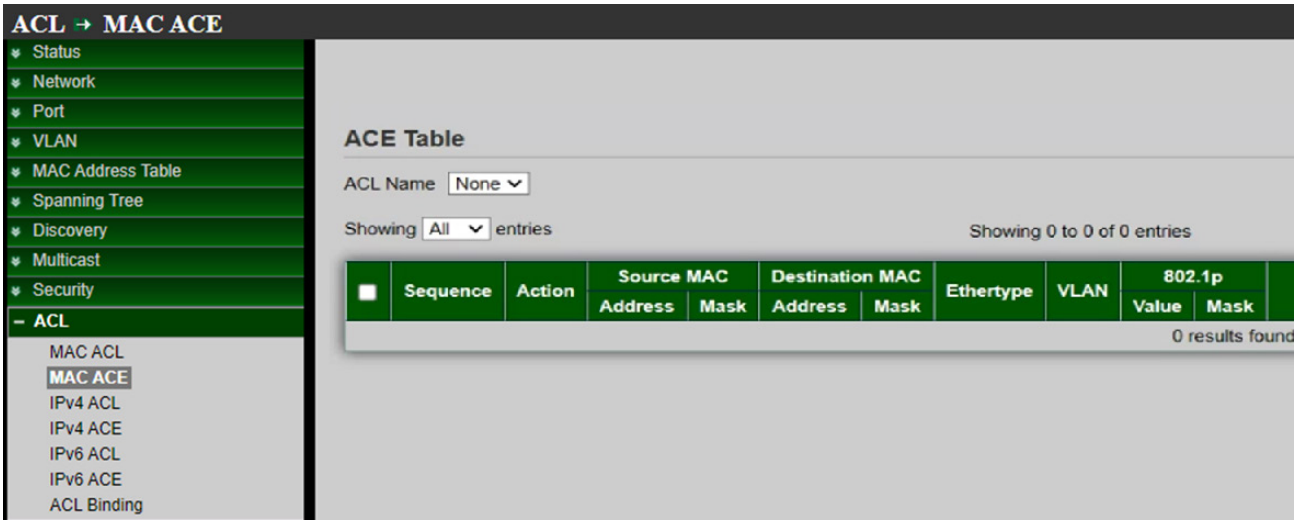
*Click the **"Apply"** button to save your changes settings.*

Field	Description
ACL Name	Display MAC ACL name.
Rule	Display the number ACE rule of ACL..
Port	L Display the port list that bind this ACL.

*Click the **"Delete"** button to delete ACL table list.*

11.2 MAC ACE

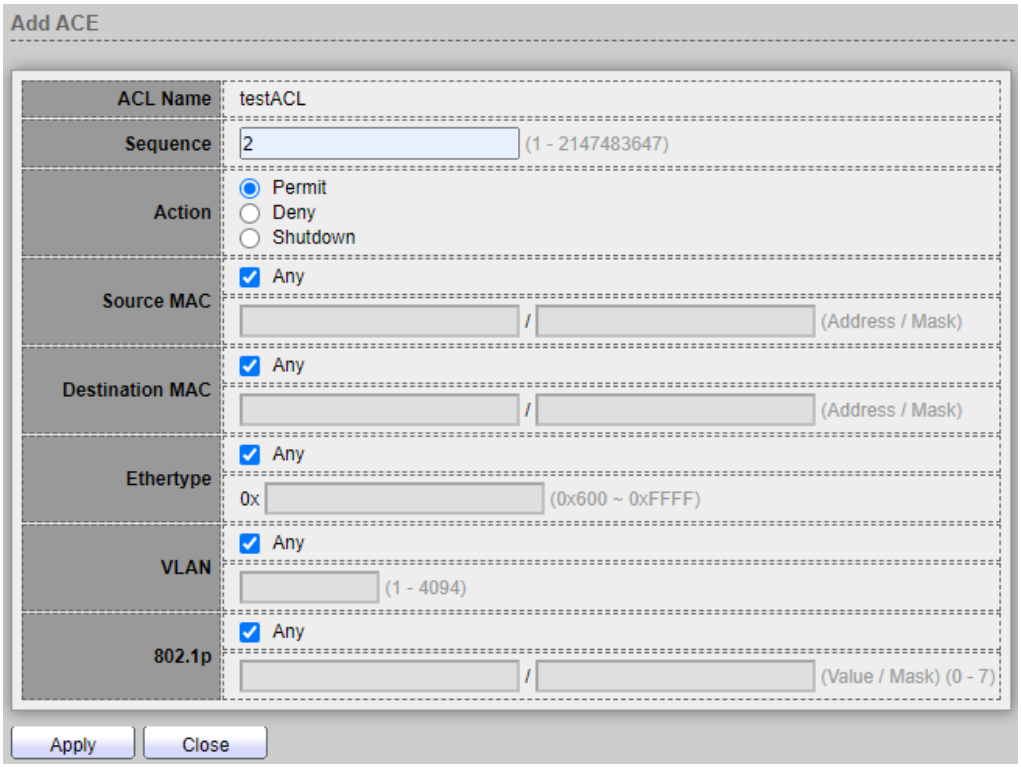
MAC ACE will check all frames for a match. Setting **"add"** and "Edit" and **"Delete"** for this function management, This page allow user to add, edit or delete ACE rule. An ACE rule cannot be edited or deleted if ACL under binding. New ACE cannot be added if ACL under binding .



- **ACL Name:** Select the ACL name to which an ACE is being added.

Field	Description
Sequence	Display the sequence of ACE.
Action	Display the action of ACE
Source MAC	Display the source MAC address and mask of ACE.

Destination MAC	Display the destination MAC address and mask of ACE.
Ethertype	Display the Ethernet frame type of ACE.
VLAN ID	Display the VLAN ID of ACE
802.1p Value	Display the 802.1p value of ACE.
802.1p Mask	Display the 802.1p mask of ACE.



- **ACL Name:** Display the ACL name to which an ACE is being added.
- **Sequence:** ACEs with higher sequence are processed first (1 is the highest priority). Only available on Add Dialog.
- **Action:** Administrator can select the action after ACE match packet.
  - **Permit:** Forward packets that meet the ACE criteria.
  - **Deny:** Drop packets that meet the ACE criteria.
  - **Shutdown:** Drop packets that meet the ACE criteria, and disable the port from where the packets were received. Such ports can be reactivated from the Port Settings page.
- **Source MAC:** Select the type for source MAC address.
  - **Any:** All source addresses are acceptable.
  - **User Defined:** Only a source address or a range of source addresses which users define are

acceptable. Enter the source MAC address and mask to which will be matched.

- **Destination MAC:** Destination MAC Select the type for Destination MAC address.
  - **Any:** All destination addresses are acceptable.
  - **User Defined:** Only a destination address or a range of destination addresses which users define are acceptable. Enter the destination MAC address and mask to which will be matched.

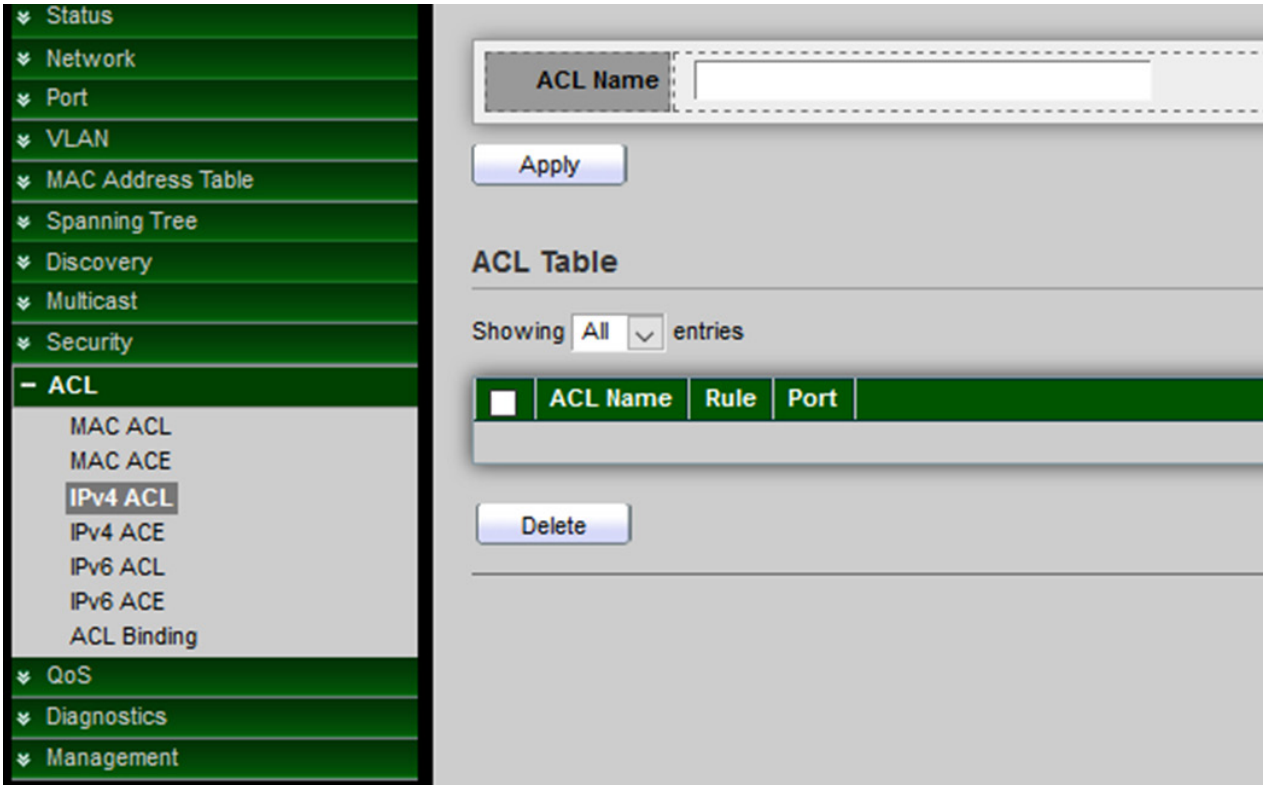
Note	Set F is show value, 0 is mask value, E.g. If an MAC is 8C:4D:EA:11:22:33 the mask value FF:FF:FF:00:00:00 indicates that only the first three bytes of the destination MAC address are used(8C:4D:EA).

- **Ethertype:** Select the type for Ethernet frame type.
  - **Any:** All Ethernet frame type is acceptable.
  - **User Defined:** Only an Ethernet frame type which users define is acceptable. Enter the Ethernet frame type value to which will be matched.
- **VLAN ID:** Select the type for VLAN ID.
  - **Any:** All VLAN ID is acceptable.
  - **User Defined:** User Defined: Only a VLAN ID which users define is acceptable. Enter the VLAN ID to which will be matched.
- **802.1p:** Select the type for 802.1p value.
  - **Any:** All 802.1p value is acceptable.
  - **User Defined:** User Defined: Only an 802.1p value or a range of 802.1p value which users define is acceptable. Enter the 802.1p value and mask to which will be matched.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

11.3 IPv4 ACL

Mainly creates IPv4 ACLs profile. The IPv4 ACLs are used to check IPv4 packets, This page allow user to add or delete Ipv4 ACL rule. A rule cannot be deleted if under binding.



- **ACL Name:** Create a name of ACL.

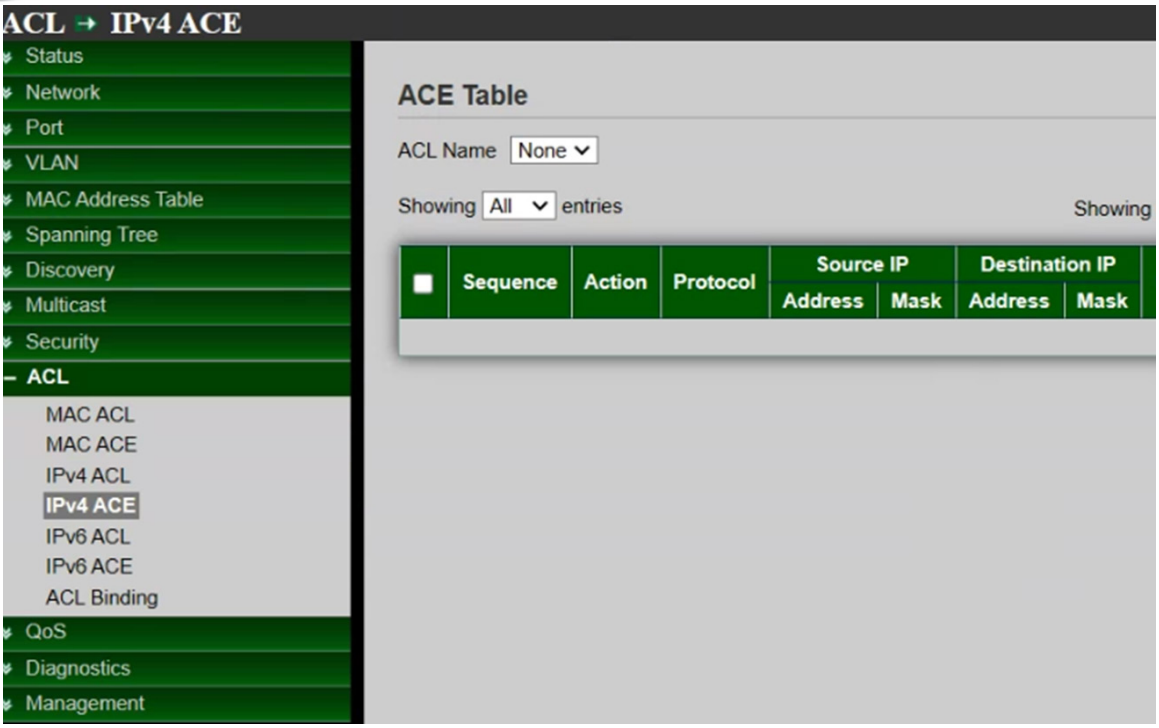
*Click the **"Apply"** button to save your changes settings.*

Field	Description
ACL Name	Display IPv4 ACL name
Rule	Display the number ACE rule of ACL
Port	Display the port list that bind this ACL

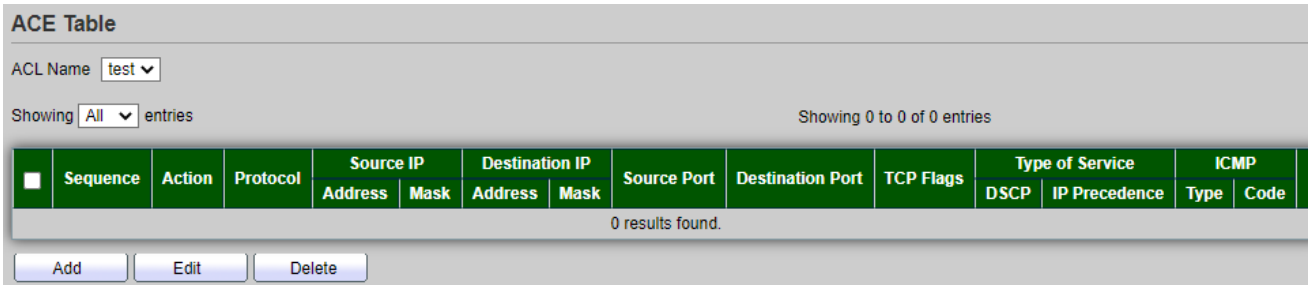
*Click the **"Delete"** button to delete the table list.*

11.4 IPv4 ACE

This page allow user to add, edit or delete ACE rule. An ACE rule cannot be edited or deleted if ACL under binding. New ACE cannot be added if ACL under binding, Setting **"add"** and "Edit" and **"Delete"** for this function management.

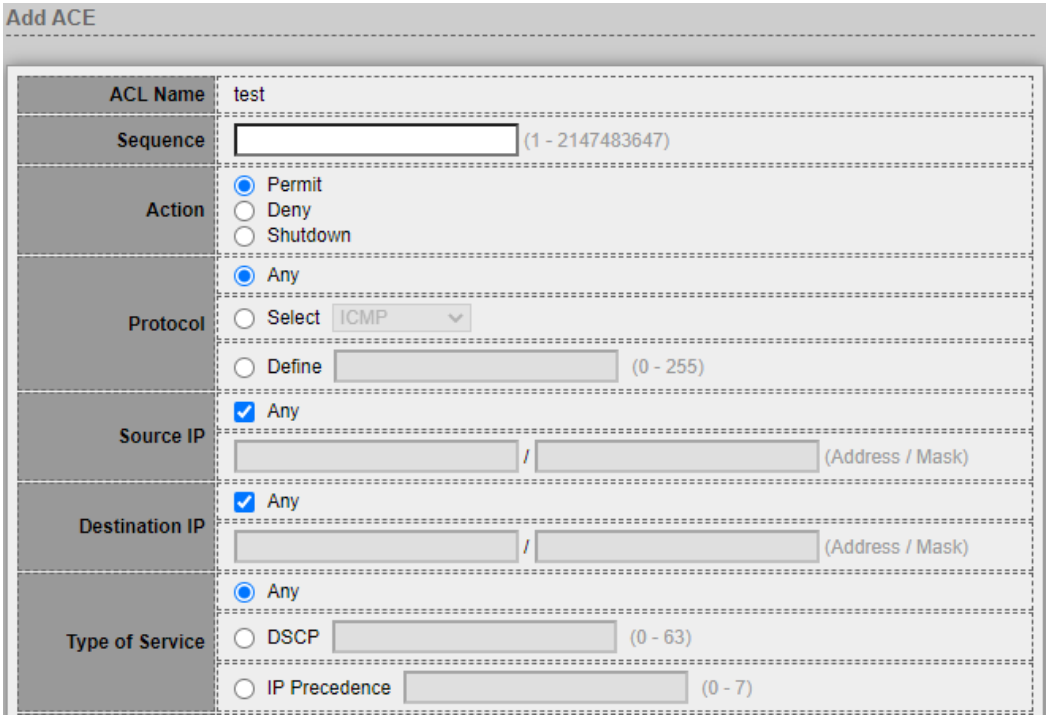


➢ **ACL Name:** Select the ACL name to which an ACE is being added.



Field	Description
Sequence	Display the sequence of ACE.
Action	Display the action of ACE.
Protocol	Display the protocol value of ACE.
Source IP	Display the source IP address and mask of ACE: • **Address:** Display for the IPv4 IP address. • **Mask :** Display for the Mask address.
Destination IP	Display the destination IP address and mask of ACE: • **Address:** Display for the IPv4 IP address. • **Mask :** Display for the Mask address.
Source Port	Display single source port or a range of source ports of ACE. Only available

	when protocol is TCP or UDP.
Destination Port	Display single destination port or a range of destination ports of ACE. Only available when protocol is TCP or UDP.
TCP Flags	Display the TCP flag value if ACE. Only available when protocol is TCP.
Type of Service	Display the ToS value of ACE which could be DSCP or IP Precedence.
ICMP	Display the ICMP type and code of ACE. Only available when protocol is ICMP.



- **ACL Name:** Display the ACL name to which an ACE is being added.
- **Sequence:** Specify the sequence of the ACE ,ACEs with higher sequence are processed first (1 is the highest priority). Only available on Add Dialog.
- **Action:** Administrator can select the action for a match.
  - **Permit:** Forward packets that meet the ACE criteria.
  - **Deny:** Drop packets that meet the ACE criteria.
  - **Shutdown:** Drop packets that meet the ACE criteria, and disable the port from where the packets were received. Such ports can be reactivated from the Port Settings page.
- **Protocol:** Administrator can select the type of protocol for a match.

- **Any (IP):** All IP protocols are acceptable.
- **Select from list:** Select one of the following protocols from the drop-down list. (ICMP/IPinIP/TCP/EGP/IGP/UDP/HMP/RDP/IPV6/IPV6:ROUT/IPV6:FRAG/ RSVP/IPV6:ICMP/OSPF/PIM/L2TP)
- **Protocol ID to match:** Enter the protocol ID.

➢ **Source IP:** Select the type for source IP address.

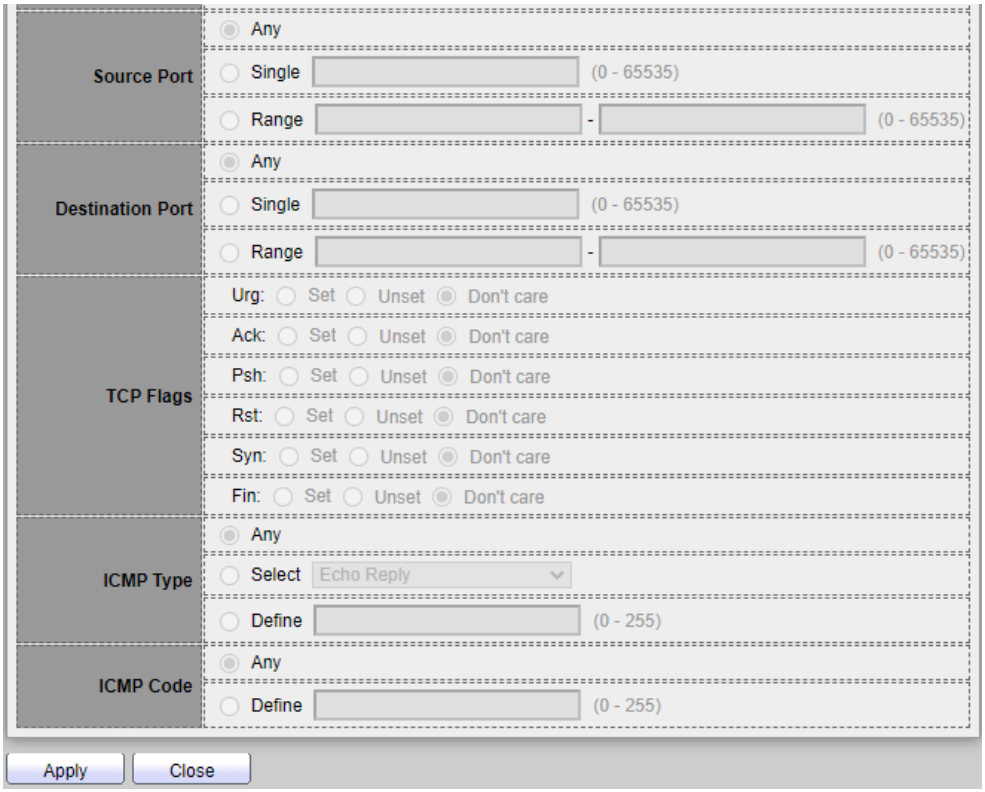
- **Any:** All source addresses are acceptable.
- **User Defined:** Only a source address or a range of source addresses which users define are acceptable. Enter the source IP address value and mask to which will be matched.

➢ **Destination IP:** Select the type for destination IP address..

- **Any:** All destination addresses are acceptable.
- **User Defined:** Only a destination address or a range of destination addresses which users define are acceptable. Enter the destination IP address value and mask to which will be matched.

➢ **Type of Service:** Select the type of service for a match.

- **Any:** All types of service are acceptable.
- **DSCP to match:** Enter a Differentiated Serves Code Point (DSCP) to match.
- **IP Precedence to match:** Enter a IP Precedence to match.



➢ **Source Port:** Select the type of protocol for a match. Only available when protocol is TCP or UDP.

- **Any:** All source ports are acceptable.
- **Single:** Enter a single TCP/UDP source port to which packets are matched.
- **Range:** Select a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.

➢ **Destination Port:** Select the type of protocol for a match. Only available when protocol is TCP or UDP.

- **Any:** All source ports are acceptable.
- **Single:** Enter a single TCP/UDP source port to which packets are matched.
- **Range:** Select a range of TCP/UDP destination ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.

➢ **TCP Flags:** Select one or more TCP flags with which to filter packets. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. Only available when protocol is TCP.

- **Set:** Match if the flag is SET.
- **Unset:** Match if the flag is Not SET.
- **Don't care:** Ignore the TCP flag.

➢ **ICMP Type:** Either select the message type by name or enter the message type number. Only available when protocol is ICMP.

- **Any:** All message types are acceptable.
- **Select from list:** Select message type by name.
- **Protocol ID to match:** Enter the number of message type.

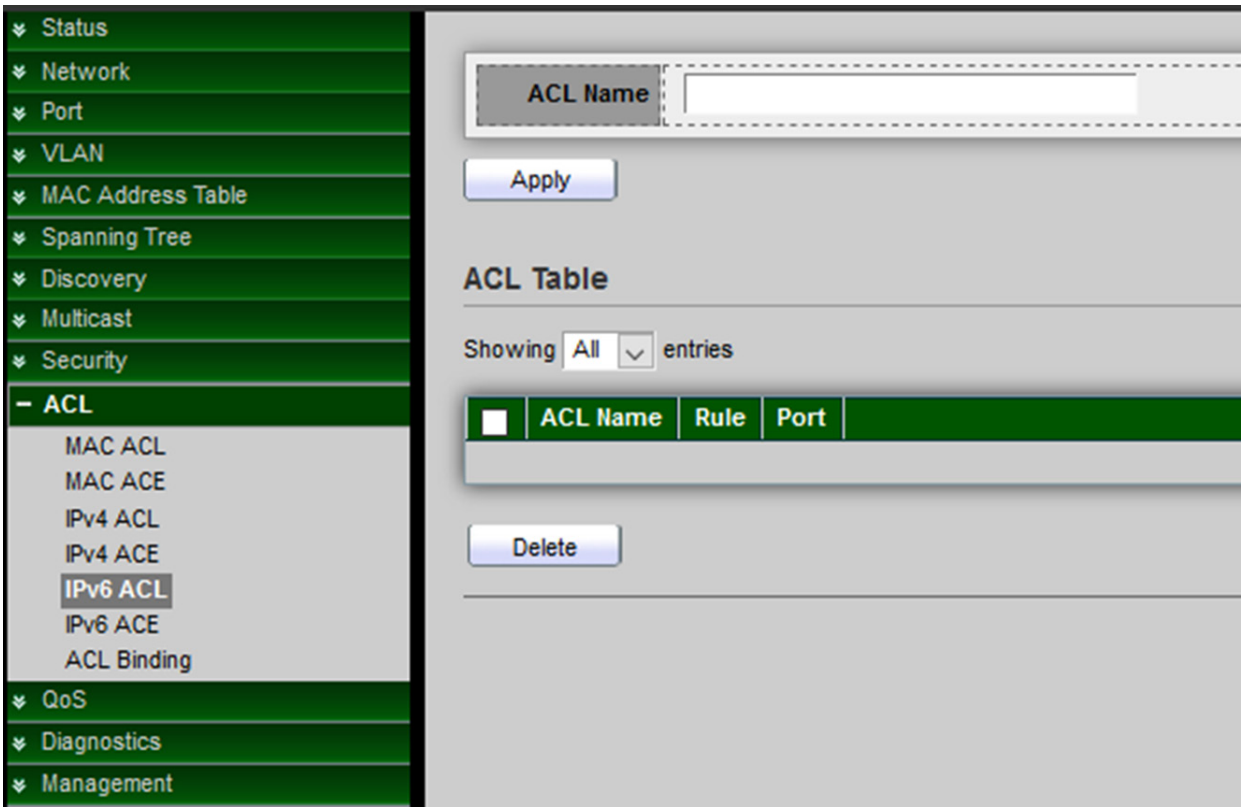
➢ **ICMP Code:** Select the type for ICMP code. Only available when protocol is ICMP.

