GS-5424PLX

User Manual

09-2020 / v1.0

Edimax Technology Co., Ltd.
No. 278, Xinhu 1st Rd., Neihu Dist., Taipei City, Taiwan
Email: support@edimax.com.tw

Edimax Technology Europe B.V.
Fijenhof 2, 5652 AE Eindhoven, The Netherlands
Email: support@edimax.nl

Edimax Computer Company
3444 De La Cruz Blvd., Santa Clara, CA 95054, USA
Email: support@edimax.com

Contents

I Product Information

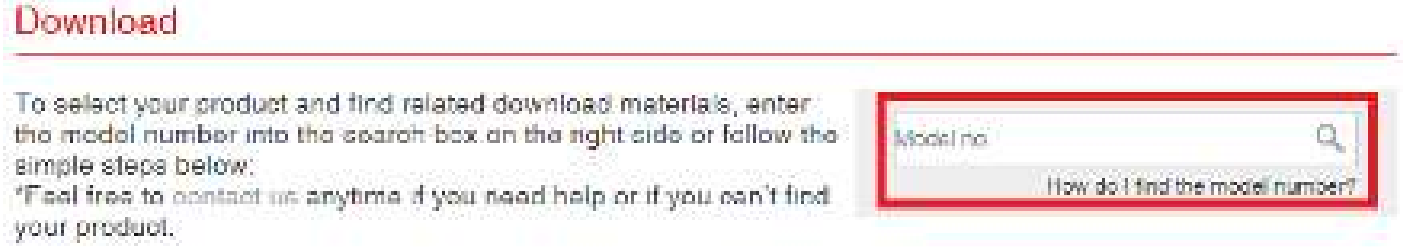
The EDIMAX GS-5424PLX long-range web-smart switch comes with a web based user interface, equipped with 24 Gigabit PoE+ ports, and SFP+ ports for 10 Gigabit uplinks and long-range copper or optical connections.

The 10 GbE connectivity fully utilizes the power of your office networking for demanding tasks, such as data backup, video conferencing, IP surveillance, high volume transaction processing, large file transferring, and more.

You can find all supporting documents from the link below or via QR Code:

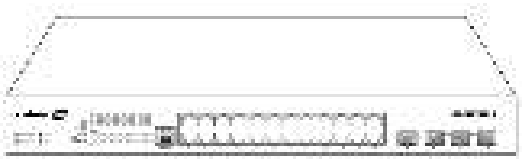
https://www.edimax.com/download

(Once you've visited the Edimax official website, please enter the model no. "GS-5424PLX" into the search box to search for your product.)



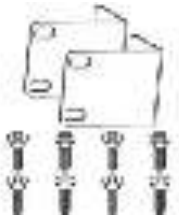
I-1 Package Content

Before start using this product, please check if there is anything missing in the package, and contact your dealer to claim the missing item(s):



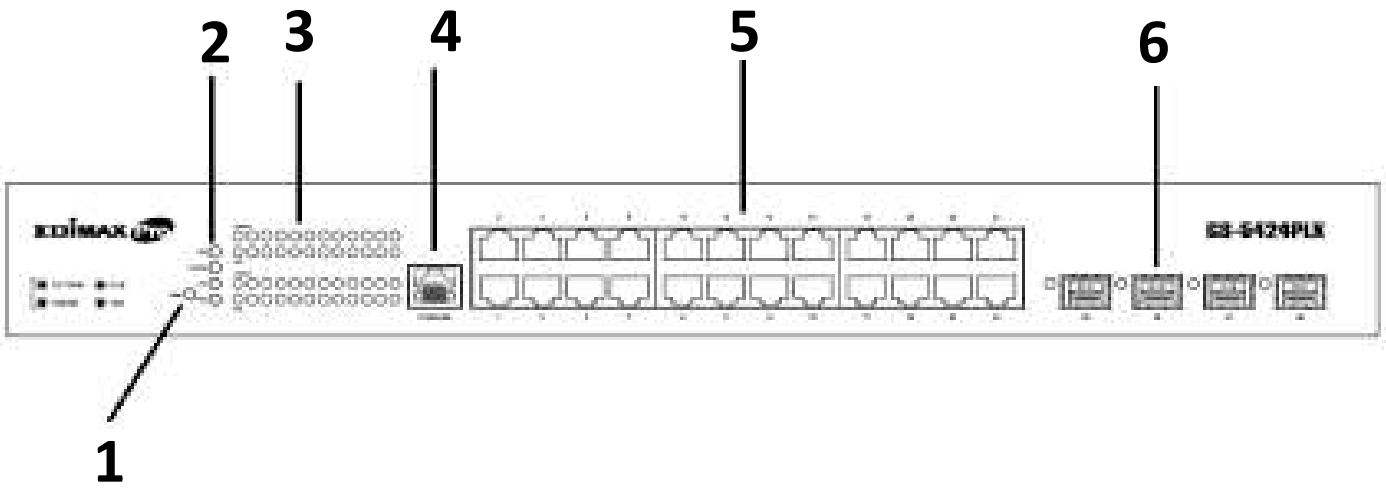
GS-5424PLX

GS-5424PLX



Power Cord

I-2 Hardware Overview



No.	Descriptions
1	Reset button
2	LED (ALM, PoE/MAX, SYS, PWR
3	LED (Link/Act)
4	CONSOLE port
5	PoE Ports (1~24)
6	SFP+ Ports (25~28)