- **Any:** All codes are acceptable.
- **User Defined:** Enter an ICMP code to match.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

11.5 IPv6 ACL

Mainly creates IPv6 ACLs profile. The IPv6 ACLs are used to check IPv6 packets, This page allow user to add or delete Ipv6 ACL rule. A rule cannot be deleted if under binding.



- **ACL Name:** Create a name of ACL.

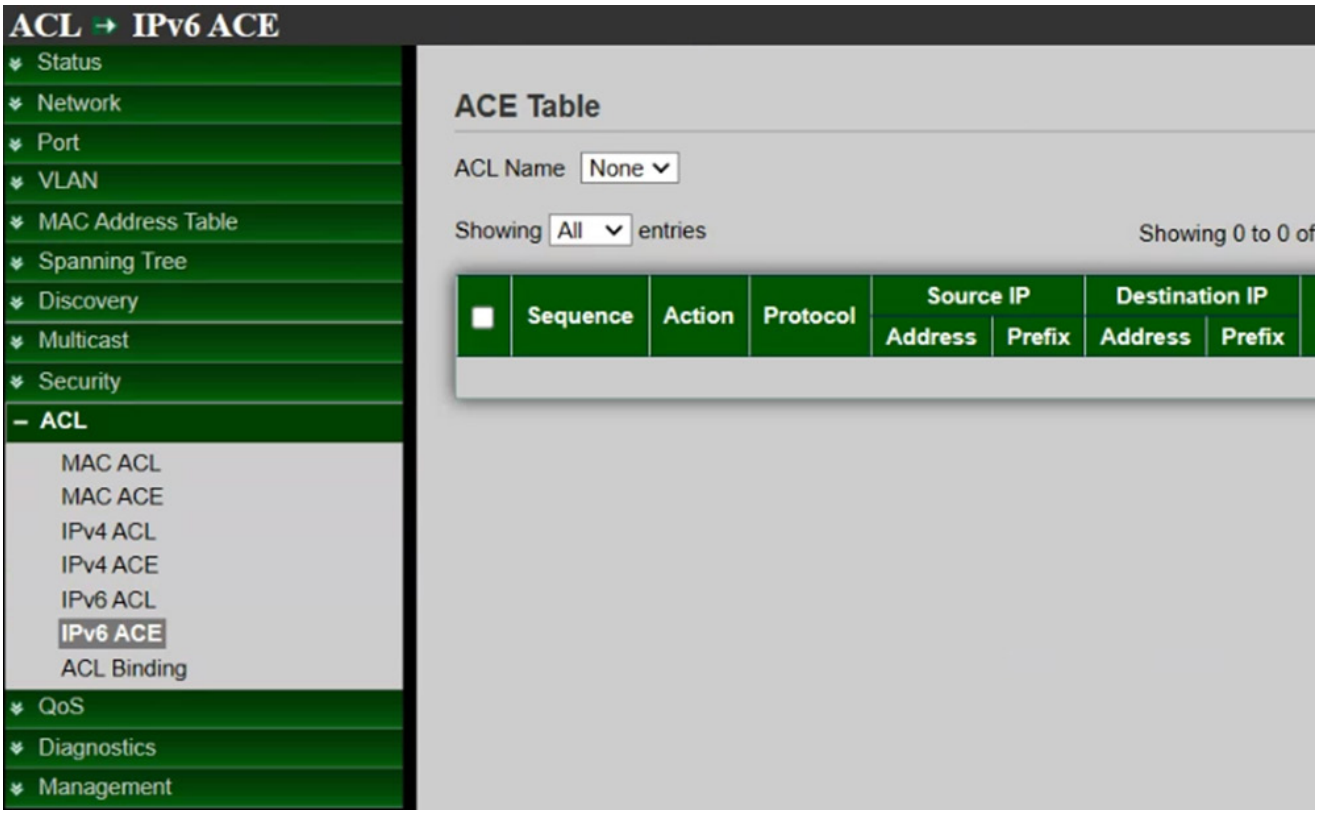
*Click the **"Apply"** button to save your changes settings.*

Field	Description
ACL Name	Display IPv6 ACL name
Rule	Display the number ACE rule of ACL
Port	Display the port list that bind this ACL

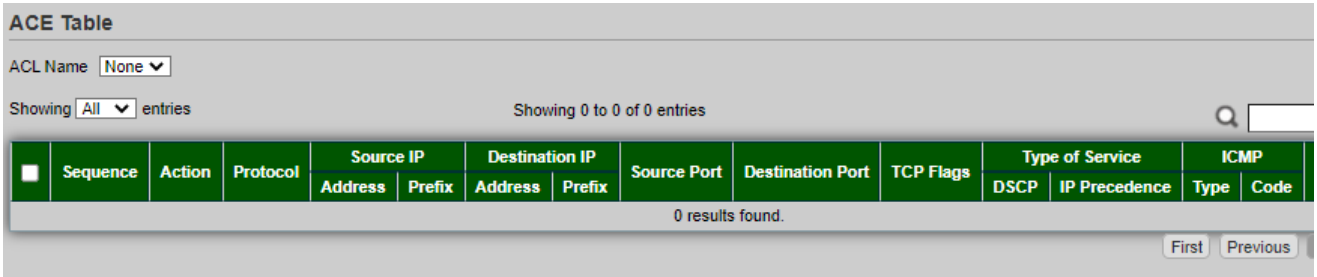
*Click the **"Delete"** button to delete the table list.*

11.6 IPv6 ACE

This page allow user to add, edit or delete ACE rule. An ACE rule cannot be edited or deleted if ACL under binding. New ACE cannot be added if ACL under binding, Setting **"add"** and "Edit" and **"Delete"** for this function management.

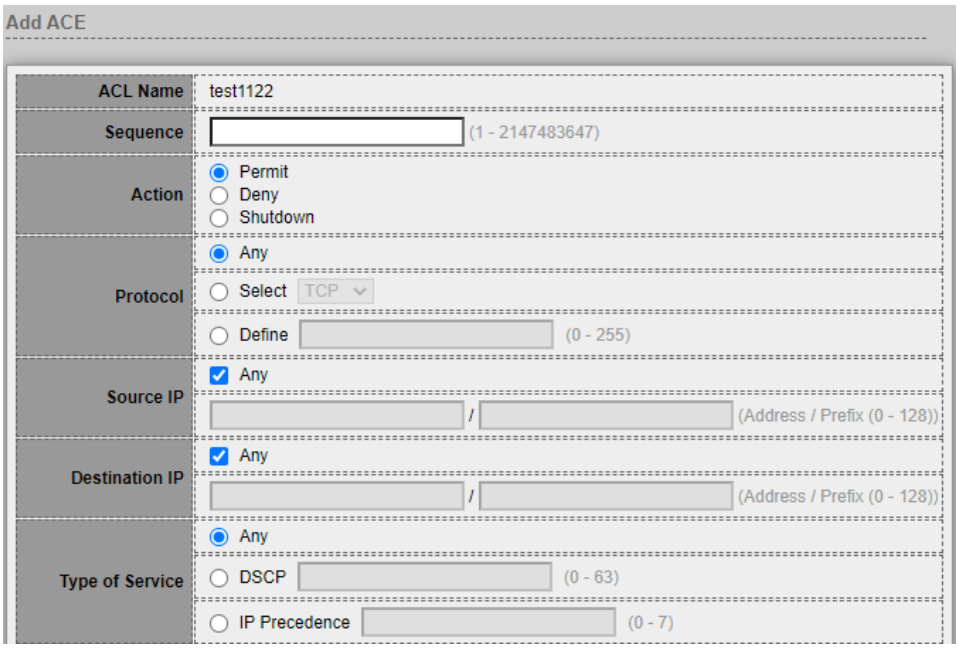


➢ **ACL Name:** Select the ACL name to which an ACE is being added.



Field	Description
Sequence	Display the sequence of ACE.
Action	Display the action of ACE.
Protocol	Display the protocol value of ACE.
Source IP	Display the source IP address and mask of ACE: • **Address:** Display for the IPv4 IP address.

	• **Mask :** Display for the Mask address.
Destination IP	Display the destination IP address and mask of ACE: • **Address:** Display for the IPv4 IP address. • **Mask :** Display for the Mask address.
Source Port	Display single source port or a range of source ports of ACE. Only available when protocol is TCP or UDP.
Destination Port	Display single destination port or a range of destination ports of ACE. Only available when protocol is TCP or UDP.
TCP Flags	Display the TCP flag value if ACE. Only available when protocol is TCP.
Type of Service	Display the ToS value of ACE which could be DSCP or IP Precedence.
ICMP	Display the ICMP type and code of ACE. Only available when protocol is ICMP.



- **ACL Name:** Display the ACL name to which an ACE is being added.
- **Sequence:** Specify the sequence of the ACE ,ACEs with higher sequence are processed first (1 is the highest priority). Only available on Add Dialog.
- **Action:** Administrator can select the action for a match.
  - **Permit:** Forward packets that meet the ACE criteria.

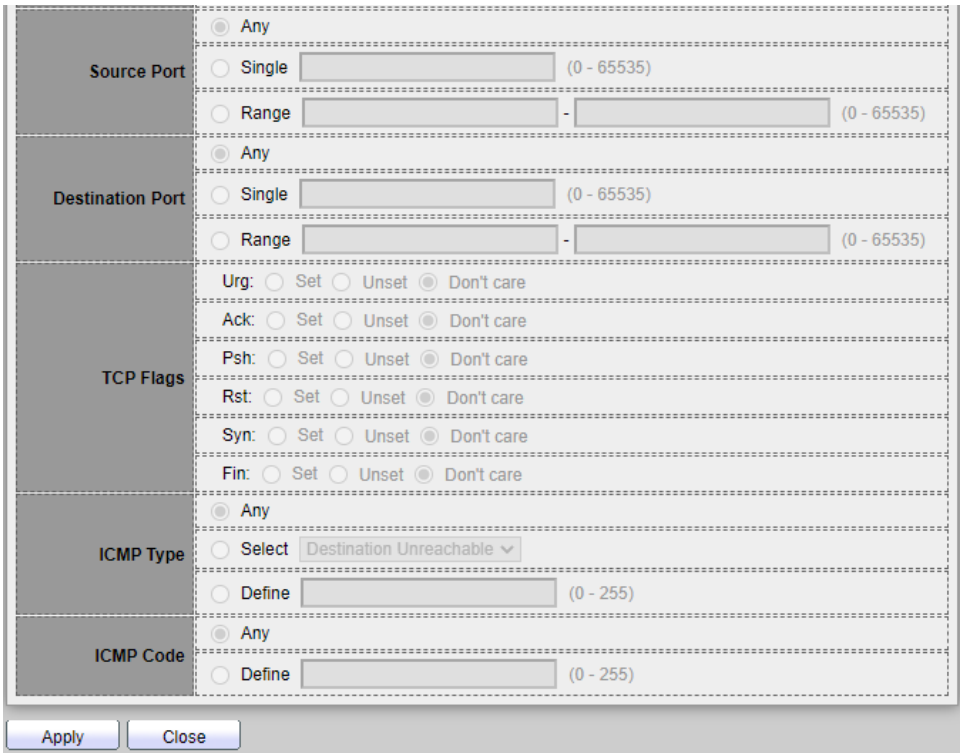
- **Deny:** Drop packets that meet the ACE criteria.
- **Shutdown:** Drop packets that meet the ACE criteria, and disable the port from where the packets were received. Such ports can be reactivated from the Port Settings page.

➢ **Protocol:** Administrator can select the type of protocol for a match.
- **Any (IP):** All IP protocols are acceptable.
- **Select from list:** Select one of the following protocols from the drop-down list. (ICMP/IPinIP/TCP/EGP/IGP/UDP/HMP/RDP/IPV6/IPV6:ROUT/IPV6:FRAG/ RSVP/IPV6:ICMP/OSPF/PIM/L2TP)
- **Protocol ID to match:** Enter the protocol ID.

➢ **Source IP:** Select the type for source IP address.
- **Any:** All source addresses are acceptable.
- **User Defined:** Only a source address or a range of source addresses which users define are acceptable. Enter the source IP address value and mask to which will be matched.

➢ **Destination IP:** Select the type for destination IP address..
- **Any:** All destination addresses are acceptable.
- **User Defined:** Only a destination address or a range of destination addresses which users define are acceptable. Enter the destination IP address value and prefix to which will be matched.

➢ **Type of Service:** Select the type of service for a match.
- **Any:** All types of service are acceptable.
- **DSCP to match:** Enter a Differentiated Serves Code Point (DSCP) to match.
- **IP Precedence to match:** Enter a IP Precedence to match.



- **Source Port:** Select the type of protocol for a match. Only available when protocol is TCP or UDP.
  - **Any:** All source ports are acceptable.
  - **Single:** Enter a single TCP/UDP source port to which packets are matched.
  - **Range:** Select a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
- **Destination Port:** Select the type of protocol for a match. Only available when protocol is TCP or UDP.
  - **Any:** All source ports are acceptable.
  - **Single:** Enter a single TCP/UDP source port to which packets are matched.
  - **Range:** Select a range of TCP/UDP destination ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
- **TCP Flags:** Select one or more TCP flags with which to filter packets. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. Only available when protocol is TCP.
  - **Set:** Match if the flag is SET.
  - **Unset:** Match if the flag is Not SET.
  - **Don't care:** Ignore the TCP flag.
- **ICMP Type:** Either select the message type by name or enter the message type number. Only available when protocol is ICMP.

- **Any:** All message types are acceptable.
- **Select from list:** Select message type by name.
- **Protocol ID to match:** Enter the number of message type.

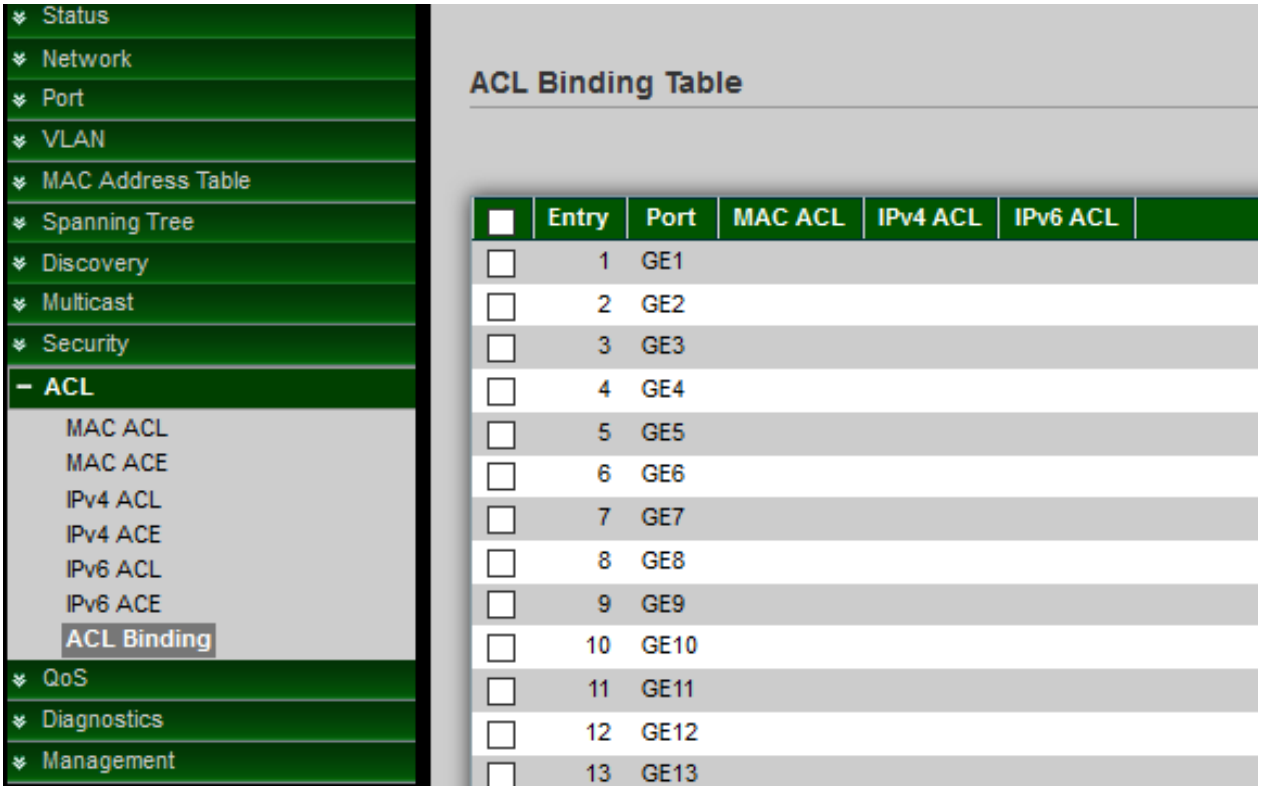
➢ **ICMP Code:** Select the type for ICMP code. Only available when protocol is ICMP.

- **Any:** All codes are acceptable.
- **User Defined:** Enter an ICMP code to match.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

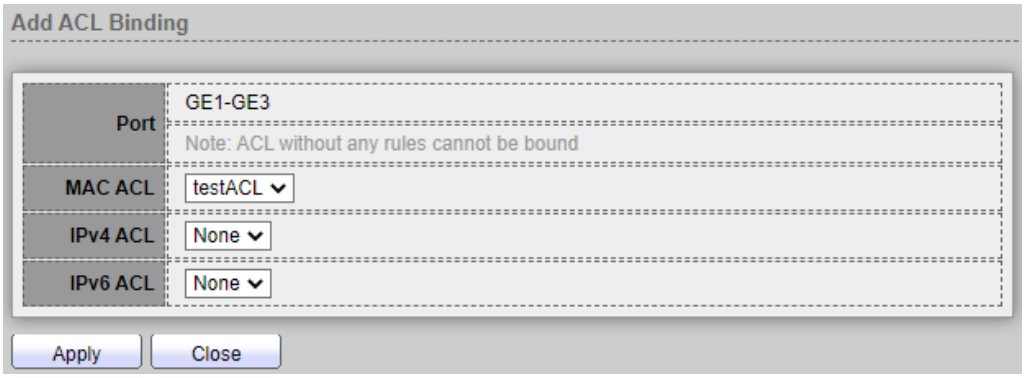
11.7 ACL Binding

This page allow user to bind or unbind ACL rule to or from interface. IPv4 and Ipv6 ACL cannot be bound to the same port simultaneously , Administrator can from ACL Binding Table to select ports. When an ACL is bound to an interface, its ACE rules are applied to packets arriving at that interface. Packets that do not match any of the ACEs in the ACL are matched to a default rule, whose action is to drop unmatched packets.



Field	Description
Port	Display port entry ID.

MAC ACL	Display mac ACL name that bound of interface. Empty means no rule bound.
IPv4 ACL	Display ipv4 ACL name that bound of interface. Empty means no rule bound.
IPv6 ACL	Display ipv6 ACL name that bound of interface. Empty means no rule bound.



- **Port:** Displays selected Port number.
- **MAC ACL:** MAC ACLs that are bound to the interface, Select mac ACL name from list to bind.
- **IPv4 ACL:** IPv4 ACLs that are bound to the interface, Select IPv4 ACL name from list to bind.
- **IPv6 ACL:** IPv6 ACLs that are bound to the interface, Select IPv6 ACL name from list to bind.

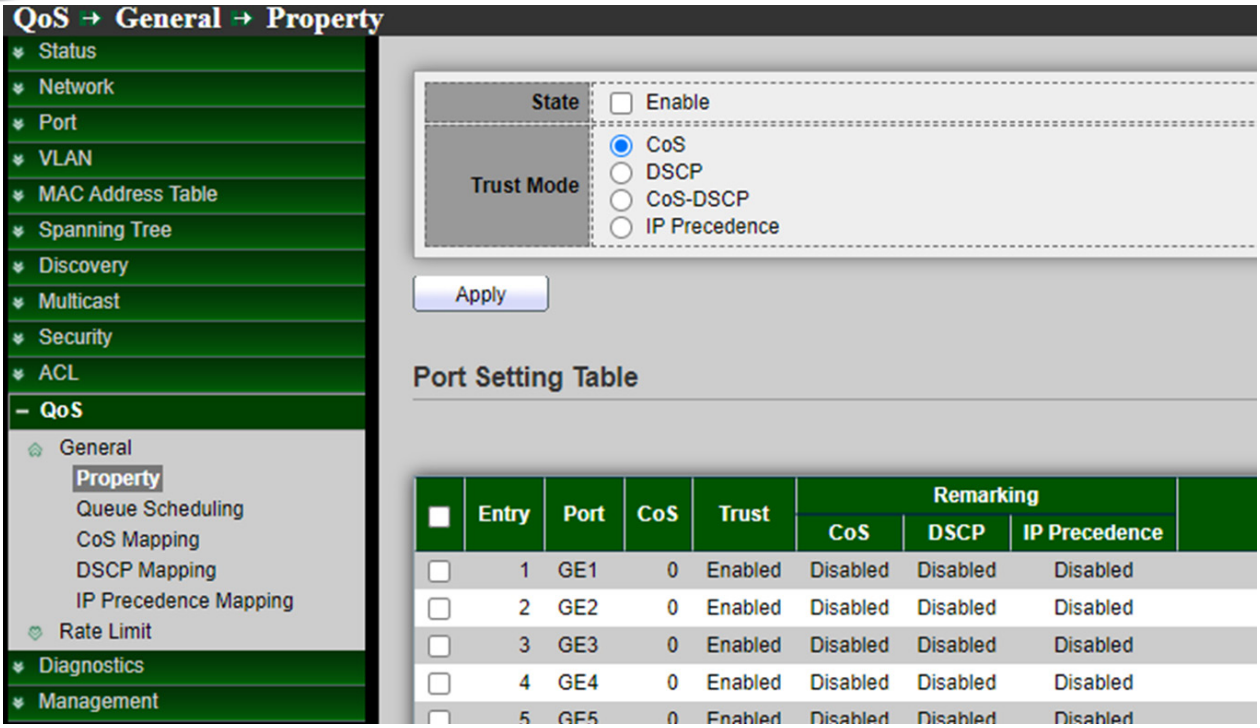
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

12. QoS

The quality of service (QoS) feature is applied throughout the network to ensure that network traffic is prioritized according to required criteria and the desired traffic receives preferential treatment.

12.1 Property

The QoS feature is used to optimize network performance, Use the QoS general pages to configure settings for general purpose

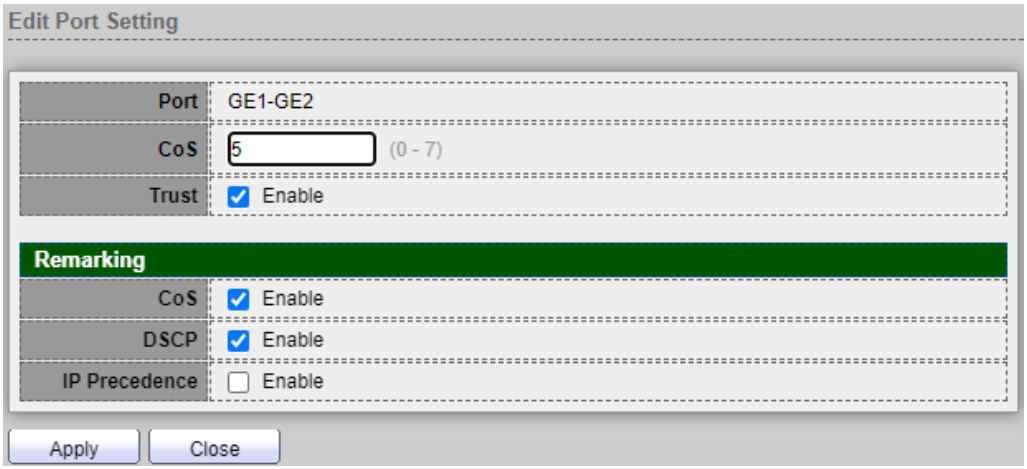


- **State:** Administrator can enable or disable this QoS Feature.
- **Trust Mode:** Administrator can select CoS / DSCP / CoS-DSCP and IP Precedence mode.
  - **CoS:** Traffic is mapped to queues based on the CoS field in the VLAN tag, or based on the per-port default CoS value (if there is no VLAN tag on the incoming packet), the actual mapping of the CoS to queue can be configured on port setting dialog.
  - **DSCP:** All IP traffic is mapped to queues based on the DSCP field in the IP header. The actual mapping of the DSCP to queue can be configured on the DSCP mapping page. If traffic is not IP traffic, it is mapped to the best effort queue..
  - **CoS-DSCP:** Select to use Trust CoS mode for non-IP traffic and Trust DSCP mode for IP traffic.
  - **IP Precedence:** Traffic is mapped to queues based on the IP precedence. The actual mapping of the IP precedence to queue can be configured on the IP Precedence mapping page.

*Click the **"Apply"** button to save your changes settings.*

Field	Description
Port	Interface of port name.
CoS	Port default CoS priority value for the selected ports.
Trust	Port trust state:

	• **Enabled:** Traffic will follow trust mode in global setting. • **Disabled:** Traffic will always use best efforts.
Remarking (CoS)	Remarking (CoS) Port CoS remaking admin state: • **Enabled:** CoS remarking is enabled. • **Disabled:** CoS remarking is disabled.
Remarking (DSCP)	Port DSCP remaking admin state: • **Enabled:** DSCP remarking is enabled. • **Disabled:** DSCP remarking is disabled.



- **Port:** Displays selected port number.
- **CoS:** Set default CoS/802.1p priority value for the selected ports,Set the default CoS value to be assigned for incoming packets (that do not have a VLAN tag). The range is 0 to 7.
- **Trust:** Set checkbox to enable/disable port trust state.
- **Remarking:**
  - **CoS:** Set checkbox to enable/disable port CoS remarking, Traffic is mapped to queues based on the VPT field in the VLAN tag, or based on the per-port default CoS value (if there is no VLAN tag on the incoming packet), the actual mapping of the VPT to queue can be configured on the CoS to Queue page.
  - **DSCP:** Set checkbox to enable/disable port DSCP remarking,All IP traffic is mapped to queues based on the DSCP field in the IP header. The actual mapping of the DSCP to queue can be configured on the DSCP to Queue page. If traffic is not IP traffic, it is mapped to the best effort queue.
  - **IP Precedence:** Set checkbox to enable/disable port IP Precedence remarking, Traffic is mapped to queues based on the IP precedence. The actual mapping of the IP precedence to queue can be configured on the IP Precedence to Queue page.

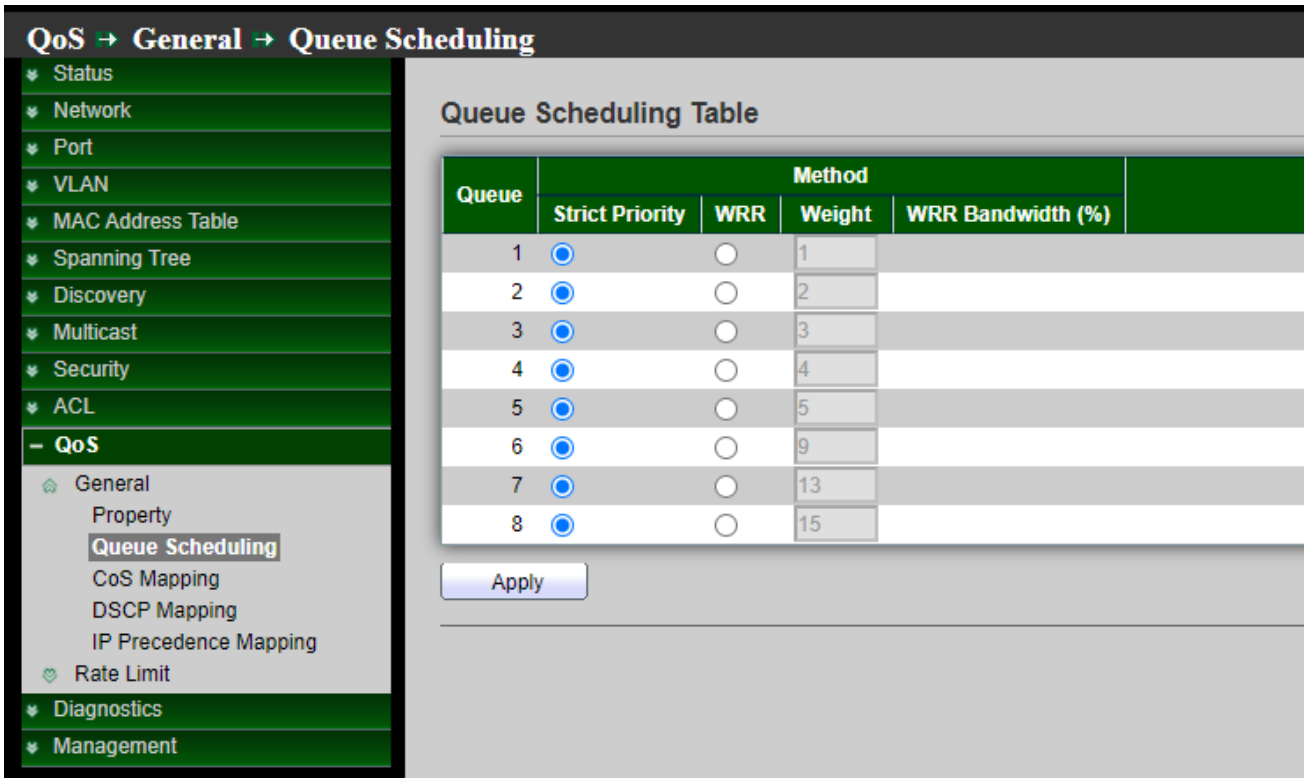
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

12.2 Queue Scheduling

The switch supports eight queues for each interface. Queue number 8 is the highest priority queue. Queue number 1 is the lowest priority queue. There are two ways of determining how traffic in queues is handled, Strict Priority (SP) and Weighted Round Robin (WRR).

- Strict Priority (SP)—Egress traffic from the highest priority queue is transmitted first. Traffic from the lower queues is processed only after the highest queue has been transmitted, which provide the highest level of priority of traffic to the highest numbered queue.
- Weighted Round Robin (WRR)—In WRR mode the number of packets sent from the queue is proportional to the weight of the queue (the higher the weight, the more frames are sent).

The queuing modes can be selected on the Queue page.When the queuing mode is by Strict Priority, the priority sets the order in which queues are serviced, starting with queue_8 (the highest priority queue) and going to the next lower queue when each queue is completed.
When the queuing mode is Weighted Round Robin, queues are serviced until their quota has been used up and then another queue is serviced. It is also possible to assign some of the lower queues to WRR, while keeping some of the higher queues in Strict Priority. In this case traffic for the SP queues is always sent before traffic from the WRR queues. After the SP queues have been emptied, traffic from the WRR queues is forwarded. (The relative portion from each WRR queue depends on its weight).

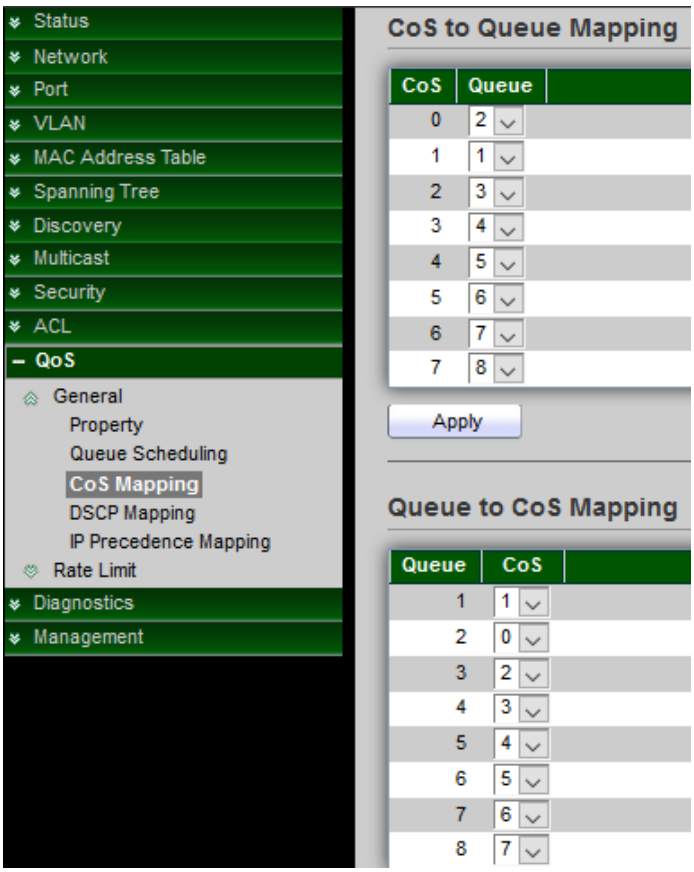


Field	Description
Queue	Queue ID to configure
Strict Priority	Set queue to strict priority type
WRR	Set queue to Weight round robin type
Weight	If the queue type is WRR, set the queue weight for the queue.
WRR Bandwidth	Percentage of WRR queue bandwidth

*Click the **"Apply"** button to save your changes settings.*

12.3 CoS Mapping

The CoS to Queue table determines the egress queues of the incoming packets based on the 802.1p priority in their VLAN tags. For incoming untagged packets, the 802.1p priority will be the default CoS/802.1p priority assigned to the ingress ports.Use the Queues to CoS table to remark the CoS/802.1p priority for egress traffic from each queue.



CoS to Queue Mapping

- **CoS:** CoS value.
- **Queue:** Select queue id for the CoS value.

*Click the **"Apply"** button to save your changes settings.*

Queue to CoS Mapping

- **Queue:** Queue ID.
- **Cos:** Select CoS value for the queue id.

*Click the **"Apply"** button to save your changes settings.*

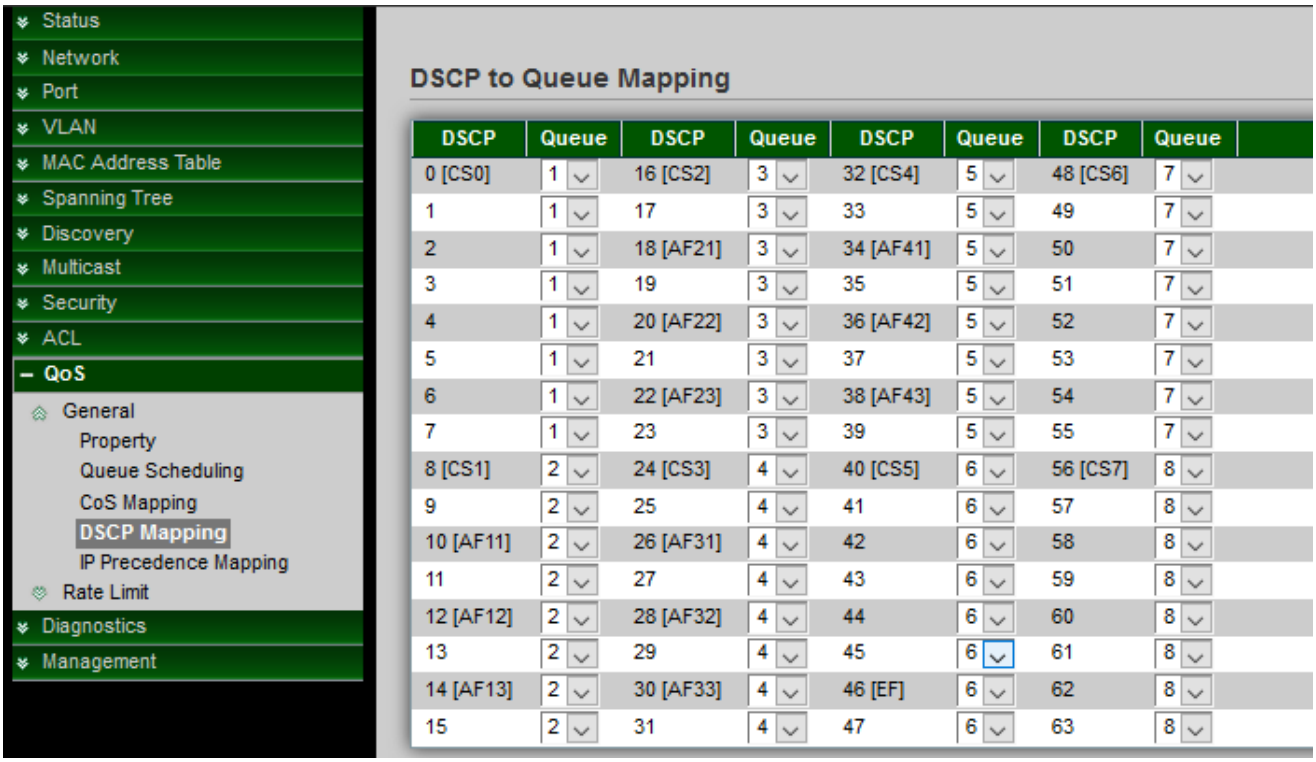
CoS (0 to 7) 7 is highest	Queue(1 to 8) 8 is highest priority	Description
0	2	Background
1	1	Best Effort
2	3	Excellent Effort
3	4	Critical Application LVS phone SIP
4	5	Video
5	6	Voice IP phone default
6	7	Interwork Control LVS phone RTP
7	8	Network Control

12.4 DSCP Mapping

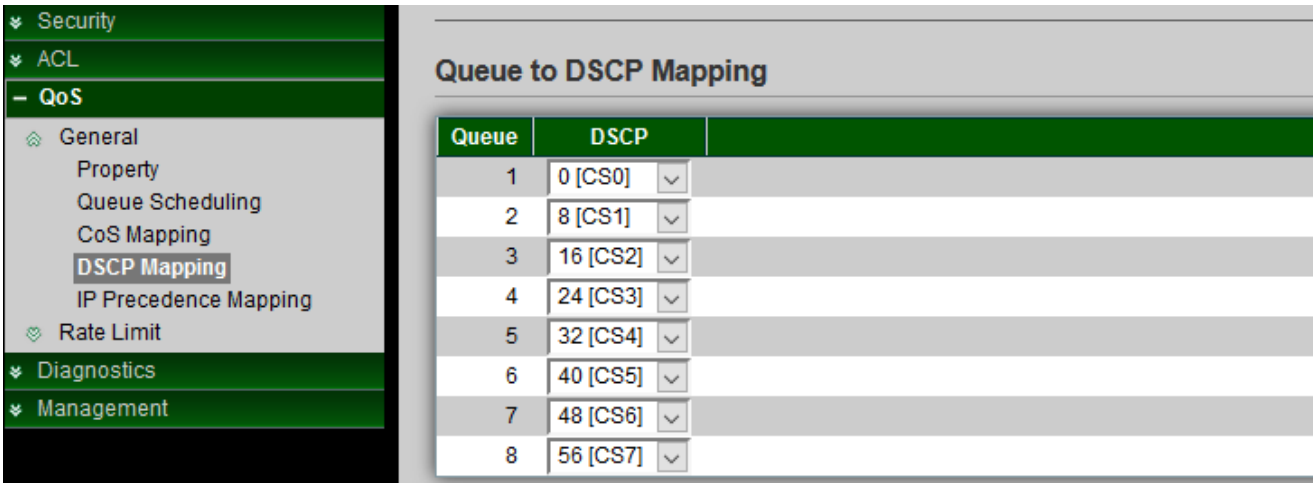
The DSCP to Queue table determines the egress queues of the incoming IP packets based on their DSCP values. The original VLAN Priority Tag (VPT) of the packet is unchanged.

This DSCP values range from 0 through 63, whereas the internal forwarding priority values range from 1 through 8. Any DSCP value within a given range is mapped to the same internal forwarding priority value. These include the CS (Class Selector), AF (Assured Forwarding) and EF (Expedited Forwarding). For example, a packet with a DSCP tag value of 1 can be assigned to the High queue.

Use the Queues to DSCP page to remark DSCP value for egress traffic from each queue.



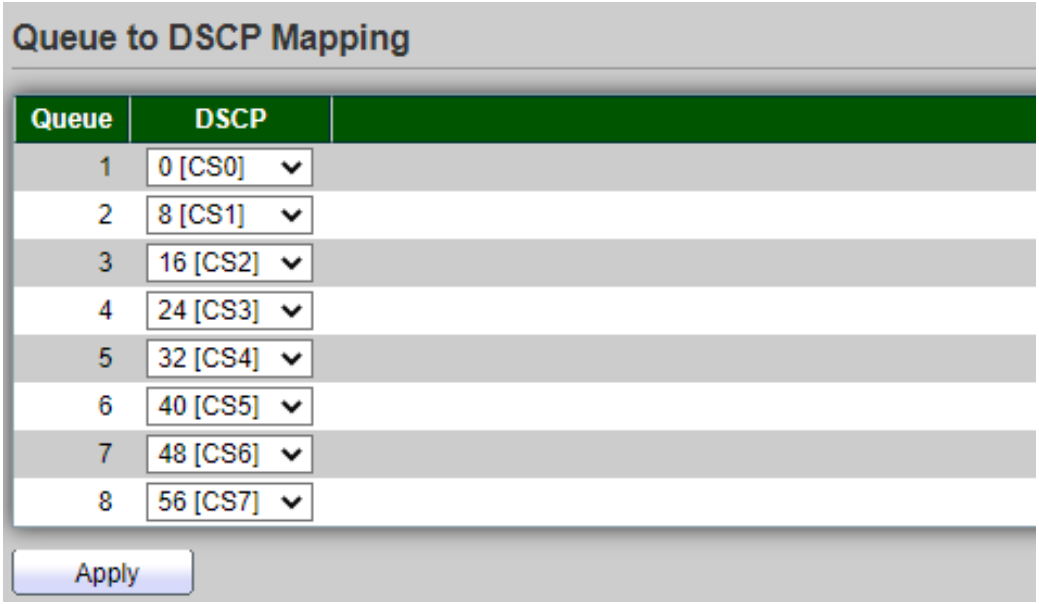
DSCP to Queue Mapping



- **DSCP:** DSCP value.
- **Queue:** Select queue id for DSCP value.

*Click the **"Apply"** button to save your changes settings.*

Queue to DSCP Mapping

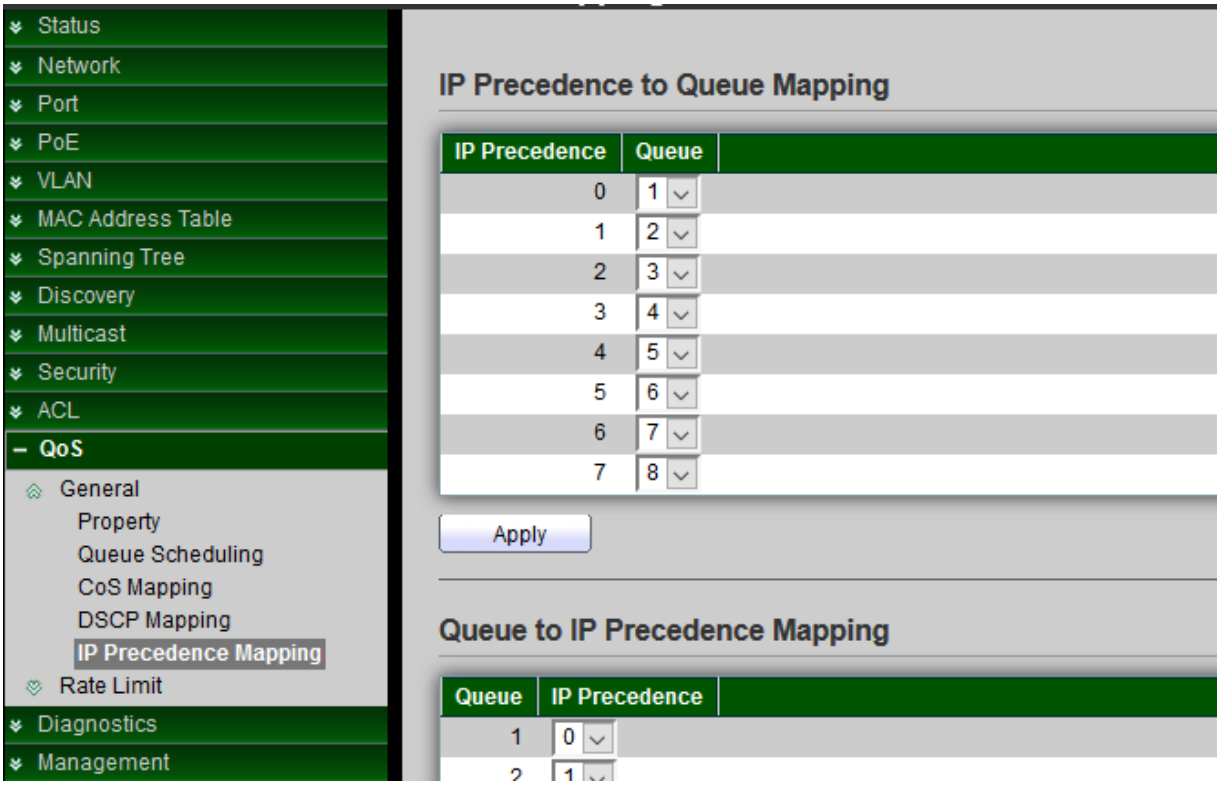


- **Queue:** DSCP value.
- **DSCP:** Select DSCP value for queue id.

*Click the **"Apply"** button to save your changes settings.*

12.5 IP Precedence to Queue Mapping

This page allow user to configure IP Precedence to Queue mapping and Queue to IP Precedence mapping , The IP Precedence standard uses the first 3 bits of the ToS byte to mark packets with 8 levels of priority, numbered 0-7, with 0 being the lowest priority and 7 the highest. Because IP Precedence and ToS use different bits in the ToS byte to mark the priority of a packet, they can co-exist in the same packet header without interfering with each other.



IP Precedence to Queue mapping

- **IP Precedence:** IP Precedence value.
- **Queue:** Queue value which IP Precedence is mapped.

*Click the **"Apply"** button to save your changes settings.*

Queue to IP Precedence mapping

- **Queue:** Queue ID.
- **IP Precedence:** IP Precedence value which queue is mapped.

*Click the **"Apply"** button to save your changes settings.*

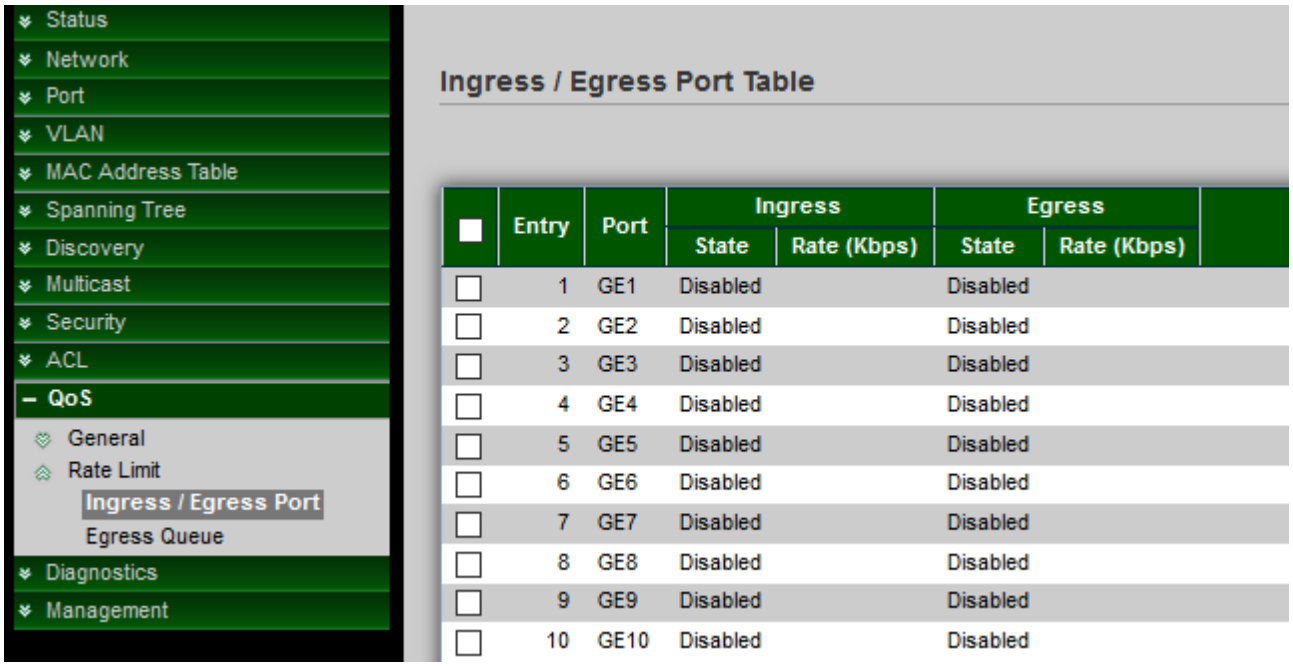
12.6 Rate Limit

This page allow user to configure ingress port rate limit and egress port rate limit. The ingress rate limit is the number of bits per second that can be received from the ingress interface. Excess bandwidth above this limit is discarded.

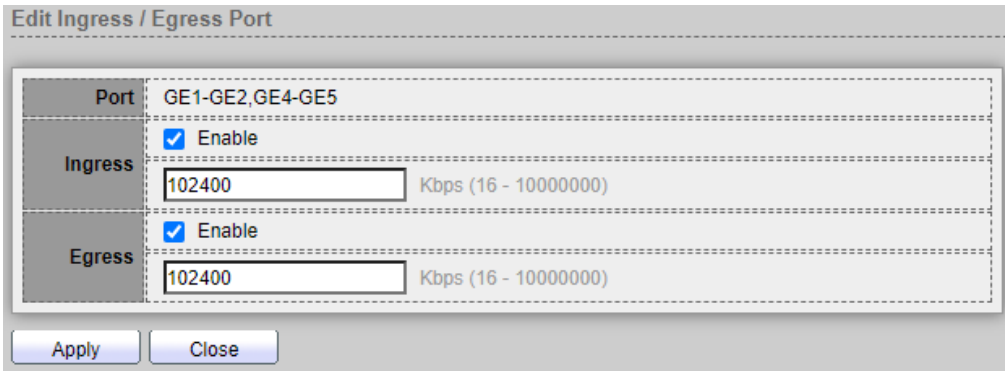
12.6.1 Ingress / Egress Port

The rate limiting function can be configured to limit of Ingress/Egress traffic on a particular interface.

Administrator can set Ingress/Egress rate limiting in Ports. The usage rate is 16 to 10000000 Kbps



Field	Description
Port	Port name.
Trust	Port ingress rate limit state: • **Enabled:** To enabled Ingress rate limit function. • **Disabled:** To disabled the Ingress rate limit function.
Ingress (Rate)	Port ingress rate limit value if ingress rate state is enabled.
Ingress (Rate)	Port ingress rate limit value if ingress rate state is enabled.
IP Precedence	IP Precedence value which queue is mapped.
Trust	Port egress rate limit state: • **Enabled:** To enabled Egress rate limit function. • **Disabled:** To disabled Egress rate limit function.
Egress (Rate)	Port egress rate limit value if egress rate state is enabled.

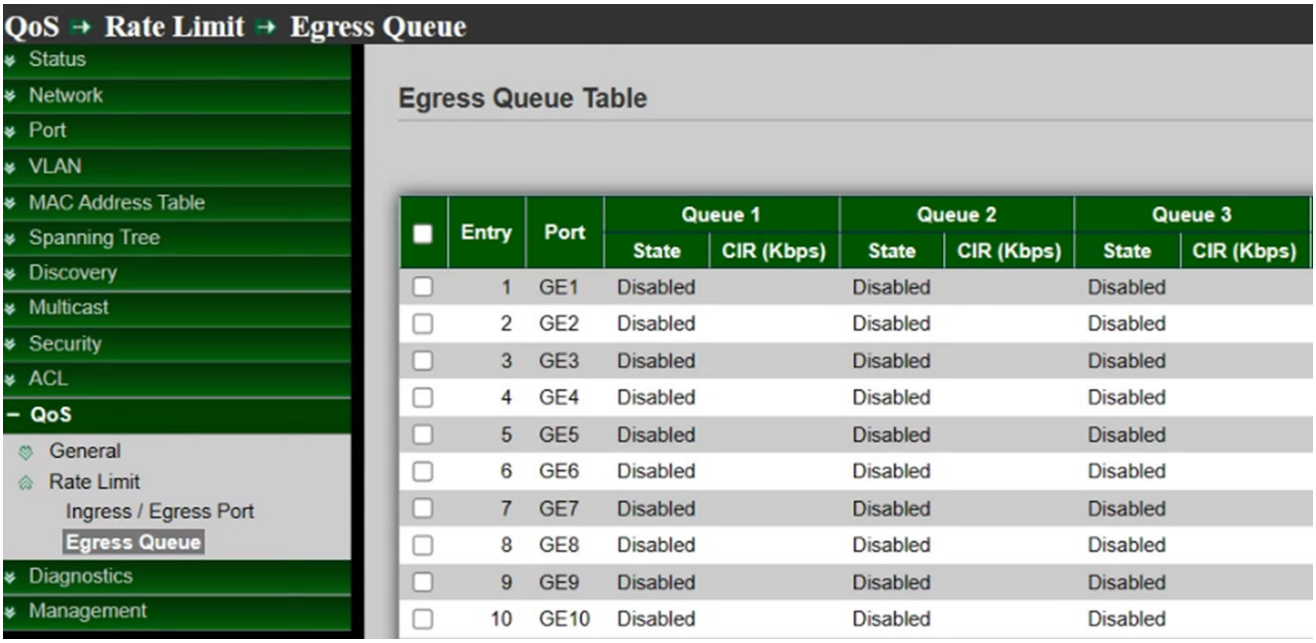


- **Port:** Select the checkbox for port list.
- **Ingress :** Set checkbox to enable/disable ingress rate limit. If ingress rate limit is enabled, rate limit value need to be assigned, The control Range is “16-10000000 Kbps”.
- **Ingress :** Set checkbox to enable/disable egress rate limit. If egress rate limit is enabled, rate limit value need to be assigned, The control Range is “16-10000000 Kbps”.
- **Ingress :** Set checkbox to enable/disable ingre

*Click the **“Apply”** button to save your changes or **“Close”** the button to close settings.*

12.6.2 Egress Queue

The Egress Queue function can be configured priority Queue by QoS. Egress rate limiting is performed by shaping the output load.Administrator can set Ingress Queue by limiting QoS . The usage rate is 16 to 1000000 Kbps, Please Click "Edit" button to set the Egress Queue Port menu.



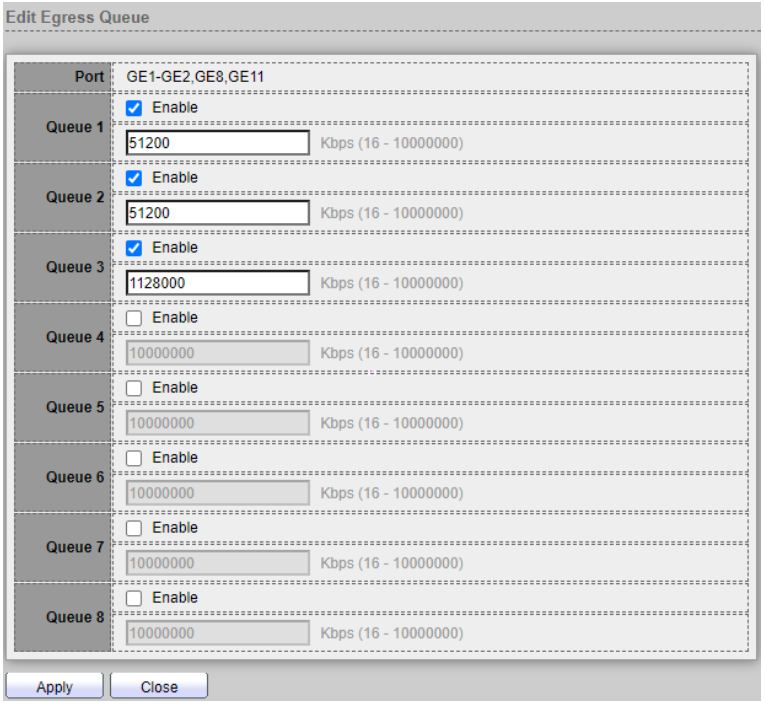
Entry	Port	Queue 1		Queue 2		Queue 3	
		State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)
1	GE1	Disabled		Disabled		Disabled	
2	GE2	Disabled		Disabled		Disabled	
3	GE3	Disabled		Disabled		Disabled	
4	GE4	Disabled		Disabled		Disabled	
5	GE5	Disabled		Disabled		Disabled	
6	GE6	Disabled		Disabled		Disabled	
7	GE7	Disabled		Disabled		Disabled	
8	GE8	Disabled		Disabled		Disabled	
9	GE9	Disabled		Disabled		Disabled	
10	GE10	Disabled		Disabled		Disabled	

Egress Queue Table

Entry	Port	Queue 1		Queue 2		Queue 3		Queue 4		Queue 5		Queue 6		Queue 7		Queue 8	
		State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)
1	GE1	Enabled	51200	Enabled	51200	Enabled	62496	Disabled		Disabled		Disabled		Disabled		Disabled	
2	GE2	Enabled	51200	Enabled	51200	Enabled	62496	Disabled		Disabled		Disabled		Disabled		Disabled	
3	GE3	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
4	GE4	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
5	GE5	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
6	GE6	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
7	GE7	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
8	GE8	Enabled	51200	Enabled	51200	Enabled	62496	Disabled		Disabled		Disabled		Disabled		Disabled	
9	GE9	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	

Field	Description
Port	Interface of port number.
Queue 1 (State)	Port egress queue 1 rate limit state • **Enabled:** Egress queue rate limit is enabled. • **Disabled:** Egress queue rate limit is disabled.
Queue 1 (CIR)	Queue 1 egress committed information rate.
Queue 2 (State)	Port egress queue 2 rate limit state. • **Enabled:** Egress queue rate limit is enabled. • **Disabled:** Egress queue rate limit is disabled.
Queue 2 (CIR)	Queue 2 egress committed information rate.
Queue 3 (State)	Port egress queue 3 rate limit state. • **Enabled:** Egress queue rate limit is enabled. • **Disabled:** Egress queue rate limit is disabled.
Queue 3 (CIR)	Queue 3 egress committed information rate.
Queue 4 (State)	Port egress queue 4 rate limit state. • **Enabled:** Egress queue rate limit is enabled. • **Disabled:** Egress queue rate limit is disabled.
Queue 4 (CIR)	Queue 4 egress committed information rate.
Queue 5 (State)	Port egress queue 5 rate limit state. • **Enabled:** Egress queue rate limit is enabled. • **Disabled:** Egress queue rate limit is disabled.
Queue 5 (CIR)	Queue 5 egress committed information rate.
Queue 6 (State)	Port egress queue 6 rate limit state. • **Enabled:** Egress queue rate limit is enabled.

	• **Disabled:** Egress queue rate limit is disabled
Queue 6 (CIR)	Queue 6 egress committed information rate.
Queue 7 (State)	Port egress queue 7 rate limit state. • **Enabled:** Egress queue rate limit is enabled. • **Disabled:** Egress queue rate limit is disabled.



Set checkbox to enable/disable ingress priority queue 1 to~ queue 8 level , The control range is "16-1000000 Kbps"

- **Port:** Select one or multiple ports for the configure.
- **Queue 1:** Set checkbox to enable/disable egress queue 1 rate limit.
  - **Enable:** If egress rate limit is enabled, rate limit value need to be assigned.
- **Queue 2:** Set checkbox to enable/disable egress queue 2 rate limit.
  - **Enable:** If egress rate limit is enabled, rate limit value need to be assigned.
- **Queue 3:** Set checkbox to enable/disable egress queue 3 rate limit.
  - **Enable:** If egress rate limit is enabled, rate limit value need to be assigned.
- **Queue 4:** Set checkbox to enable/disable egress queue 4 rate limit.
  - **Enable:** If egress rate limit is enabled, rate limit value need to be assigned.
- **Queue 5:** Set checkbox to enable/disable egress queue 5 rate limit.
  - **Enable:** If egress rate limit is enabled, rate limit value need to be assigned.

- **Queue 6:** Set checkbox to enable/disable egress queue 6 rate limit.
  - **Enable:** If egress rate limit is enabled, rate limit value need to be assigned.
- **Queue 7:** Set checkbox to enable/disable egress queue 7 rate limit.
  - **Enable:** If egress rate limit is enabled, rate limit value need to be assigned.
- **Queue 8:** Set checkbox to enable/disable egress queue 8 rate limit.
  - **Enable:** If egress rate limit is enabled, rate limit value need to be assigned.

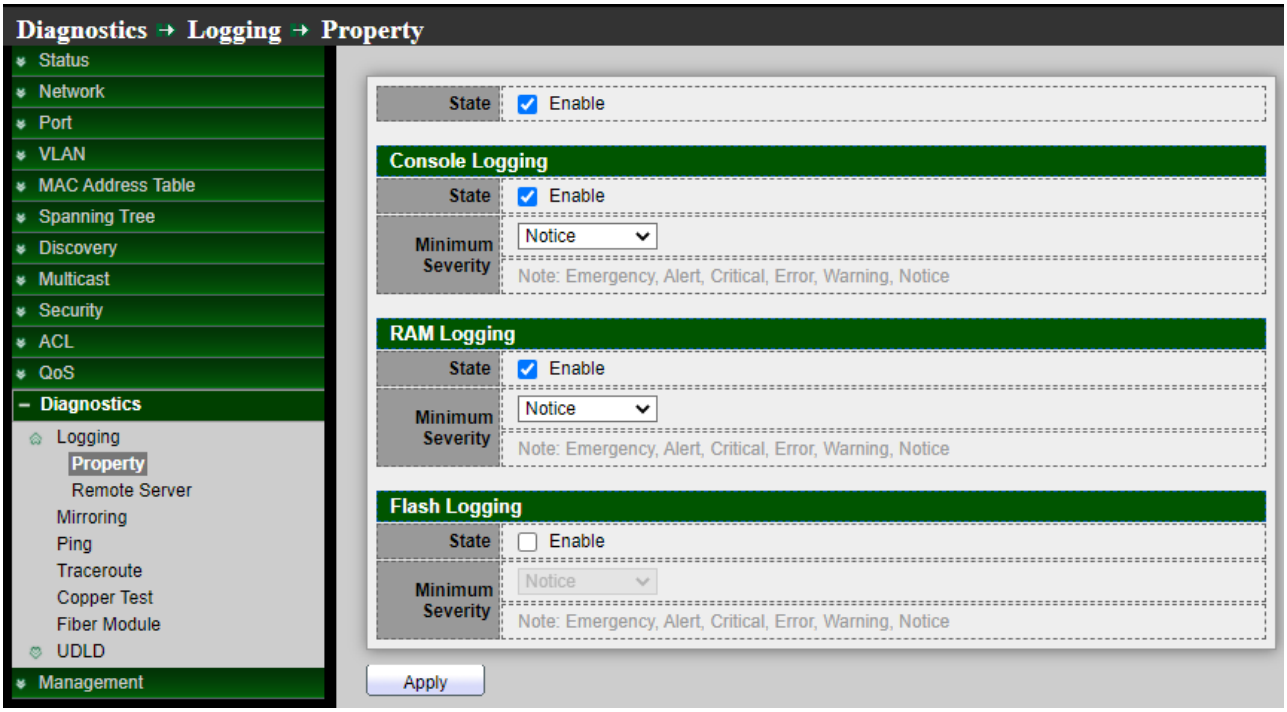
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

13. Diagnostics

13.1 Logging

13.1.1 Property

This function support log message includes Console / RAM / Flash message send to remote log server. Administrator can enable or disable this function. Use the Diagnostics pages to configure settings for the switch diagnostics feature or operating diagnostic utilities.



- **State:** When the logging service is enabled, logging configuration of each destination rule can be individually configured. If the logging service is disabled, no messages will be sent to these destinations.

- **Enable:** Enable/Disable the global logging services.

➢ **Aggregation:**

- **Enable:** Enable/Disable the aggregation services.
- **Aging:** 15~3600 Second. The default is 300 second.

➢ **Console Logging:**

- **State:** Enable/Disable the Console Logging services.
- **Minimum Severity:** The minimum severity for the Console Logging. Including selection of events such as Emergency, Alert, Critical, Error, Warning, Notice, Information, Debug, etc.

➢ **RAM Loggong:**

- **State:** Enable/Disable the RAM Loggong services.
- **Minimum Severity:** The minimum severity for the RAM logging. Including selection of events such as Emergency, Alert, Critical, Error, Warning, Notice, Information, Debug, etc.

➢ **Flash Loggong:**

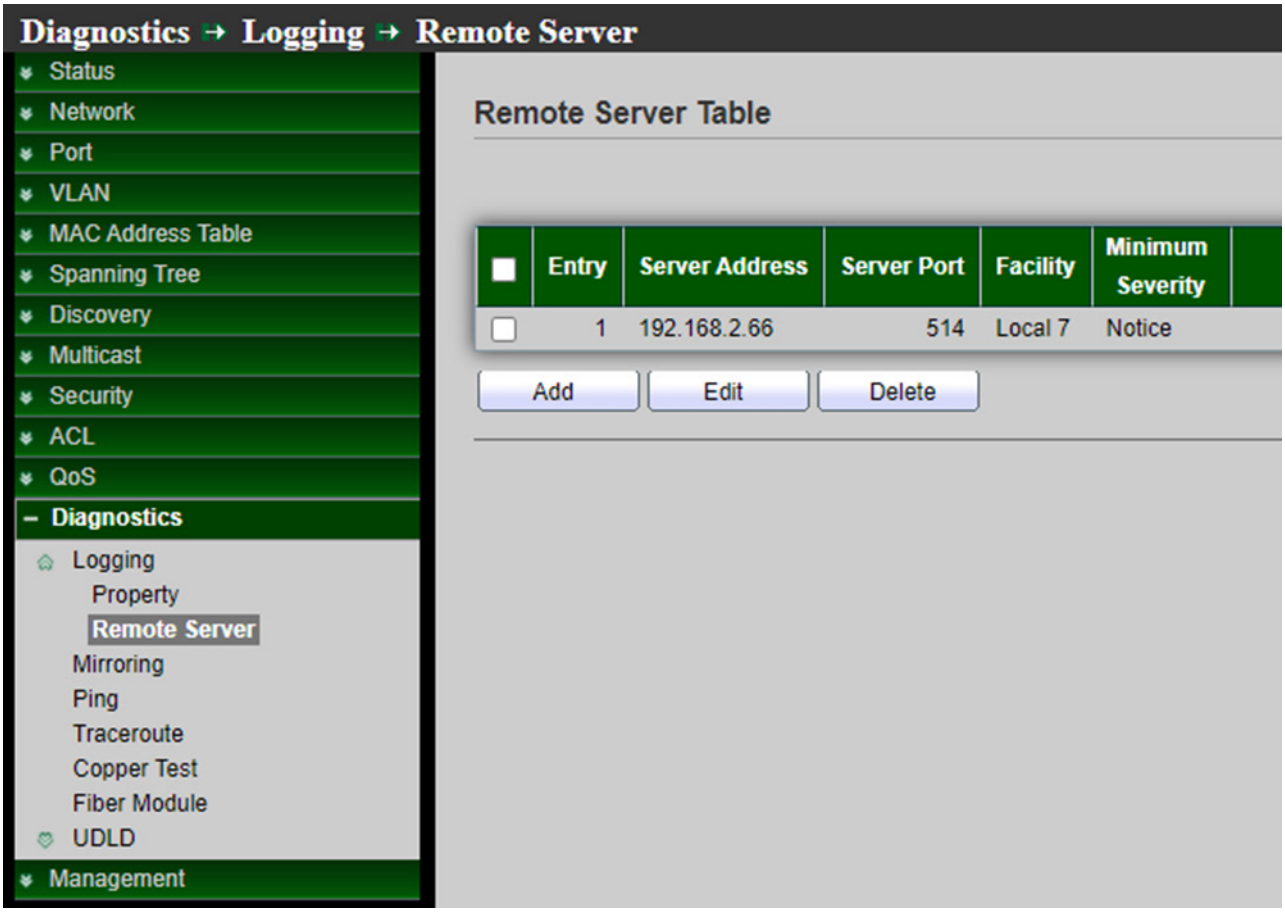
- **State:** Enable/Disable the Flash Loggong services.
- **Minimum Severity:** The minimum severity for the flash logging. Including selection of events such as Emergency, Alert, Critical, Error, Warning, Notice, Information, Debug, etc.

Note	• Emergency—System is not usable. • Alert—Action is needed. • Critical—System is in a critical condition. • Error—System is in error condition. • Warning—System warning has occurred. • Notice—System is functioning properly, but a system notice has occurred. • Informational—Device information. • Debug—Detailed information about an event.

*Click the **"Apply"** button to save your changes settings.*

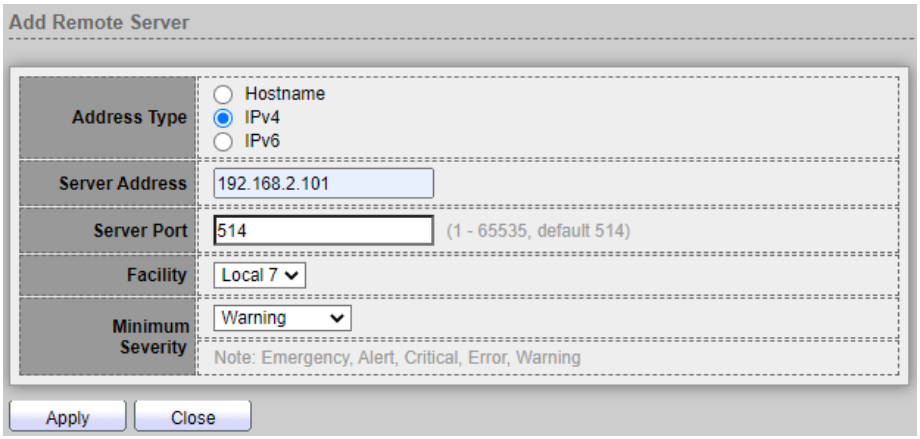
13.1.2 Remote Server

Use the Remote Log Servers page to define the remote SYSLOG servers where log messages are sent (using the SYSLOG protocol). For each server, you can configure the severity of the messages that it receives, Setting **"add"** and "Edit" and **"Delete"** for this function management.



Field	Description
Server Address	The IP address of the remote logging server.
Server Ports	The port number of the remote logging server.
Facility	The facility of the logging messages. It can be one of the following values: local0, local1, local2, local3, local4, local5, local6, and l7.
Minimum Severity	The minimum severity. • **Emergence:** System is not usable. • **Alert:** Immediate action is needed. • **Critical:** System is in the critical condition. • **Error:** System is in error condition. • **Warning:** System warning has occurred. • **Notice:** System is functioning properly, but a system notice has occurred.

- **Informational:** Device information.
- **Debug:** Provides detailed information about an event.

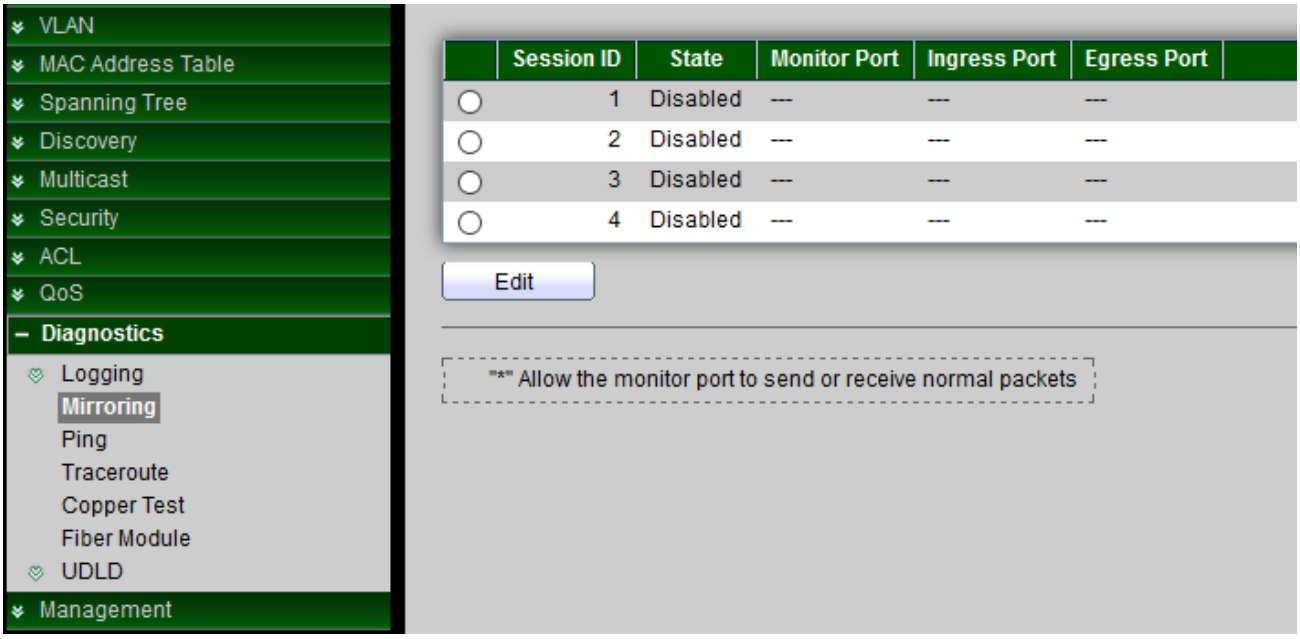


- **Address Type:** Administrator can select use Hostname or IPv4/6 connection remote log server.
- **Server Address:** Enter the IP address of the server.
- **Server Port:** Enter service port to which the log messages are sent.
- **Facility:** Select a facility from which system logs are sent to the remote server. Only one facility can be assigned to a server.
- **Minimum Severity:** Select the minimum level of system log messages to be sent to the server.
  - **Emergence:** System is not usable.
  - **Alert:** Immediate action is needed.
  - **Critical:** System is in the critical condition.
  - **Error:** System is in error condition.
  - **Warning:** System warning has occurred.
  - **Notice:** System is functioning properly, but a system notice has occurred.
  - **Informational:** Device information.
  - **Debug:** Provides detailed information about an event..

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

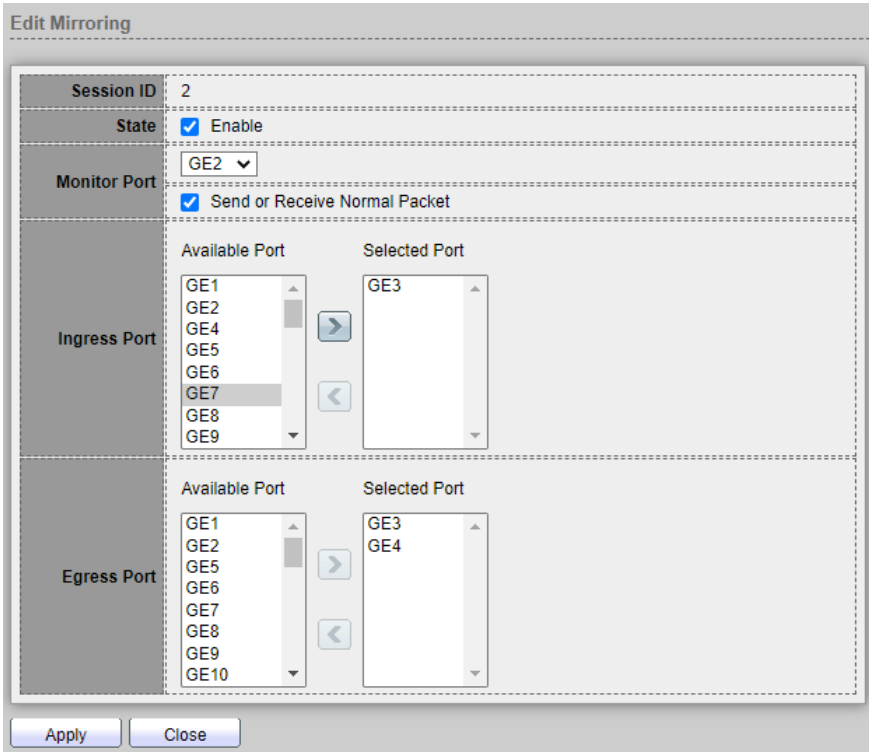
13.2 Mirroring

Mirroring function can mirror Rx/Tx traffic, Packet can mirror to destination port and for analysis.



Field	Description
Session ID	Select mirror session ID
State	Select mirror session state : port-base mirror or disable • **Enabled:** Enable port based mirror • **Disabled:** Disable mirror.
Monitor Port	Select mirror session monitor port, and select whether normal packet could be sent or received by monitor port.
Ingress port	Select mirror session source rx ports
Egress ports	Select mirror session source tx ports

*Click the "**Edit**" button to edit your settings.*



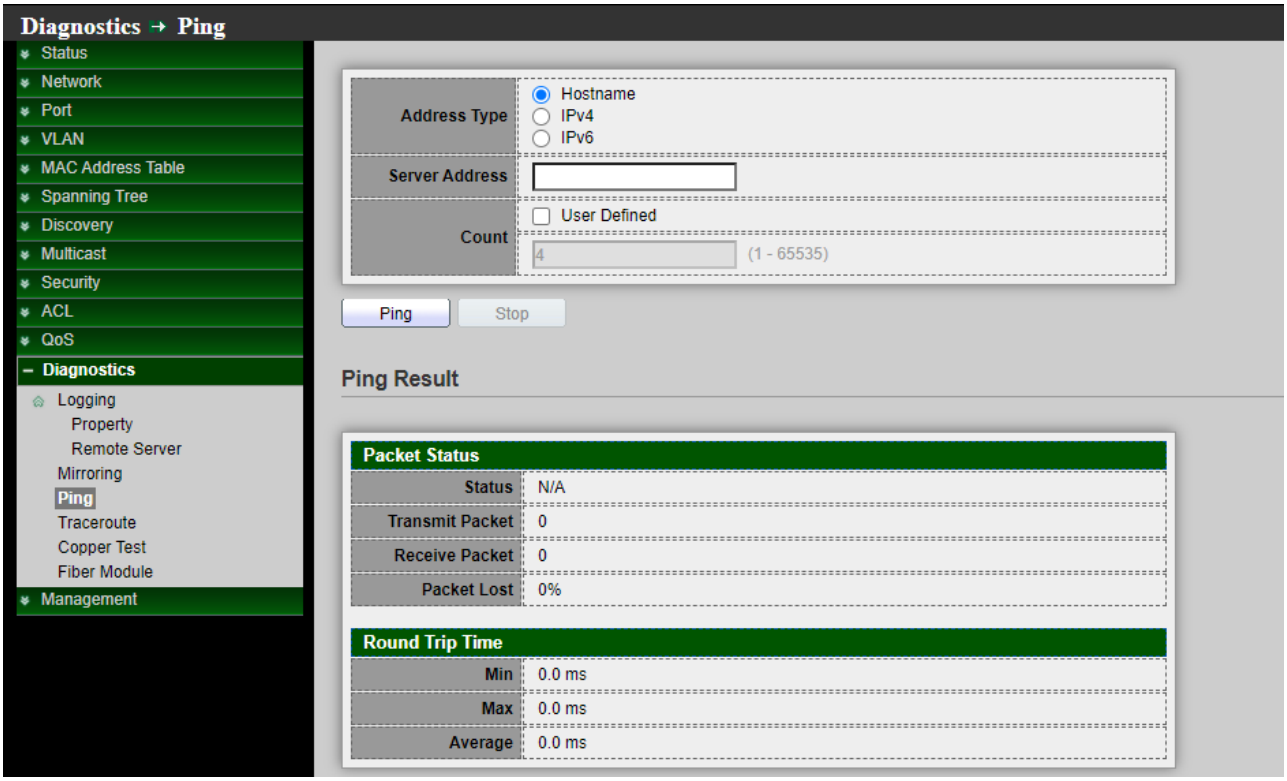
- **Session ID:** Display selected mirror session ID.
- **State:**
  - **Enable:** Enable/Disable the mirroring function.
- **Mirroring Port:** Administrator can choose a mirroring Port.
- **Ingress Port:** Administrator can choose mirrored ports for ingress.
- **Egress Port:** Administrator can choose mirrored ports for egress

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

13.3 Ping

The Ping utility tests if a remote host can be reached and measures the round-trip time for packets sent from the device to a destination device.

Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP response, sometimes called a pong. It measures the round-trip time and records any packet loss, Administrators can use this ping function to check connected device whether is active. This ping function support IPv4 and IPv6 protocol.



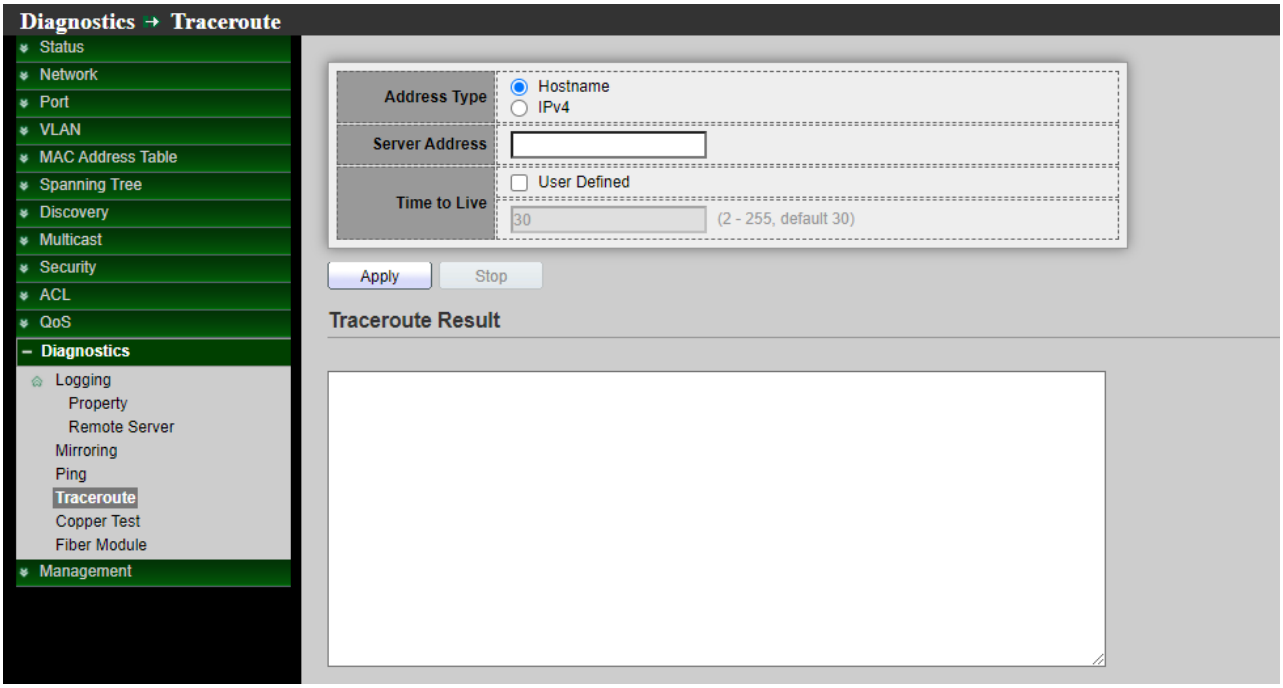
- **Address Type:** Specify the address type to “Hostname”, “IPv6”, or “IPv4”.
- **Server Address:** Specify the Hostname/IPv4/IPv6 address for the remote logging server.
- **Count:** Specify the numbers of each ICMP ping request.

*Click the **“Ping”** button to ping result appears.*

Field	Description
Packet Status	Displays whether the ping succeeded or failed. • **Status:** Displays the ping result status of “ Success” or “Ping failed (timeout)”. • **Transmit Packet:** Number of packets sent by ping. • **Receive Packet:** Number of packets received by ping. • **Packet Lost:** Percentage of packets lost in ping process.
Round Trip Time	Displays the ping **round trip time.** • **Min:** Shortest time for packet to return. • **Max:** Longest time for packet to return. • **Average:** Average time for packet to return

13.4 Traceroute

Traceroute discovers the IP routes along which packets were forwarded by sending an IP packet to the target host and back to the switch. The Traceroute page displays each hop between the switch and a target host and the round-trip time to each hop.

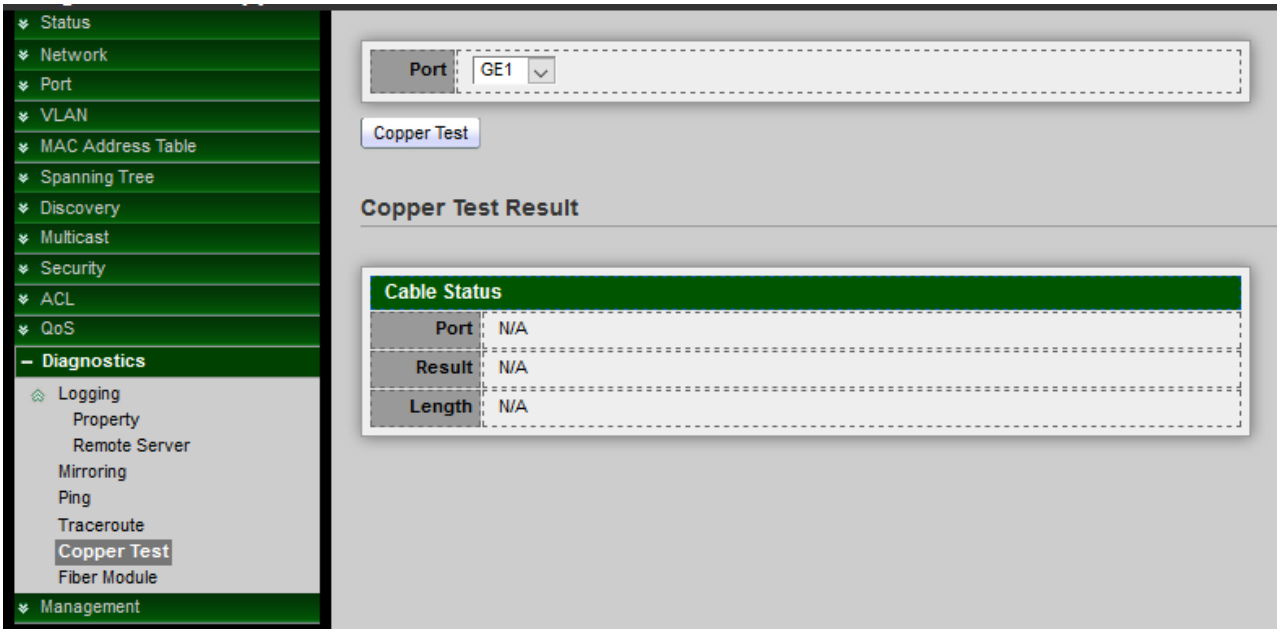


- **Address Type:** Specify the address type to “Hostname”, or “IPv4”.
- **Server Address:** Specify the Hostname/IPv4 address for the remote logging server.
- **Time to Live :**Enter the maximum number of hops that Traceroute permits. This is used to prevent a case where the sent frame gets into an endless loop. The Traceroute command terminates when the destination is reached or when this value is reached. To use the default value (30), select Use Default.

*Click the **“Apply”** button to Traceroute result appears.*

13.5 Copper Test

Administrator can use this function check port Result whether is working, if working then display it.



Field	Description
Port	Specify the interface for the copper test.

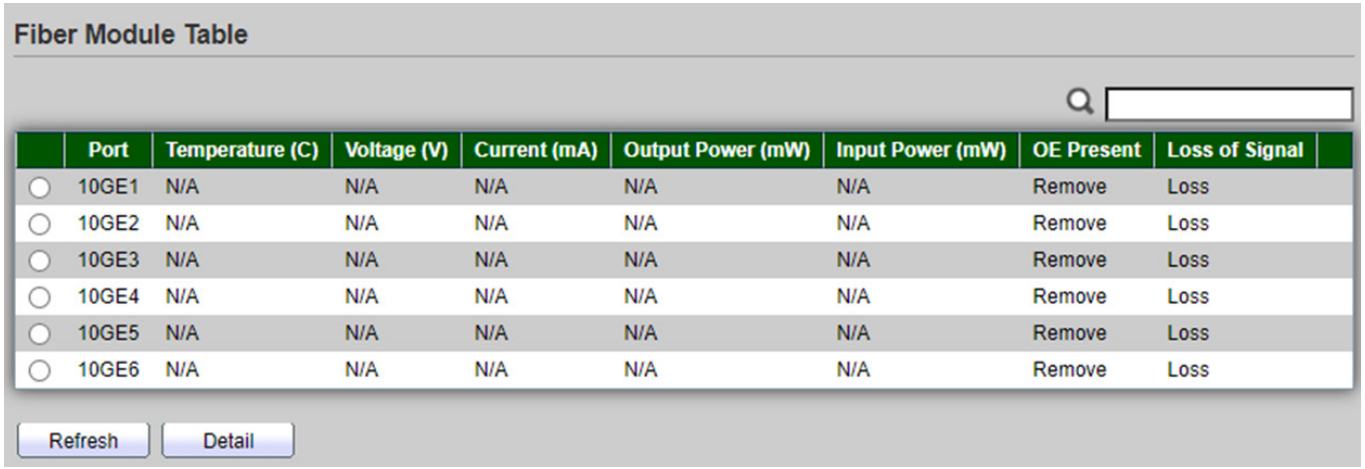
*Click the **"Copper Test"** button to Copper Test result appears.*

Cable Status

Field	Description
Port	The interface for the copper test.
Result	The status of copper test. It include: • **OK:** Correctly terminated pair. • **Short Cable:** Shorted pair. • **Open Cable:** Open pair, no link partner. • **Impedance Mismatch:** Terminating impedance is not in the reference range. • **Line Drive:**
Length	Distance in meter from the port to the location on the cable where the fault was discovered.

13.6 Fiber Module

Display Fiber module messenger. The Optical Module Status page displays the operational information reported by the Small Form-factor Pluggable (SFP) transceiver. Some information may not be available for SFPs without the supports of digital diagnostic monitoring standard SFF-8472.



Field	Description
Port	Interface or port number.
Temperature	Internally measured transceiver temperature.
Voltage	Internally measured supply voltage.
Current	Measured TX bias current.
Output Power	Measured TX output power in mill watts.
Input Power	Measured RX received power in mill watts.
Transmitter Fault	State of TX fault.
OE Present	Indicate transceiver has achieved power up and data is ready.
Loss of Signal	Loss of signal.
Refresh	Refresh the page.
Detail	The detail information on the specified port.

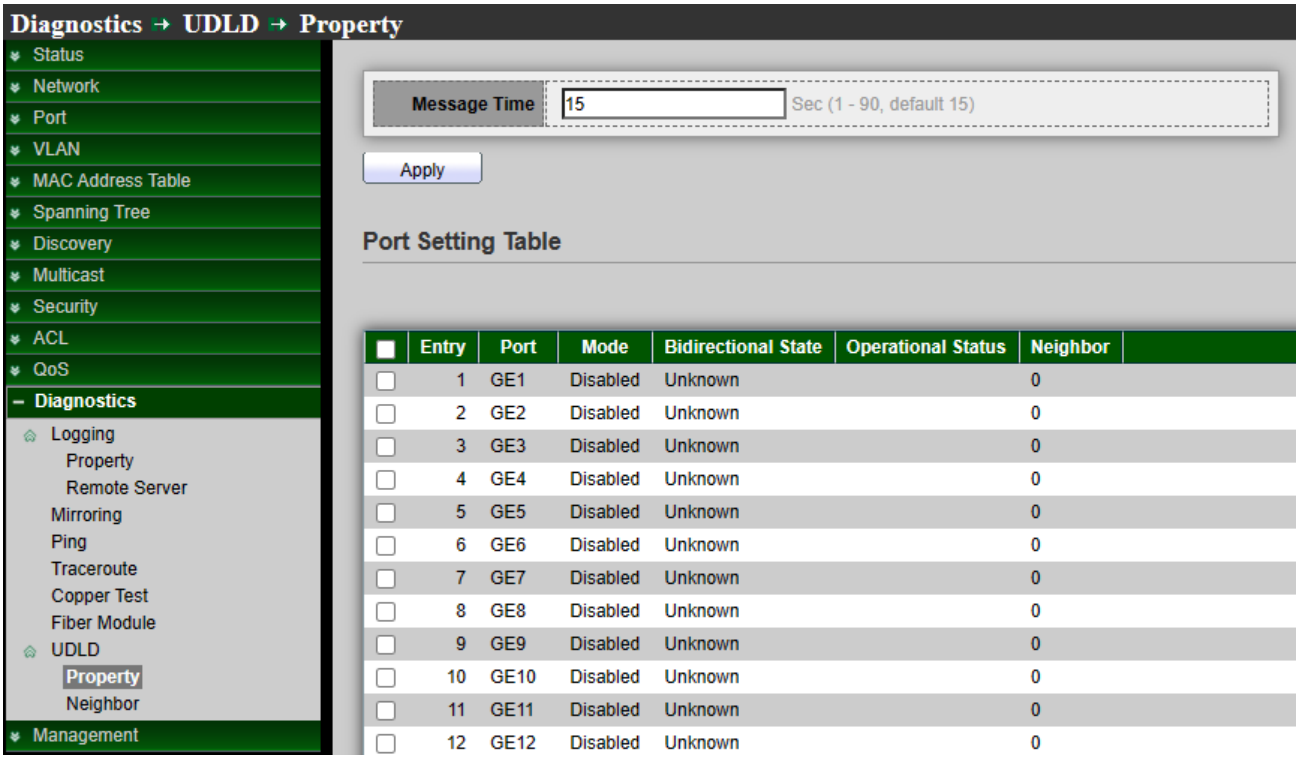
*Click the **"Refresh"** button to refresh this page or click the "**Detail**" button to check detail information.*

13.7 UDLD

Uni-Directional Link Detection (UDLD) monitors a link between two devices and brings the ports on both ends of the link down if the link goes down at any point between the two devices, Use the UDLD pages to configure settings of UDLD function.

13.7.1 Property

This page allow user to configure global and per interface settings of UDLD.



- **Message Time:** To use the UDLD protocol all connected switches and interfaces have to be configured for it. A UDLD configured switch sends UDLD advertisements, "hello" packets to its neighbors and expects to receive one in the designated hold time (the default hold time is 15mins). If this doesn't happen the UDLD disables the unresponsive interface..

*Click the **"Apply"** button to save your changes settings.*

Field	Description
Port	Display port ID of entry.

Mode	Display UDLD running mode of interface.
Bidirectional State	Display bidirectional state of interface.
Operational Status	Display operational status of interface
Neighbor	Display the number of neighbor of interface

- **Port:** Select one or multiple ports for the configure.
- **Mode:** Select UDLD running mode of interface.
  - **Disabled:** Disable UDLD function.
  - **Normal:** Running on normal mode that port goes to Link Up One phase after last neighbor ages out.
  - **Aggressive:** Running on aggressive mode that port goes to Re-Establish phase after last neighbor ages out.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

13.7.2 Neighbor

Each switch port that is configured for UDLD exchanges UDLD protocol packets that include information about the port's device and port ID, and the port also sends the same device and port ID information that it knows about its connected neighbor.

Because of this, a port should receive its own device and port ID information from its neighbor if the link is bi-directional. If a port does not receive information about its own device and port ID from its neighbor, the link is considered to be unidirectional.

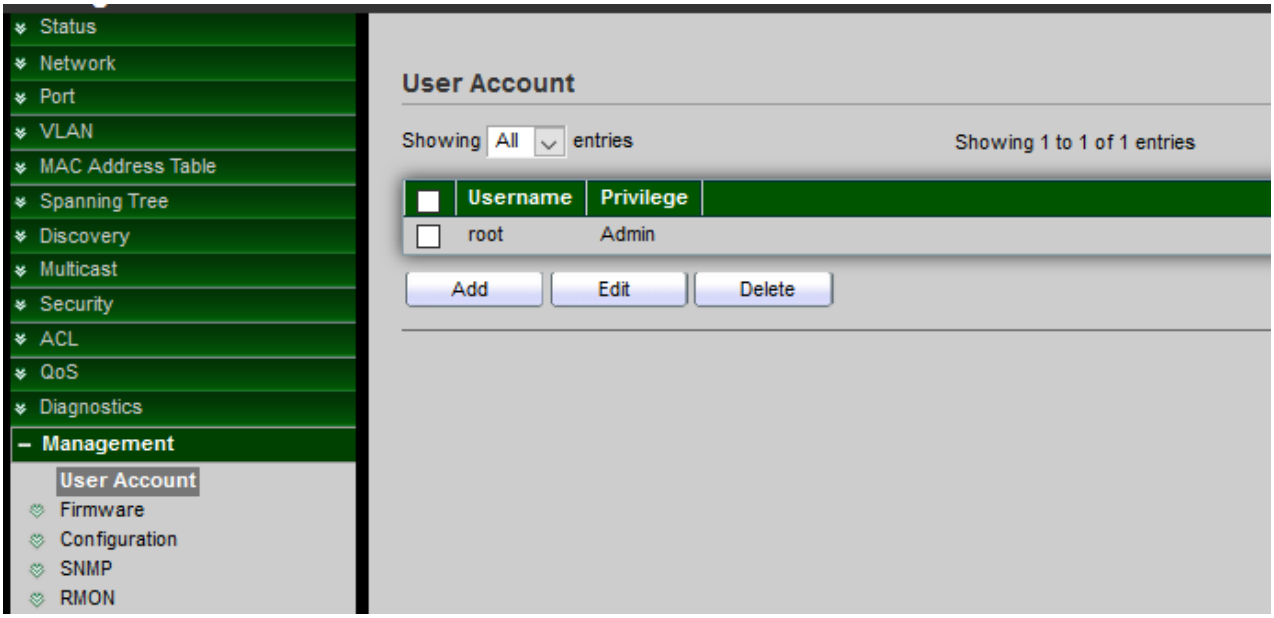
This can occur when the link is up on both sides, but one side is not receiving packets, or when wiring mistakes occur, causing the transmit and receive wires to not be connected to the same ports on both ends of a link.

Field	Description
Entry	Display entry index.
Expiration Time	Display expiration time before age out.
Current Neighbor State	Display neighbor current state
Device ID	Display neighbor device ID.
Device Name	Display neighbor device name.
Port ID	Display neighbor port ID that connected.
Message Interval	Display neighbor message interval.
Timeout Interval	Display neighbor timeout interval

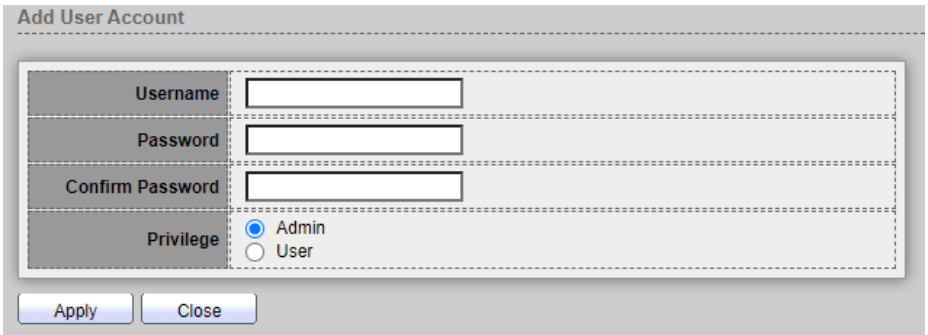
14. Management

14.1 User Account

The default username/password is root/default. Administrator can modify login password or create new username / password and defined Privilege, Setting **“add”** and “Edit” and **“Delete”** function for this management.



Field	Description
Username	User name of the account
Privilege	Display privilege level for new account. • **Admin:** Allow to change switch settings. Privilege value equals to 15. • **User:** See switch settings only. Not allow to change it. Privilege level equals to 1.



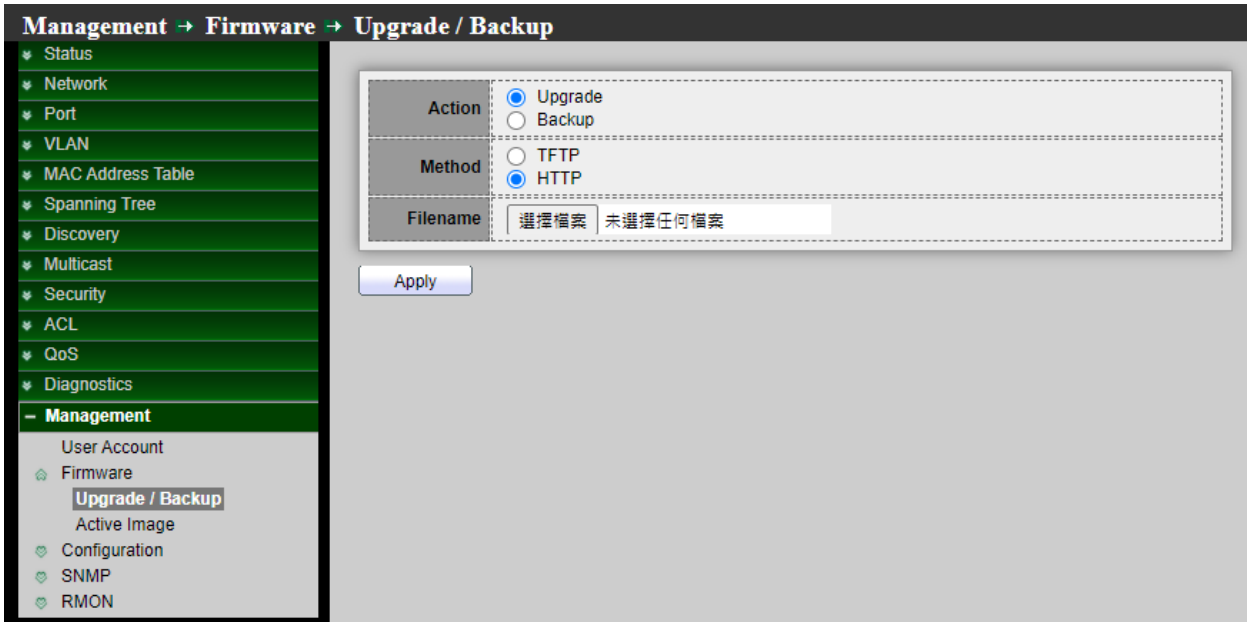
- **Username:** User name of the account.
- **Password:** Set password of the account.
- **Confirm Password:** Set the same password of the account as in “Password” field.
- **Privilege:** Select privilege level for new account.
  - **Admin:** Allow to change switch settings. Privilege value equals to 15.
  - **User:** See switch settings only. Not allow to change it. Privilege level equals to 1.

*Click the **“Apply”** button to save your changes or **“Close”** the button to close settings.*

14.2 Firmware

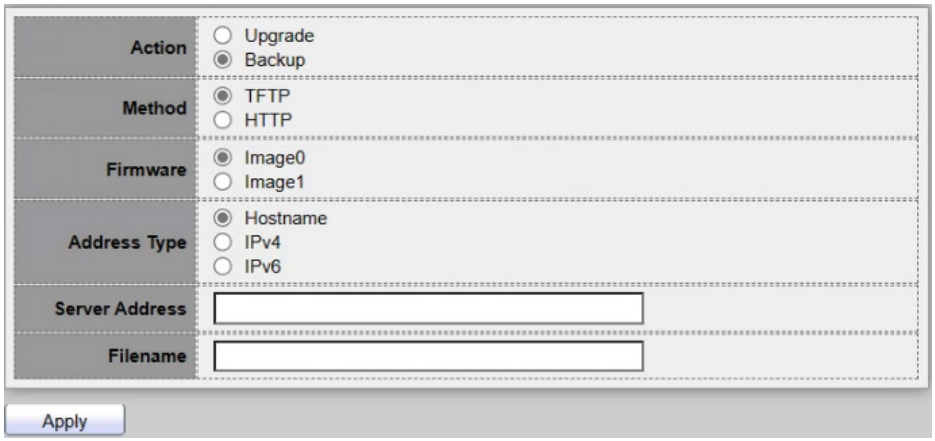
14.2.1 Upgrade / Backup

Administrator can upgrade or backup firmware, method can choose use TFTP or HTTP protocol. If choose backup then administrator can choose firmware image to backup.



- **Action:** Firmware operations.
  - **Upgrade:** Upgrade firmware from remote host to DUT.
  - **Backup:** Backup firmware image from DUT to remote host.
- **Method:** Firmware upgrade / backup method.
  - **TFTP:** Using TFTP to upgrade/backup firmware.
  - **HTTP:** Using WEB browser to upgrade/backup firmware.
- **Filename:** Use browser to upgrade firmware, you should select firmware image file on your host PC.

*Click the **“Apply”** button to save your changes settings.*

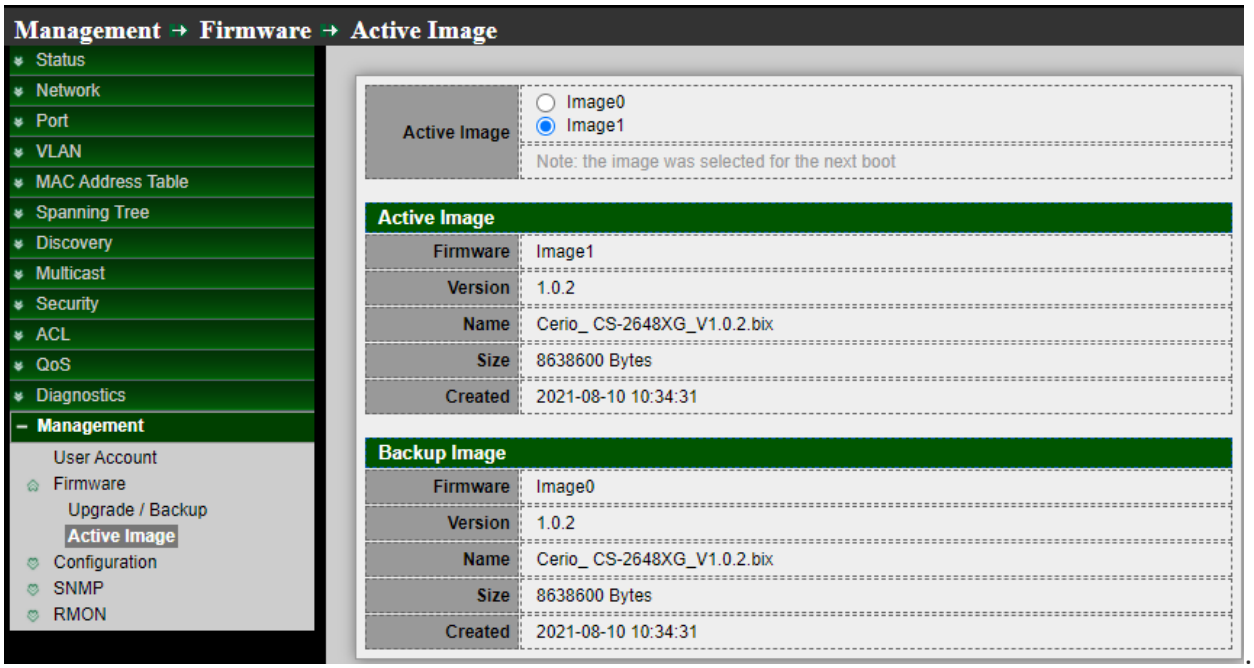


- **Action:** Firmware operations.
  - **Upgrade:** Upgrade firmware from remote host to DUT.
  - **Backup:** Backup firmware image from DUT to remote host.
- **Method:** Firmware upgrade / backup method.
  - **TFTP:** Using TFTP to upgrade/backup firmware.
  - **HTTP:** Using WEB browser to upgrade/backup firmware.
- **Firmware:** Firmware partition need to backup.
  - **Image0:** Firmware image in flash partition 0.
  - **Image1:** Firmware image in flash partition 1.
- **Address Type:** Specify TFTP server address type
  - **Hostname:** Use domain name as server address.
  - **IPv4:** Use IPv4 as server address.
  - **IPv6:** Use IPv6 as server address
- **Server Address:** Specify TFTP server address.
- **Filename:** Firmware image file name on remote TFTP server.

*Click the **"Apply"** button to save your changes settings.*

14.2.2 Active Image

This page allows user to select firmware image on next booting and show firmware information on both flash partitions, If the Switch has upload multiple firmware in system then administrator can choose a firmware to do system default start.



- **Active Image:** Select firmware image to use on next booting.
  - **Image0:** Select the flash partition 0 for Firmware image0 to active.
  - **Image1:** Select the flash partition 1 for Firmware image1 to active.

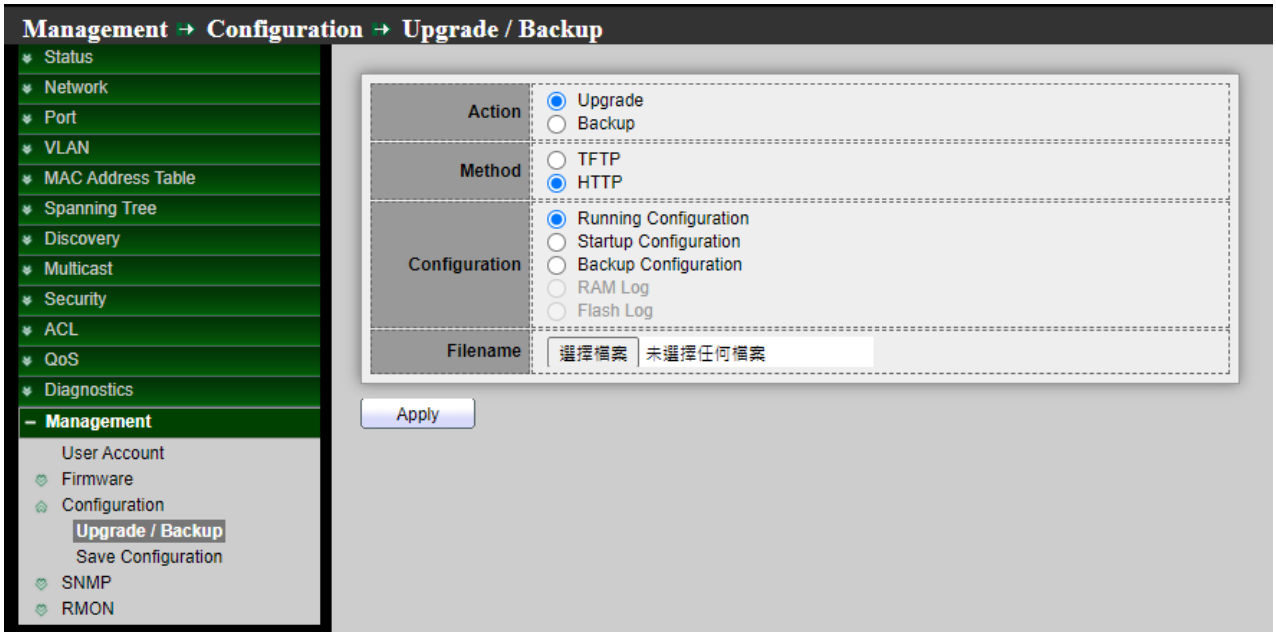
Field	Description
Active Image	• **Firmware:** Firmware image. • **Version:** Firmware version.. • Name: Firmware name. • **Size:** Firmware image size. • **Created:** Firmware image created date.
Backup Image	• **Firmware:** Firmware image. • **Version:** Firmware version.. • Name: Firmware name. • **Size:** Firmware image size. • **Created:** Firmware image created date.

*Click the **"Apply"** button to save your changes settings.*

14.3 Configuration

14.3.1 Upgrade / Backup

Administrator can backup system configuration file to PC or upload configuration file to Switch system, This page allow user to upgrade or backup firmware image through HTTP or TFTP server.



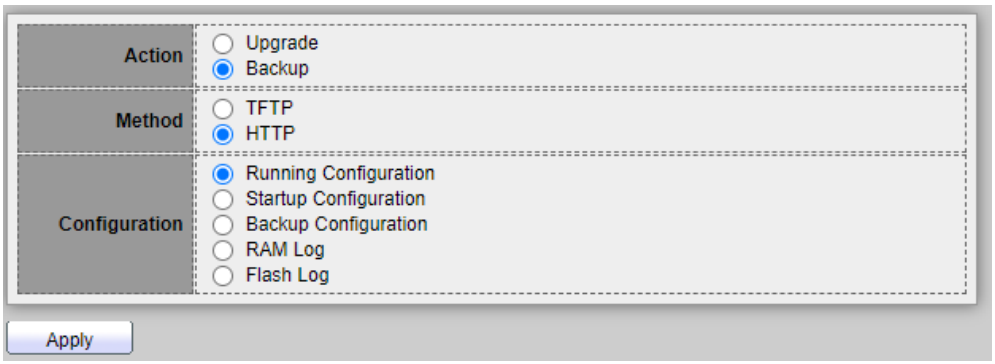
Upgrade Configuration

- **Action:** Configuration operations.
  - **Upgrade:** Upgrade firmware from remote host to DUT.
  - **Backup:** Backup firmware image from DUT to remote host.
- **Method:** Configuration upgrade method.
  - **TFTP:** Using TFTP to upgrade firmware.
  - **HTTP:** Using WEB browser to upgrade firmware.
- Configuration: Configuration Type.
  - **Running Configuration:** Merge to current running configuration file.
  - **Startup Configuration:** Replace startup configuration file.
  - **Backup Configuration:** Replace backup configuration file.
- **Address Type:** Specify TFTP server address type
  - **Hostname:** Use domain name as server address.
  - **IPv4:** Use IPv4 as server address.
  - **IPv6:** Use IPv6 as server address

- **Server Address:** Specify TFTP server address.
- **Filename:** Configuration file name on remote TFTP server.

*Click the **"Apply"** button to save your changes settings.*

Backup Configuration

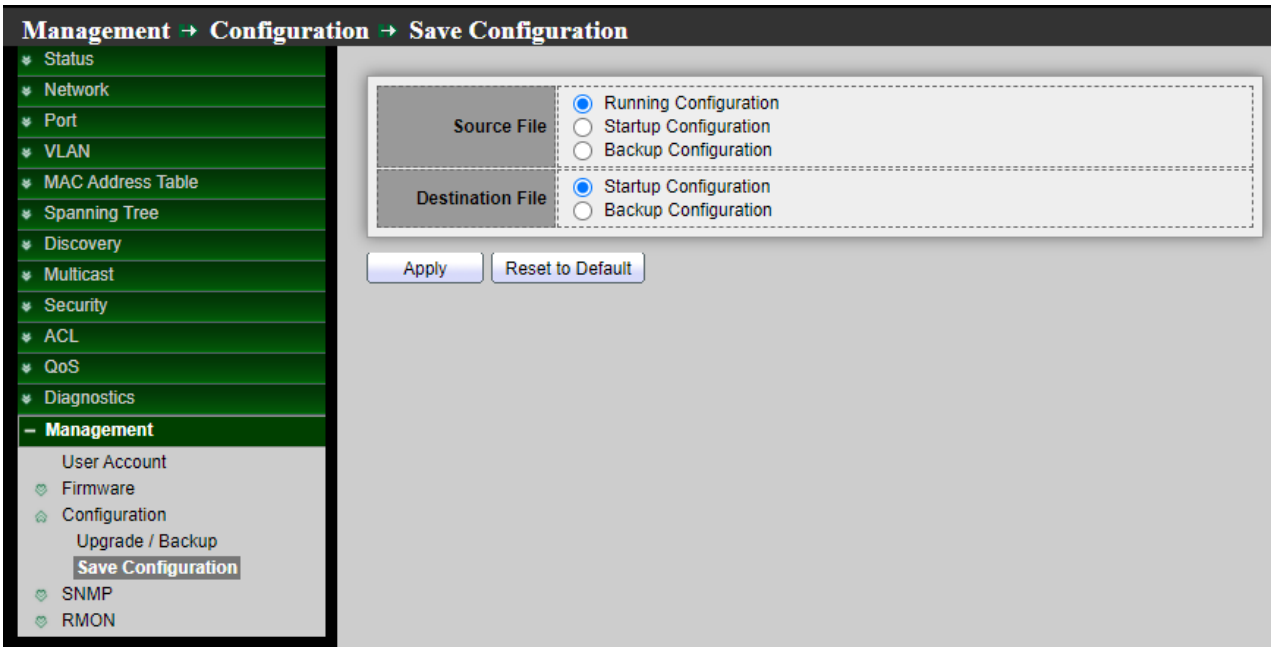


- **Action:** Configuration operations.
  - **Upgrade:** Upgrade firmware from remote host to DUT.
  - **Backup:** Backup firmware image from DUT to remote host.
- **Method:** Configuration backup method.
  - **TFTP:** Using TFTP to backup firmware.
  - **HTTP:** Using WEB browser to backup firmware.
- Configuration**:** Configuration Type.
  - **Running Configuration:** Backup running configuration file.
  - **Startup Configuration:** Backup start configuration file.
  - **Backup Configuration:** Backup backup configuration file.
  - **RAM Log:** Backup log file stored in RAM.
  - **Flash Log:** Backup log files store in Flash.

*Click the **"Apply"** button to save your changes settings.*

14.3.2 Save Configuration

When administrator to click Apply on any window, changes that you made to the switch configuration settings are stored only in the Running Configuration. To preserve the parameters in the Running Configuration, the Running Configuration must be copied to another configuration type or saved as a file on another device, This page allow user to manage configuration file saved on DUT and click “Restore Factory Default” button to restore factory defaults.



- **Source File:** Source file types
  - **Running Configuration:** Copy running configuration file to destination.
  - **Startup Configuration:** Copy startup configuration file to destination.
  - **Backup Configuration:** Copy backup configuration file to destination.
- **Destination File: Destination** file types.
  - **Startup Configuration:** Save file as startup configuration.
  - **Backup Configuration:** Save file as backup configuration.

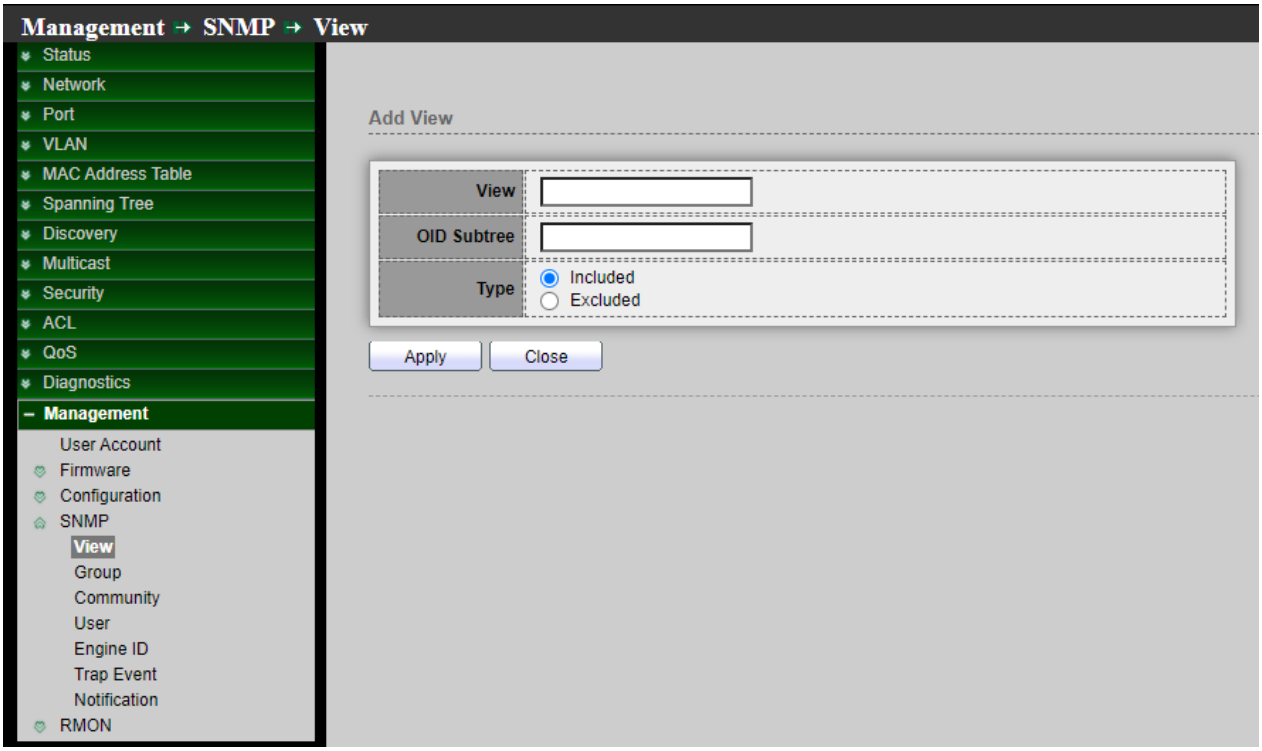
*Click the **“Apply”** button to save your changes or Chick “**Restore Factory Default**” the button to back to factory default setting.*

14.4 SNMP

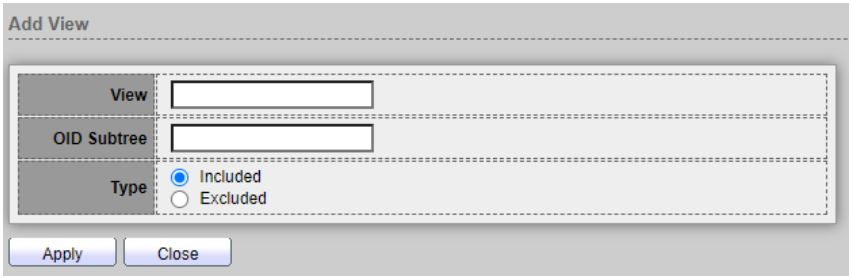
The SNMP supports SNMP v1, v2, and v3. It also reports system events to trap receivers using the traps defined in the Management Information Base (MIB) that it supports.

14.4.1 View

A view is a user-defined label for a collection of MIB tree subtrees. Each subtree ID is defined by the OID of the root of the relevant subtrees. You can either use well-known names to specify the root of the desired subtree or enter an OID. Setting **"add"** or **"Delete"** to management.



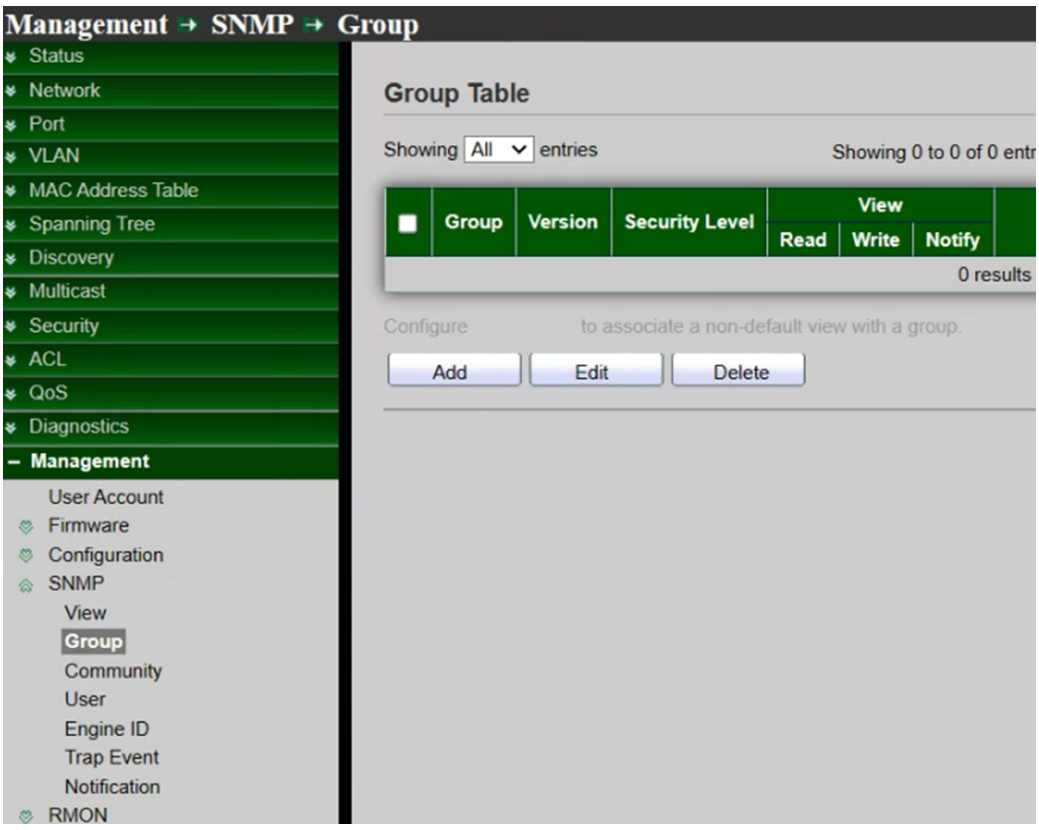
Field	Description
View	The SNMP view name. Its maximum length is 30 characters.
Subtree OID	Specify the ASN.1 subtree object identifier (OID) to be included or excluded from the SNMP view.
View Type	Include or exclude the selected MIBs in the view.



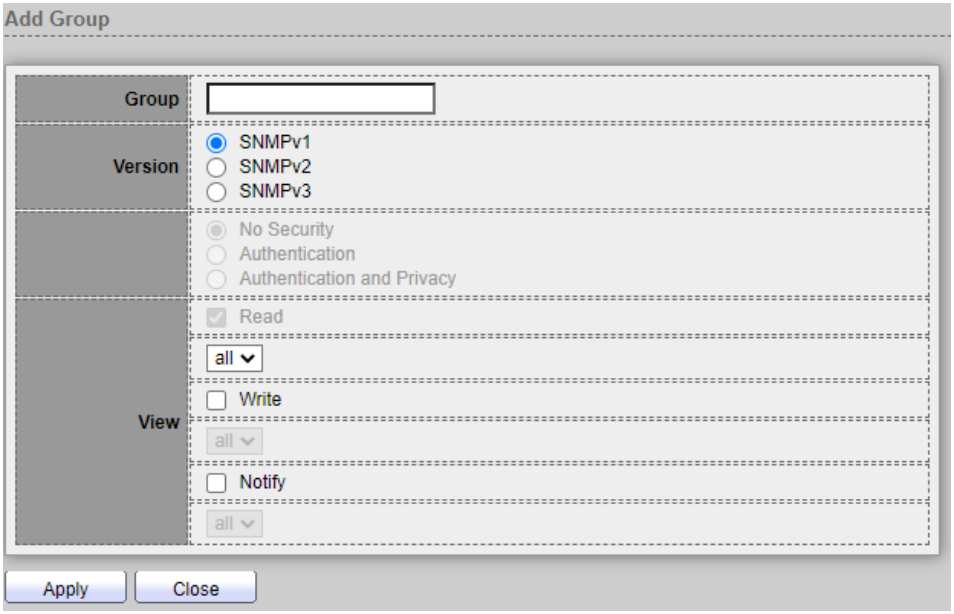
- **View:** Enter a unique view name.
- **Object Subtree:** Select User Defined to manually define an OID, or select an existing OID from the list. All descendent of this node will be included or excluded in the view.
- **Type:**
  Include: Check to include the selected MIBs in this view.
  Excluded: Check to Excluded the selected MIBs in this view.

14.4.2 Group

In SNMPv1 and SNMPv2, a community string is sent along with the SNMP frames. The community string acts as a password to gain access to an SNMP agent. However, neither the frames nor the community string are encrypted. So SNMPv1 and SNMPv2 are not secure. In SNMPv3 can configure Authentication and Privacy is more secure. Setting **"add"** and "Edit" and **"Delete"** function for this management



Field	Description
Group	Specify SNMP group name, and the maximum length is 30 characters.
Version	Spedify SNMP version • **SNMPv1:** SNMP Version 1. • **SNMPv2:** Community-based SNMP Version 2c. • **SNMPv3:** User security model SNMP version 3.
Security Level	Specify SNMP security level • **No Security :** Specify that no packet authentication is performed. • **Authentication:** Specify that no packet authentication without encryption performed. • **Authentication and Privacy:** Specify that no packet authentication with encryption is performed.
Version	Spedify SNMP version • **SNMPv1:** SNMP Version 1. • **SNMPv2:** Community-based SNMP Version 2c. • **SNMPv3:** User security model SNMP version 3.
Security Level	Specify SNMP security level • **No Security :** Specify that no packet authentication is performed. • **Authentication:** Specify that no packet authentication without encryption performed. • **Authentication and Privacy:** Specify that no packet authentication with encryption is performed.
View	Spedify SNMP version • **Read:** Group read view name.. • **Write:** Group write view name. • **Notify:** The view name that sends only traps with contents that is included in SNMP view selected for notification.
Read	Group read view name
Write	Group write view name.
Notify	The view name that sends only traps with contents that is included in SNMP view selected for notification.

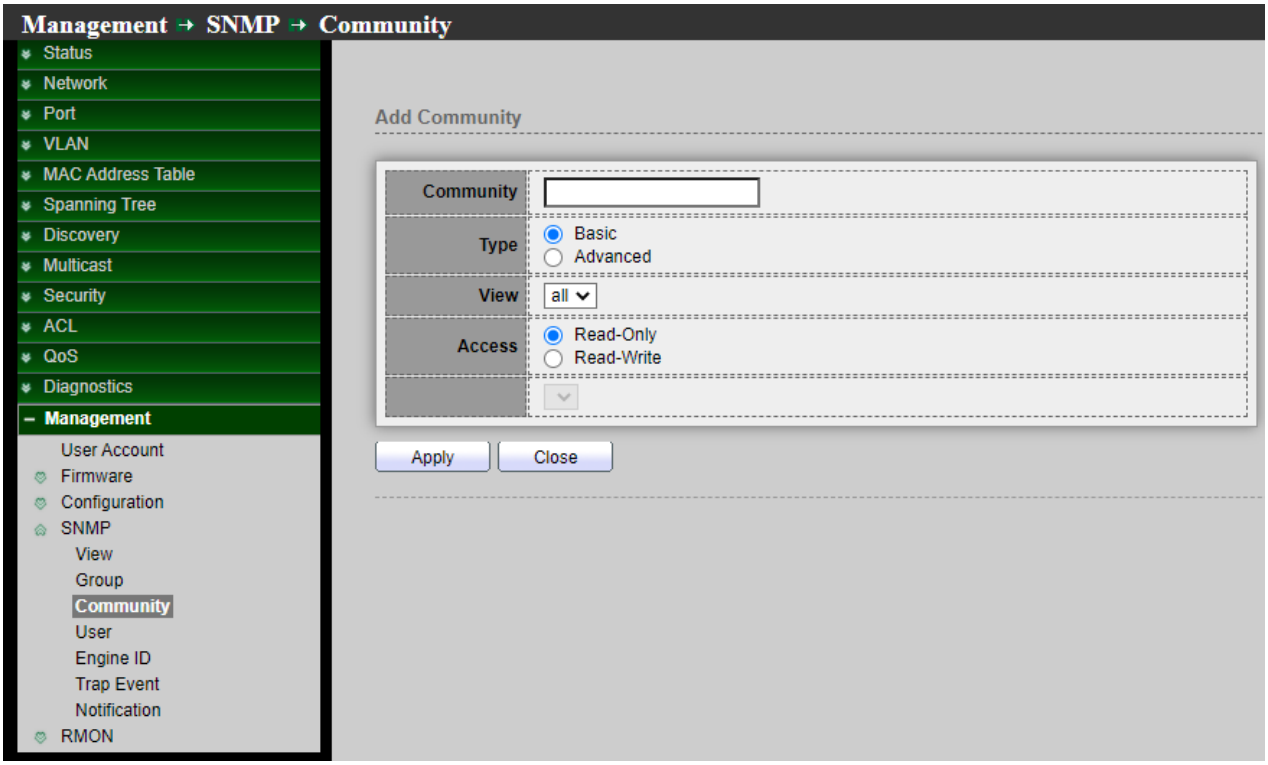


- **Group:** Specify SNMP group name, and the maximum length is 30 characters.
- **Version:** Specify SNMP version.
  - **SNMPv1:** SNMP Version 1.
  - **SNMPv2:** Community-based SNMP Version 2c.
  - **SNMPv3:** User security model SNMP version 3.
- **Security Level:** Specify SNMP security level.
  - **No Security :** Specify that no packet authentication is performed.
  - **Authentication:** Specify that no packet authentication without encryption is performed.
  - **Authentication and Privacy:** Specify that no packet authentication with entryption is performed.
- **View:**
  - **Read :** Select read view name if Read is checked.
  - **Write:** Select write view name, if Write is checked.
  - **Notify:** Select notify view name, if Notify is checked.

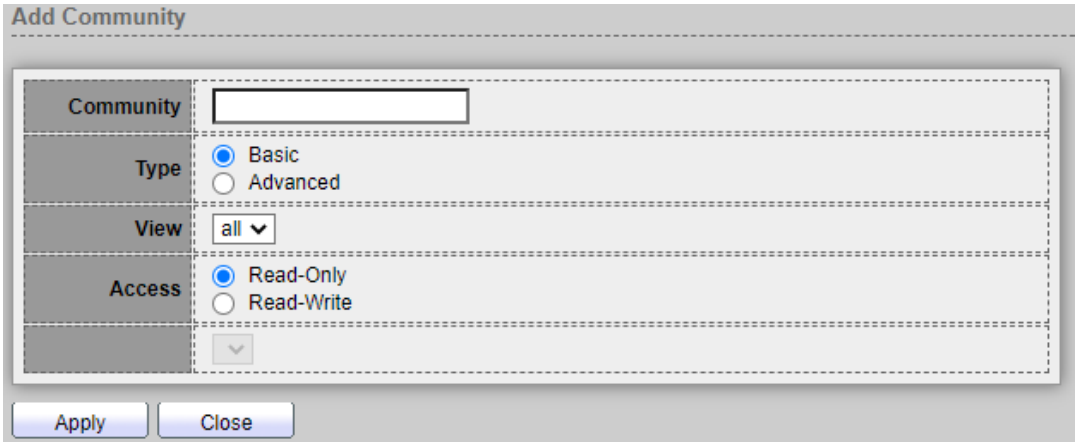
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

14.4.3 Community

Communities are only defined in SNMPv1 and v2 because SNMPv3 works with users instead of communities. The users belong to groups that have access rights assigned to them, Setting **"add"** and "Edit" and **"Delete"** function for this management.



Field	Description
Community	The SNMP community name. Its maximum length is 20 characters.
Community	SNMP Community mode. • **Basic:** snmp community specifies view and access right. • **Advanced:** snmp community specifies group.
Group	Specify the SNMP group configured by the command **SNMP group** to define the object available to the community.
View	Specify the SNMP view to define the object available to the community.
Access	SNMP access mode • **Read-Only:** Read only. • **Read-Write:** Read and write.



- **Community:** The SNMP community name. Its maximum length is 20 characters.
- **Type:** Specify SNMP version.
  - **Basic:** SNMP community specifies view and access right ,The access rights of a community can configure with Read Only or Read Write. In addition, Administrator can restrict the access to the community to only certain MIB objects by selecting a view.
  - **Advanced:** SNMP community specifies group, The access rights of a community are defined by a group. You can configure the group with a specific security model. The access rights of a group are Read, Write, and Notify.
  - **View:** Specify the SNMP view to define the object available to the community.
- **Access:** SNMP access mode.
  - **Read Only:** Read only , Management access is restricted to read-only. Changes cannot be made to the community.
  - **Read Write:** Read and write , Management access is read-write. Changes can be made to the switch configuration, but not to the community.
- **Group:** If set Type for specify SNMP version to "Advanced" type, Must be set specify the SNMP group configured by user to define the object available to the community.

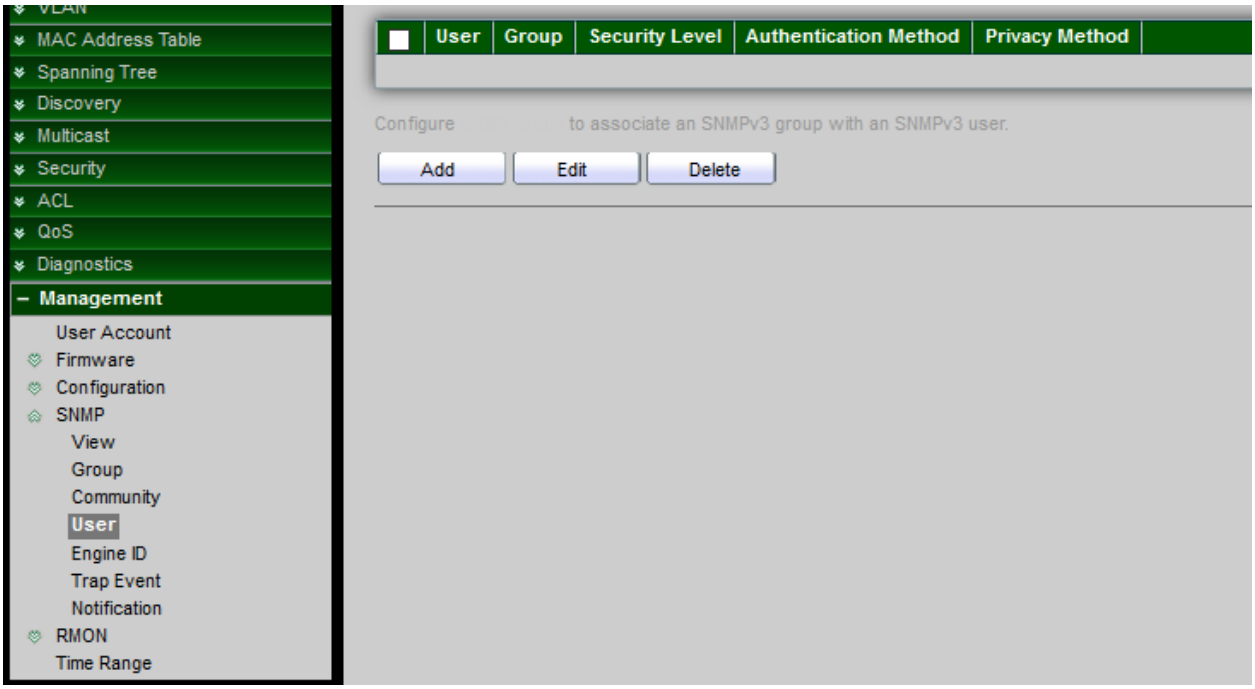
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

14.4.4 User

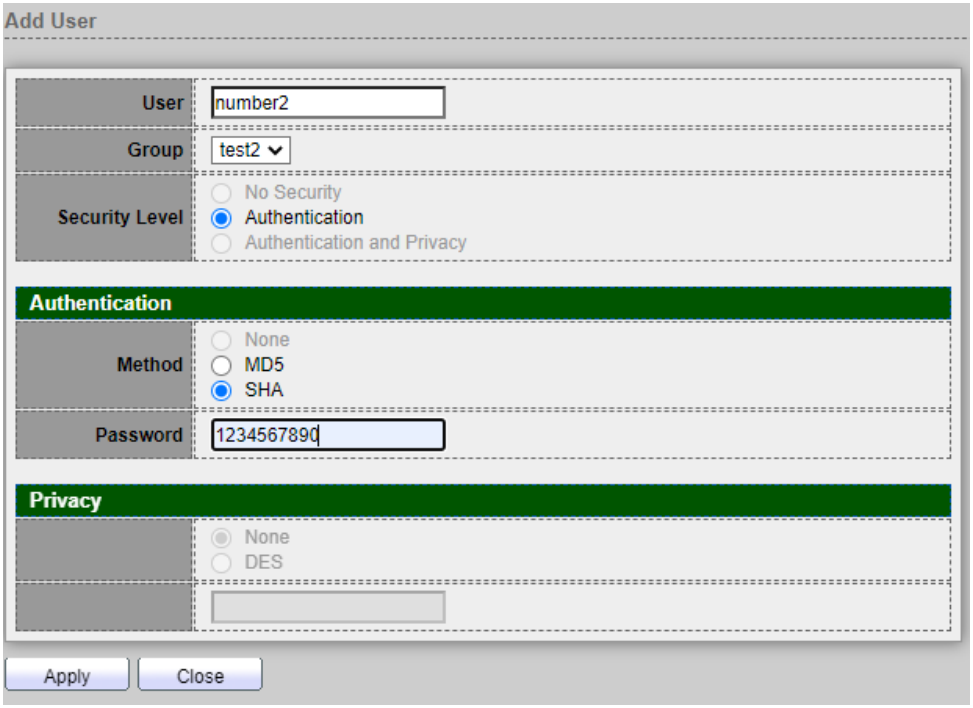
An SNMP user is defined by the login credentials (username, passwords, and authentication method) and by the context and scope in which it operates by association with a group and an Engine ID. The configured user has the attributes of its group, having the access privileges configured within the associated view.

Groups enable network managers to assign access rights to a group of users, instead of a single user. A user can only be a member of a single group.

Administrator need to create a SNMPv3 user, a SNMPv3 group must be available, Setting **"add"** and "Edit" and **"Delete"** function for this management.



Field	Description
User	Specify the SNMP user name on the host that connects to the SNMP agent. The max character is 30 characters. For the SNMP v1 or v2c, the user name must match the community name
Group	Specify the SNMP group to which the SNMP user belongs.
Security Level	SNMP privilege mode • **No Security :** Specify that no packet authentication is performed. • **Authentication:** Specify that no packet authentication without encryption is performed. • **Authentication and Privacy:** Specify that no packet authentication with encryption is performed.
Authentication Method	Authentication Protocol which is available when Privilege Mode is **Authentication** or **Authentication and Privacy**. • **None:** No authentication required. • **MD5:** Specify the HMAC-MD5-96 authentication protocol. • **SHA:** Specify the HMAC-SHA-96 authentication protocol.
Privacy Method	Encryption Protocol • **None:** No privacy required. • **DES:** DES gorithm



- **User:** Specify the SNMP user name on the host that connects to the SNMP agent. The max character is 30 characters.
- **Security Level:** SNMP privilege mode.
  - **No Security:** Specify that no packet authentication is performed.
  - **Authentication:** Specify that no packet authentication without encryption is performed.
  - **Authentication and Privacy:** Specify that no packet authentication with encryption is performed.

Authentication

- **Method:** Authentication Protocol which is available when Privilege Mode is Authentication or Authentication and Privacy**.**
  - **None:** No authentication required.
  - **MD5:** Specify the HMAC-MD5-96 authentication protocol.
  - **SHA:** Specify the HMAC-SHA-96 authentication protocol.
- **Password:** The authentication password, The number of character range is 8 to 32 characters.

Privacy

- **Method:** Encryption Protocol**.**
  - **None:** No privacy required.

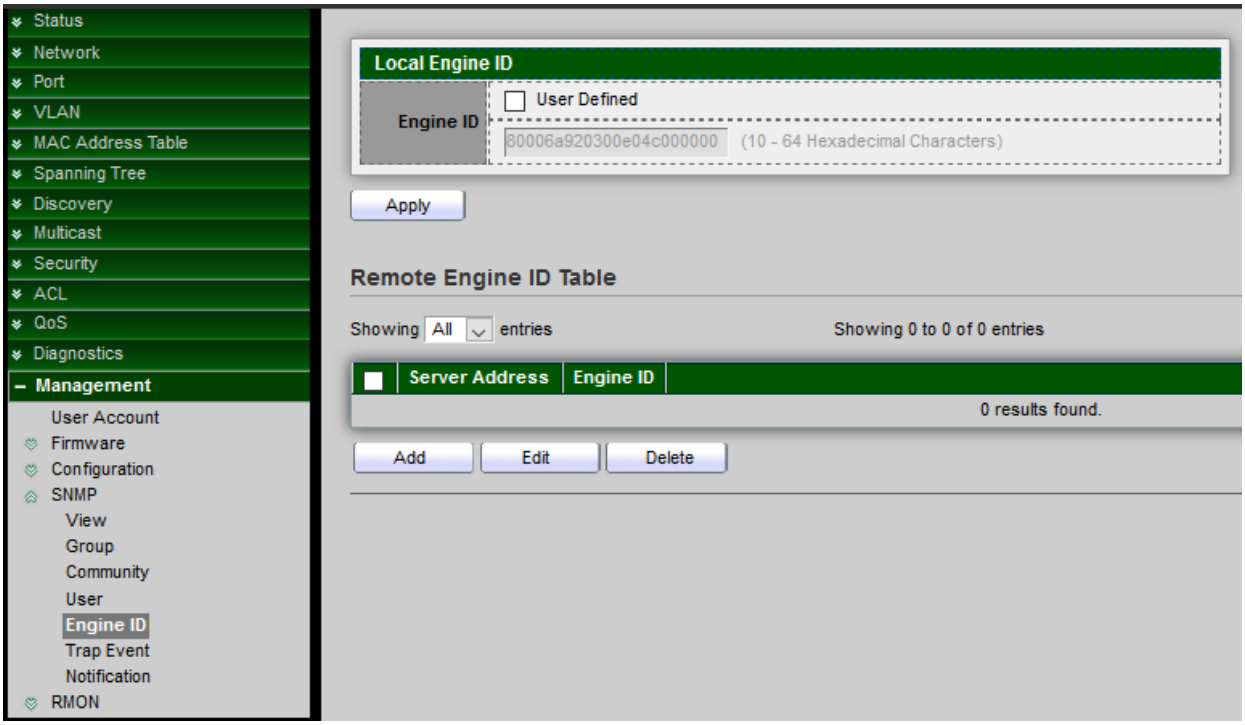
- **DES:** DES algorithm.
- **SHA:** Specify the HMAC-SHA-96 authentication protocol.

➢ **Password:** The privacy password, The number of character range is 8 to 64 characters.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

14.4.5 Engine ID

The Engine ID is only used by SNMPv3 entities to uniquely identify them. An SNMP agent is considered an authoritative SNMP engine. This means that the agent responds to incoming messages (Get, GetNext, GetBulk, Set), and sends trap messages to a manager.
Each SNMP agent maintains local information that is used in SNMPv3 message exchanges. The default SNMP Engine ID is comprised of the enterprise number and the default MAC address. The SNMP Engine ID must be unique for the administrative domain, so that no two devices in a network have the same Engine ID, Setting **"add"** and "Edit" and **"Delete"** function for this management.



Local Engine ID

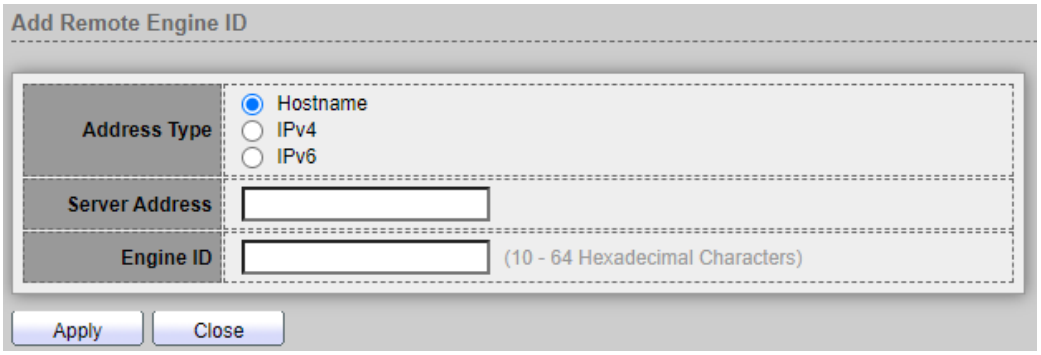
➢ **Engine ID:** If checked "User Defined", the local engine ID is configure by user, else use the default Engine ID which is made up of MAC and Enterprise ID**,** The user defined engine ID is range 10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.

*Click the **"Apply"** button to save your changes settings.*

Remote Engine ID Table

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

Field	Description
Server Address	Remote host.
Engine ID	Specify Remote SNMP engine ID. The engine ID is range10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.



- **Address Type:** Remote host address type for Hostname/IPv4/IPv6.
- **Server Address:** Remote host.
- **Engine ID:** Specify Remote SNMP engine ID. The engine ID is range10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

14.4.6 Trap Event

Administrator can choose SNMP Trap Event Type to monitor

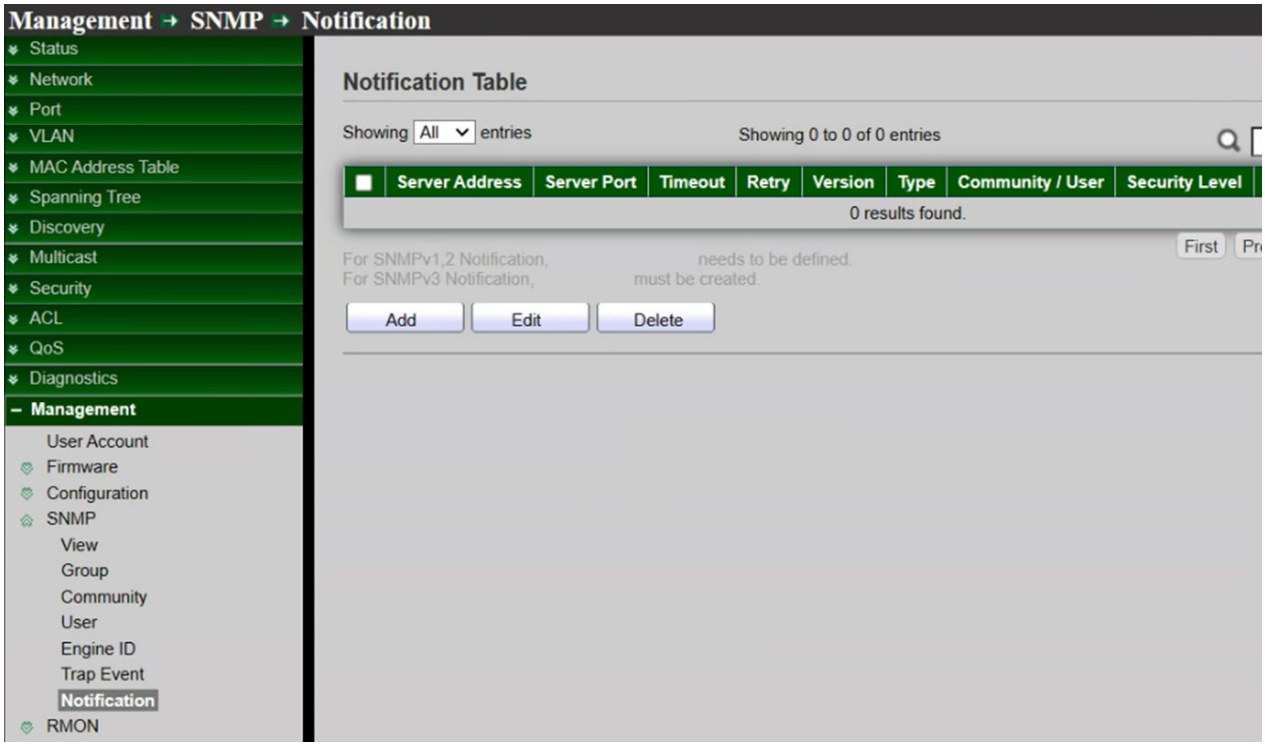
Trap messages are generated to report system events, as defined in RFC 1215. The system can generate traps defined in the MIB that it supports.

Field	Description
Authentication Failure	SNMP authentication failure trap, when community not match or user authentication password not match.
Link Up/Down	Port link up or down trap
Cold Start	Device reboot configure by user trap
Warm Start	Device reboot by power down trap

*Click the **"Apply"** button to save your changes settings.*

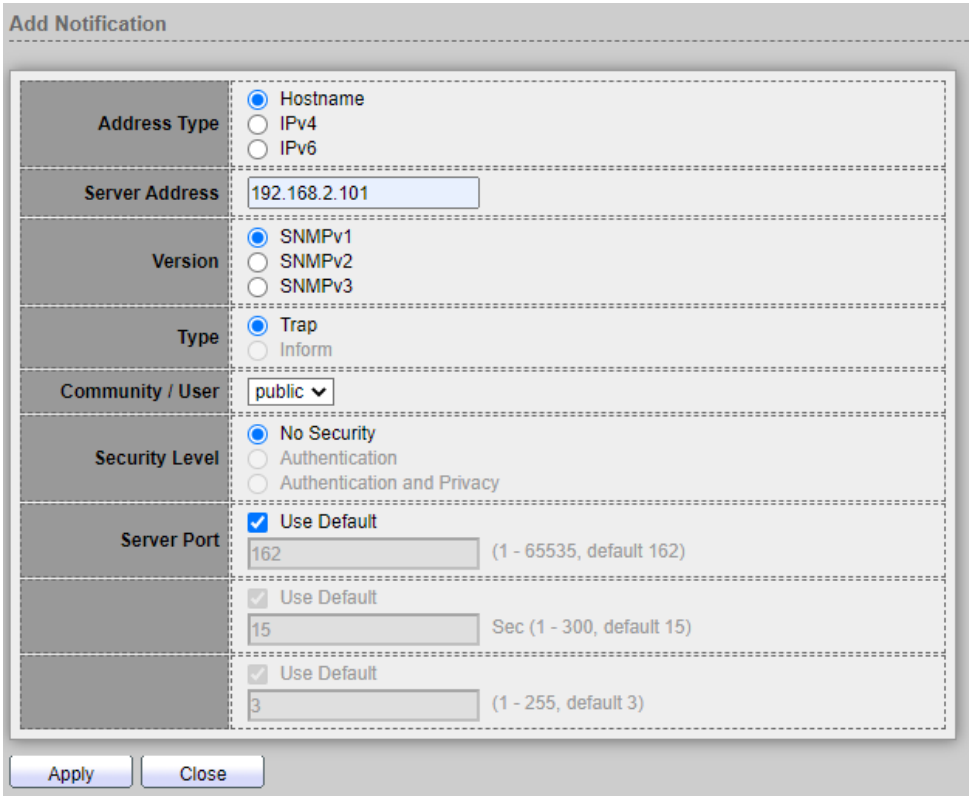
14.4.7 Notification

Notification is network nodes where the trap messages are sent by the switch. A list of notification recipients are defined as the targets of trap messages. A trap receiver entry contains the IP address of the node and the SNMP credentials corresponding to the version that will be included in the trap message. When an event arises that requires a trap message to be sent, it is sent to every node listed in the Notification Recipient Table, , Setting **"add"** and "Edit" and **"Delete"** function for this management.



Field	Description
Server Address	IP address or the hostname of the SNMP trap recipients.
Server Port	Recipients server UDP port number
Timeout	Specify the SNMP informs timeout
Retry	Specify the retry counter of the SNMP informs.
Version	Specify SNMP notification version • **SNMPv1:** SNMP Version 1 notification. • **SNMPv2:** SNMP Version 2 notification. • **SNMPv3:** SNMP Version 3 notification.

Type	Notification Type • **Trap:** Send SNMP traps to the host. • **Inform:** Send SNMP informs to the host.
Community/User	SNMP community/user name for notification. If version is SNMPv3 the name is user name, else is community name
UDP Port	Specify the UDP port number.
Timeout	Specify the SNMP informs timeout
Security Level	SNMP trap packet security level • **No Security:** Specify that no packet authentication is performed. • **Authentication:** Specify that no packet authentication without encryption is performed. • **Authentication and Privacy:** Specify that no packet authentication with



- **Address Type:** Remote host address type for Hostname/IPv4/IPv6.
- **Server Address:** IP address or the hostname of the SNMP trap recipients.
- **Version:** Specify SNMP notification version.

- **SNMPv1:** SNMP Version 1 notification.
- **SNMPv2:** SNMP Version 2 notification.
- **SNMPv3:** SNMP Version 3 notification.

➢ **Type:** Notification Type**.**
- **Trap:** Send SNMP traps to the host.
- **Inform:** Send SNMP informs to the host.(version 1 have no inform).

➢ **Community/User:** SNMP community/user name for notification. If version is SNMPv3 the name is user name, else is community name.

➢ **Security Level:** SNMP notification packet security level, the security level must less than or equal to the community/user name**.**
- **No Security:** Specify that no packet authentication is performed.
- **Authentication:** Specify that no packet authentication without encryption is performed.
- Authentication and Privacy: Specify that no packet authentication with encryption is performed.

➢ **Server Port:** Recipients server UDP port number, if "use default" checked the value is 162, else user configure.

➢ **Timeout:** Specify the SNMP informs timeout, if "use default" checked the value is 15, else user configure.

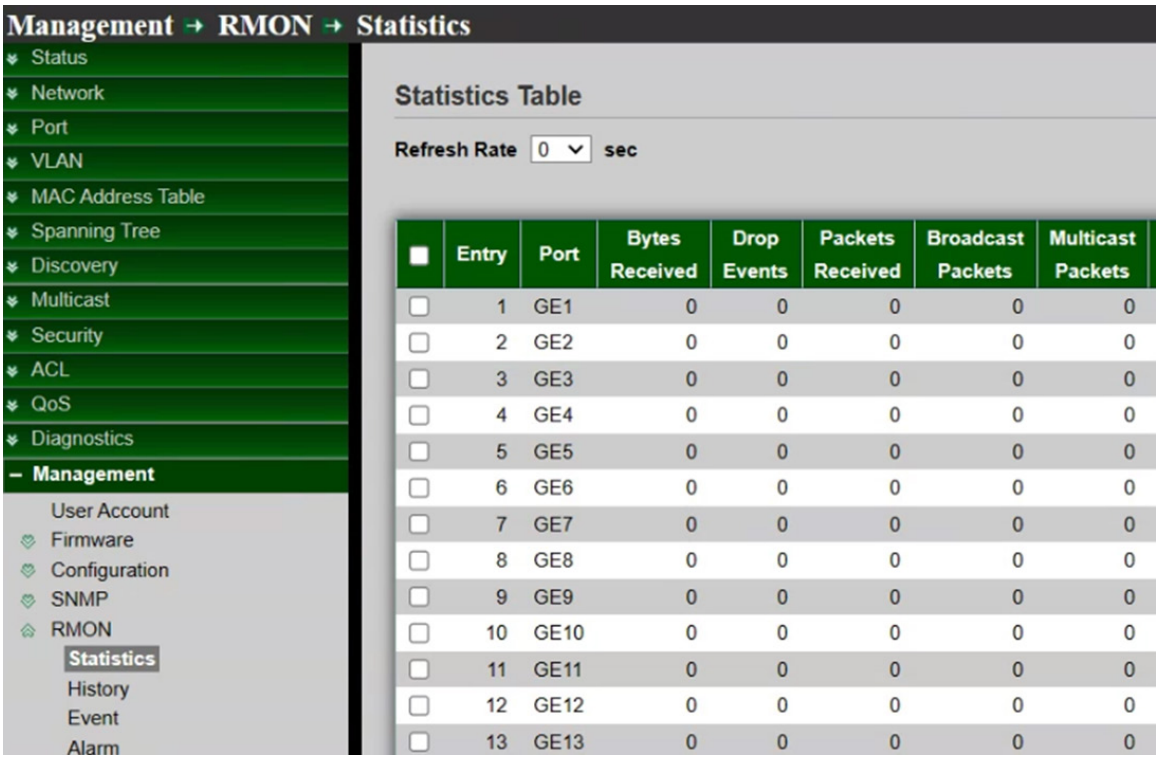
➢ **Retry:** Specify the SNMP informs retry count, if "use default" checked the value is 3, else user configure.

*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

14.5 RMON

14.5.1 Statistics

The page displays traffic statistics per interface. The refresh rate of the information can be selected. This page is useful for analyzing the amount of traffic that is both sent and received and its dispersion (Unicast, Multicast, and Broadcast) *Click the **"Clear"** button to clear this page or click the **"Refresh"** button to refresh and chick the **"View"** button to view the page .*



Entry	Port	Bytes Received	Drop Events	Packets Received	Broadcast Packets	Multicast Packets
1	GE1	0	0	0	0	0
2	GE2	0	0	0	0	0
3	GE3	0	0	0	0	0
4	GE4	0	0	0	0	0
5	GE5	0	0	0	0	0
6	GE6	0	0	0	0	0
7	GE7	0	0	0	0	0
8	GE8	0	0	0	0	0
9	GE9	0	0	0	0	0
10	GE10	0	0	0	0	0
11	GE11	0	0	0	0	0
12	GE12	0	0	0	0	0
13	GE13	0	0	0	0	0

Statistics Table

Refresh Rate 0 sec

Entry	Port	Bytes Received	Drop Events	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Oversize Packets	Fragments
1	GE1	491071	0	2953	458	545	0	0	0	0
2	GE2	0	0	0	0	0	0	0	0	0
3	GE3	0	0	0	0	0	0	0	0	0
4	GE4	0	0	0	0	0	0	0	0	0
5	GE5	0	0	0	0	0	0	0	0	0
6	GE6	0	0	0	0	0	0	0	0	0
7	GE7	0	0	0	0	0	0	0	0	0
8	GE8	0	0	0	0	0	0	0	0	0

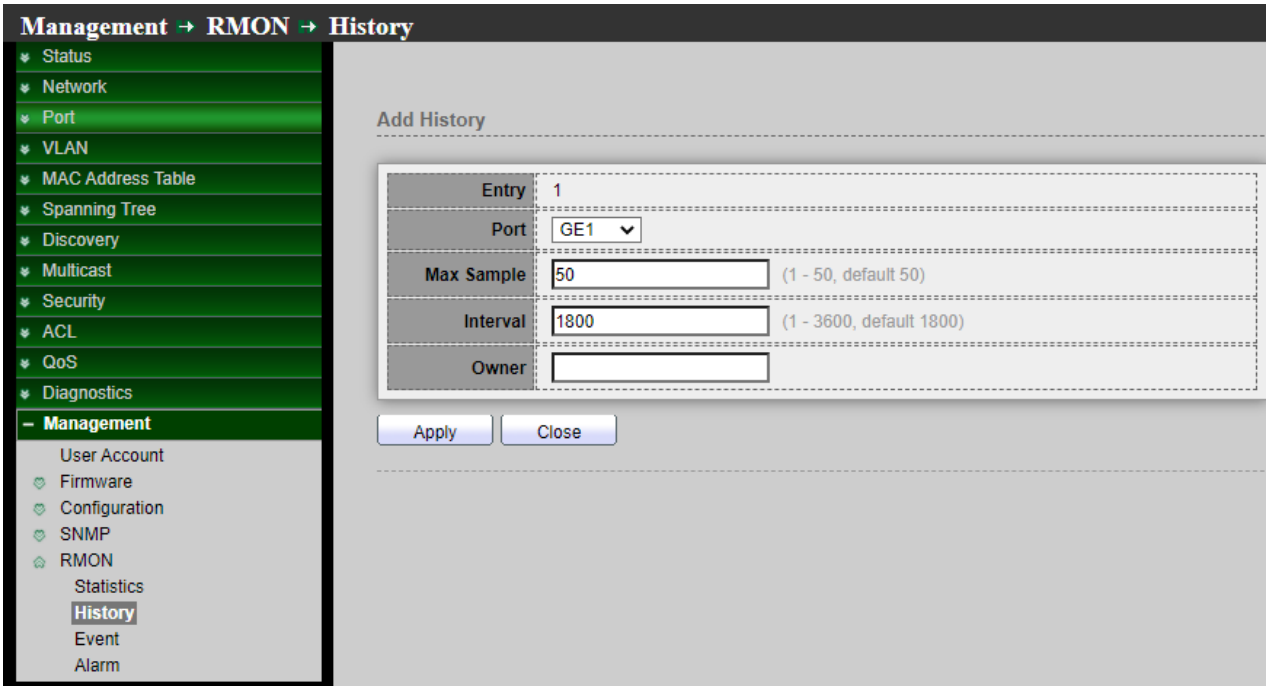
Jabbers	Collisions	Frames of 64 Bytes	Frames of 65 to 127 Bytes	Frames of 128 to 255 Bytes	Frames of 256 to 511 Bytes	Frames of 512 to 1023 Bytes	Frames Greater than 1024 Bytes
0	0	1215	1044	237	7	442	8
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Field	Description
Port	The port for the RMON statistics.
Bytes Received	Number of octets received, including bad packets and FCS octets, but excluding framing bits.
Drop Events	Number of packets that were dropped.
Packets Received	Number of packets received, including bad packets, Multicast packets, and Broadcast packets.
Broadcast Packets	Number of good Broadcast packets received. This number does not include Multicast packets.
Multicast Packets	Number of good Multicast packets received.
CRC & Align Errors	Number of CRC and Align errors that have occurred.
Undersize Packages	Number of undersized packets (less than 64 octets) received.
Oversize Packages	Number of oversized packets (over 1518 octets) received.
Fragments	Number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) eceived.
Jabbers	Number of received packets that were longer than 1632 octets. This number excludes frame bits, but includes FCS octets that had either a bad FCS (Frame Check Sequence) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. A Jabber packet is defined as an Ethernet frame that satisfies the following criteria: • Packet data length is greater than MRU. • Packet has an invalid CRC. • RX error event has not been detected.
Collision	Number of collisions received. If Jumbo Frames are enabled, the threshold of Jabber Frames is raised to the maximum size of Jumbo Frames.
Frames of 64 Bytes	Number of frames, containing 64 bytes that were received.
Frames of 65 to 127 Bytes	Number of frames, containing 65 to 127 bytes that were received.

Frames of 128 to 255 Bytes	Number of frames, containing 128 to 255 bytes that were received.
Frames of 256 to 511 Bytes	Number of frames, containing 256 to 511 bytes that were received.
Frames of 512 to 1024 Bytes	Number of frames, containing 512 to 1023 bytes that were received.
FramesGreater than 1024 Bytes	Number of frames, containing 1024 to 1518 bytes that were received

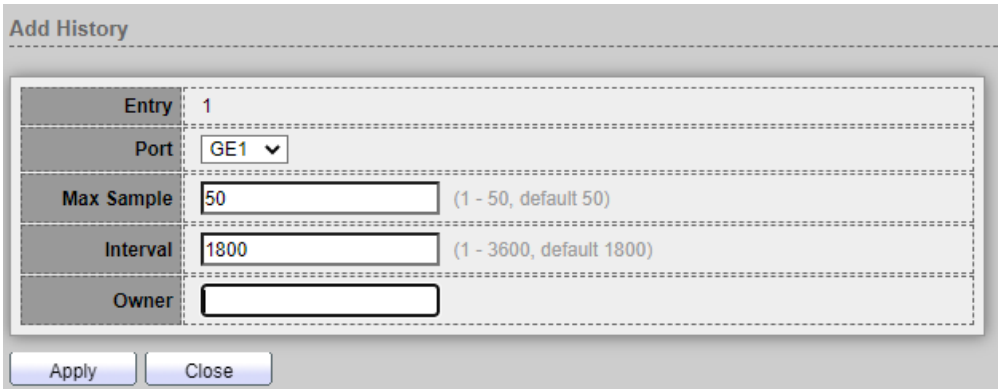
14.5.2 History

Use the History Control Table page to define the sampling frequency, amount of samples to store, and the interface from where to gather the data. After the data is sampled and stored, it appears on the History Table page that can be viewed by clicking History Table, , Setting **"add"** and "Edit" and **"Delete"** and "View" function for this management.



Field	Description
Port	The port for the RMON history.

Interval	The number of seconds for each sample.
Owner	The owner name of event (0~31 characters).
Sample	The maximum number of buckets. • **Maximum :** The maximum number of buckets. • **Current:** The current number of buckets.

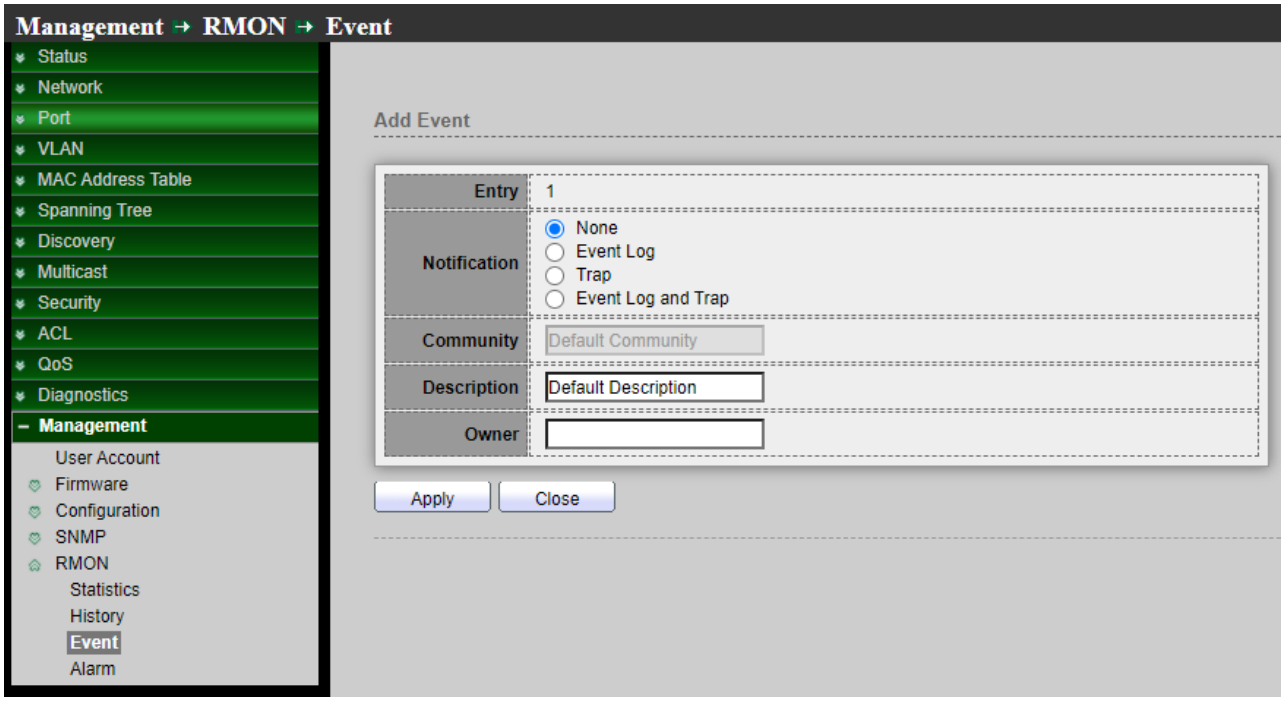


- **Port:** Select ports for the configure.
- **Max Sample:** Specify the maximum number of buckets.
- **Interval:** Enter the time in seconds that samples were collected from the interface, Specify the number of seconds for each sample
- **Owner:** Enter the RMON station or user that requested the RMON information, Specify the owner name of event (0~31 characters).

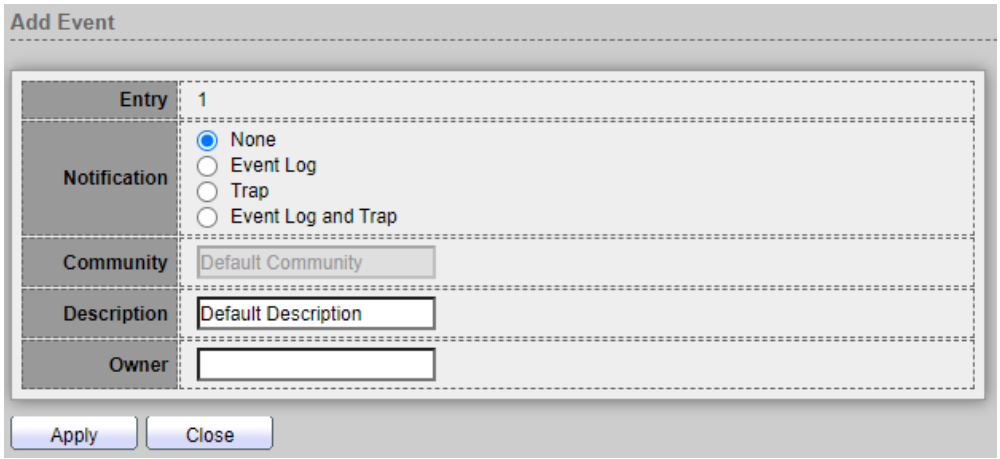
*Click the **"Apply"** button to save your changes or **"Close"** the button to close settings.*

14.5.3 Event

Events page to configure events that are actions performed when an alarm is generated (alarms are defined on the Alarms page). An event can be any combination of logs and traps. If the action includes logging of the events, they are displayed on the Event Log Table page, Setting **"add"** and "Edit" and **"Delete"** and "View" function for this management.



Field	Description
Port	Specify port for the RMON history.
Max Sample	Specify the maximum number of buckets.
Interval	Specify the number of seconds for each sample.
Owner	Specify the owner name of event (0~31 characters).

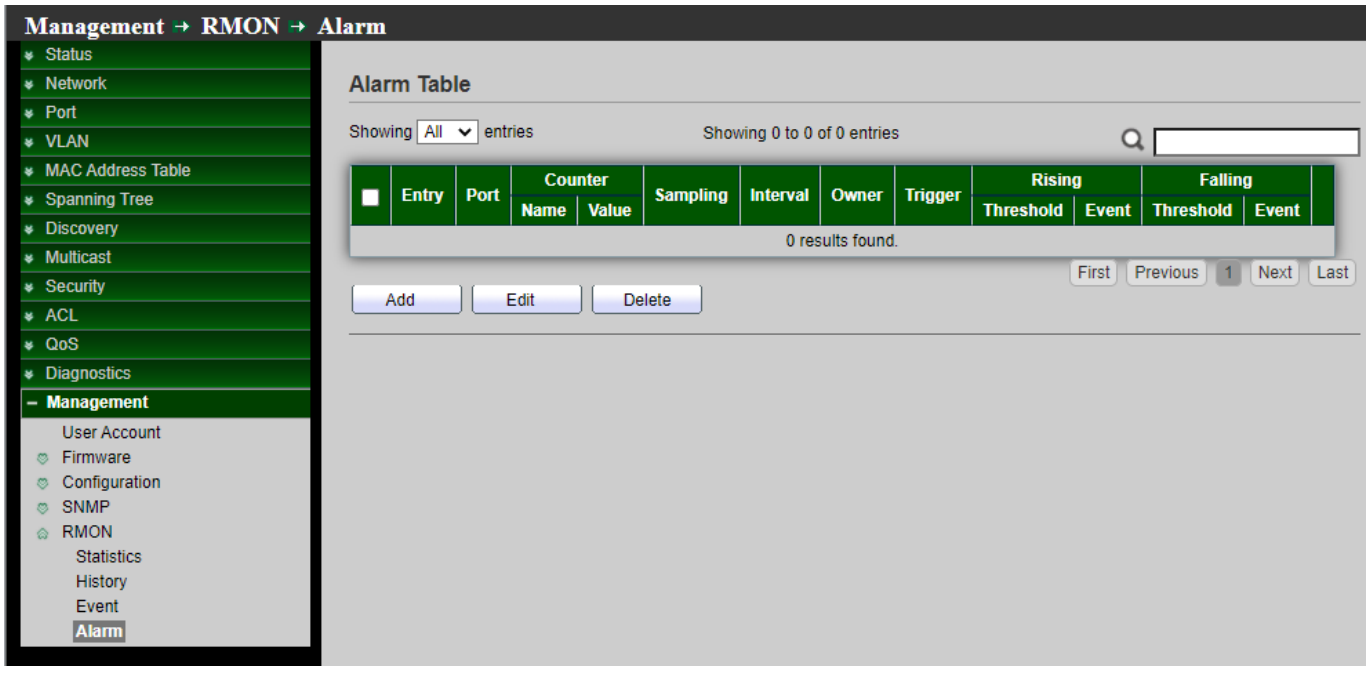


- **Community:** The SNMP community name. Its maximum length is 20 characters.
- **Notification:** Specify the notification type for the event, and the possible value are.
  - **None:** Nothing for notification.
  - **Event Log:** Logging the event in the RMON Event Log table.
  - **Trap:** Send a SNMP trap.
  - **Event Log and Trap:** Logging the event and send the SNMP trap
- **Community:** Specify the SNMP community when the notification type is specified as “Trap” and “Event Log and Trap”.
- **Description:** Specify the description for the event.
- **Owner:** Specify owner for the event.

*Click the **“Apply”** button to save your changes or **“Close”** the button to close settings.*

14.5.4 Alarm

RMON alarms provide a mechanism for setting thresholds and sampling intervals to generate exception events on any counter or any other SNMP object counter maintained by the agent. Both the rising and falling thresholds must be configured in the alarm. After a rising threshold is crossed, no rising events are generated until the companion falling threshold is crossed. After a falling alarm is issued, the next alarm is issued when a rising threshold is crossed, Setting **“add”** and “Edit” and **“Delete”** function for this management.



Field	Description
Port	The port configuration for the RMON alarm.
Counter	The counter for sampling • **DropEvents (Drop Event)**: Total number of events received in which the packets were dropped. • **Octes (Received Bytes)**: Octets. • **Pkts (Received Packets):** Number of packets. • **BroadcastPkts (Broadcast Packets Received)**: Broadcast packets. • **MulticastPkts (Multicast Packets Received)**: Multicast packets. • **CRCAlignError (CRC and Align Error)**: CRC alignment error. • **UndersizePkts (Undersize Packets)**: Number of undersized packets. • **OversizePkts (Oversize Packets)**: Number of oversized packets. • **Fragments (Fragments)**: Total number of packet fragment. • **Jabbers (Jabbers)**: Total number of packet jabber. • **Collisions (Collisions)**: Collision. • **Pkts64Octetes (Frames of 64 Bytes)**: Number of packets size 64 octets. • **Pkts65to127Octetes (Frames of 65 to 127 Bytes)**: Number of packets size 65 to 127 octets. • **Pkts128to255Octetes (Frames of 128 to 255 Bytes)**: Number of packets size 128 to 255 octets. • **Pkts256to511Octetes (Frames of 256 to 511 Bytes)**: Number of packets size 256 to 511 octets. • **Pkts512to1023Octetes (Frames of 512 to 1023 Bytes)**: Number of packets size 512 to 1023 octets. • **Pkts1024to1518Octets (Frames Greater than 1024 Bytes)**: Number of packets size 1024 to 1518 octets.
Version	The sampling type including: • **Absolute:** The selected variable value is compared directly with the thresholds at the end of the sampling interval • **Delta:** The selected variable value of the last sample is subtracted from the current value and the difference is compared with the thresholds.
Interval	The number of seconds for each sample.
Owner	The owner for the alarm entry.

Trigger	The type of event triggering.
Rising Threshold	The threshold for firing rising event.
Rising Event	The rising event when alarm was fired.
Falling Threshold	The threshold for firing falling event.
Falling Event	The falling event when alarm was fired.