I-3 LED Status

Function	Status	Description
PWR	On (**Green**)	Power on
	Off	Power off
Alert	On (**Red**)	System fault detected. (System failure due to overheating of switch or wrong voltage)
	Off	No faults detected
PoE/Max	On (**Green**)	Over PoE max power
	Off	Under PoE max power
Link/ACT (1-24 port)	On (**Green**)	Link at 1000M
	On (**Amber**)	Link at 10/100M
	Blinking	Sending or receiving data
	Off	Port disconnected or link fail
SFP+ (25-28 port)	On (**Blue**)	10G link
	On (**Green**)	1000M link
	Blinking	Data transmitting
	Off	Port disconnected or link fail
PoE	On (**Green**)	PoE power output on
	Blinking	PoE power output over 30W
	Off	PoE power output off

II Installation

This chapter describes how to install and connect your Edimax Switch. Read the following topics and perform the procedures in the correct order. Incorrect installation may cause damage to the product.

II-1 Mounting the Switch

There are two ways to physically set up the switch.

- Place the switch on a flat surface. To place the switch on a desktop, install the four rubber feet (included) on the bottom of the switch.
- Mount the switch in a standard rack (1 rack unit high).

II-1-1 Placement Tips

- Ambient Temperature — To prevent the switch from overheating, do not operate it in an area that exceeds an ambient temperature of 122°F (50°C).
- Air Flow — Be sure that there is adequate air flow around the switch.
- Mechanical Loading — Be sure that the switch is level and stable to avoid any hazardous conditions.
- Circuit Overloading — Adding the switch to the power outlet must not overload that circuit.

Follow these guidelines to install the switch securely.

- Put the switch in a stable place such as a desktop, to avoid it falling.
- Ensure the switch works in the proper AC input range and matches the voltage labeled.
- Ensure there is proper heat dissipation from and adequate ventilation around the switch.
- Ensure the switch's location can support the weight of the switch and its accessories.

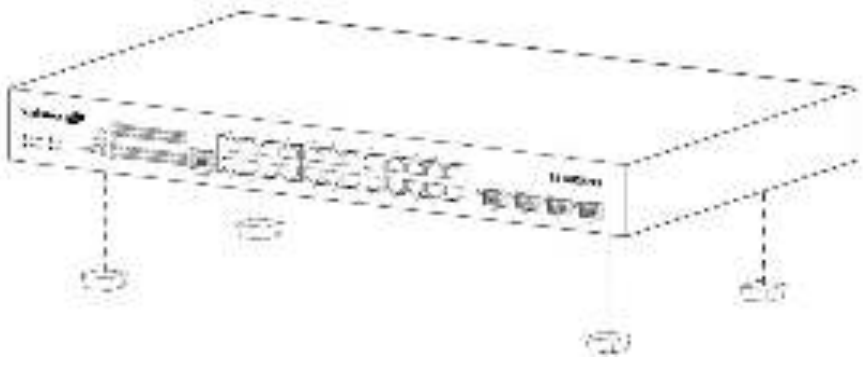


Figure 4 - Desktop Installation

II-1-2 Rack Mounting

You can mount the switch in any standard size, 19-inch (about 48 cm) wide rack. The switch requires 1 rack unit (RU) of space, which is 1.75 inches (44.45 mm) high.

For stability, load the rack from the bottom to the top, with the heaviest devices on the bottom. A top-heavy rack is likely to be unstable and may tip over.

When mounting smaller switch products into a standard 19-inch rack, a pair of extension brackets (sometimes referred to as ears) are needed to adapt the switch to the rack size.

These extension brackets are mounted on the switch using the screws provided in the kit, and have two holes that are used to then screw the switch into the rack.

An example of one type of these extension brackets is shown in the following figure.

A common problem that occurs during rack mounting is the distance between the screw holes on the rack. Some racks are made with a uniform distance between all of the holes, and others have the holes organized into groups (see photo on the next page for an example).

When organized into groups, the switch must be placed in the rack so that the holes in the extension brackets line up correctly.

1. Align the mounting brackets with the mounting holes on the switch's side panels and secure the brackets with the screws provided.

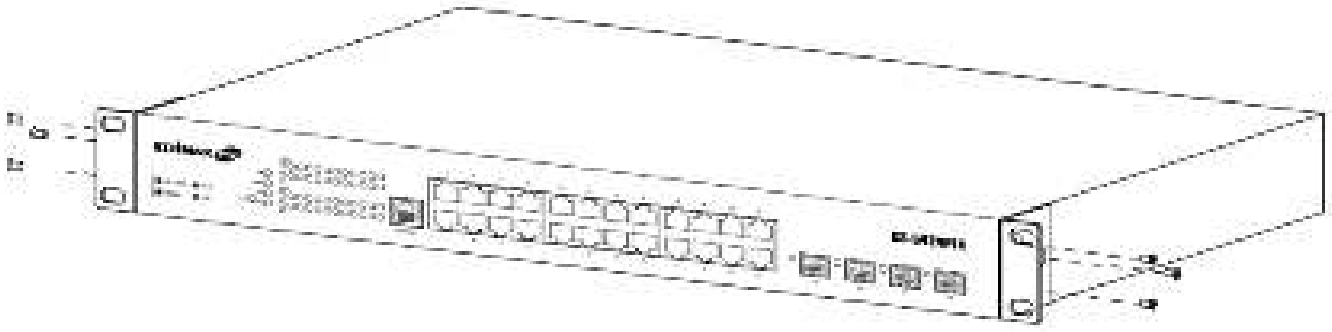


Figure 5 - Bracket Installation

2. Secure the switch on the equipment rack with the screws provided.

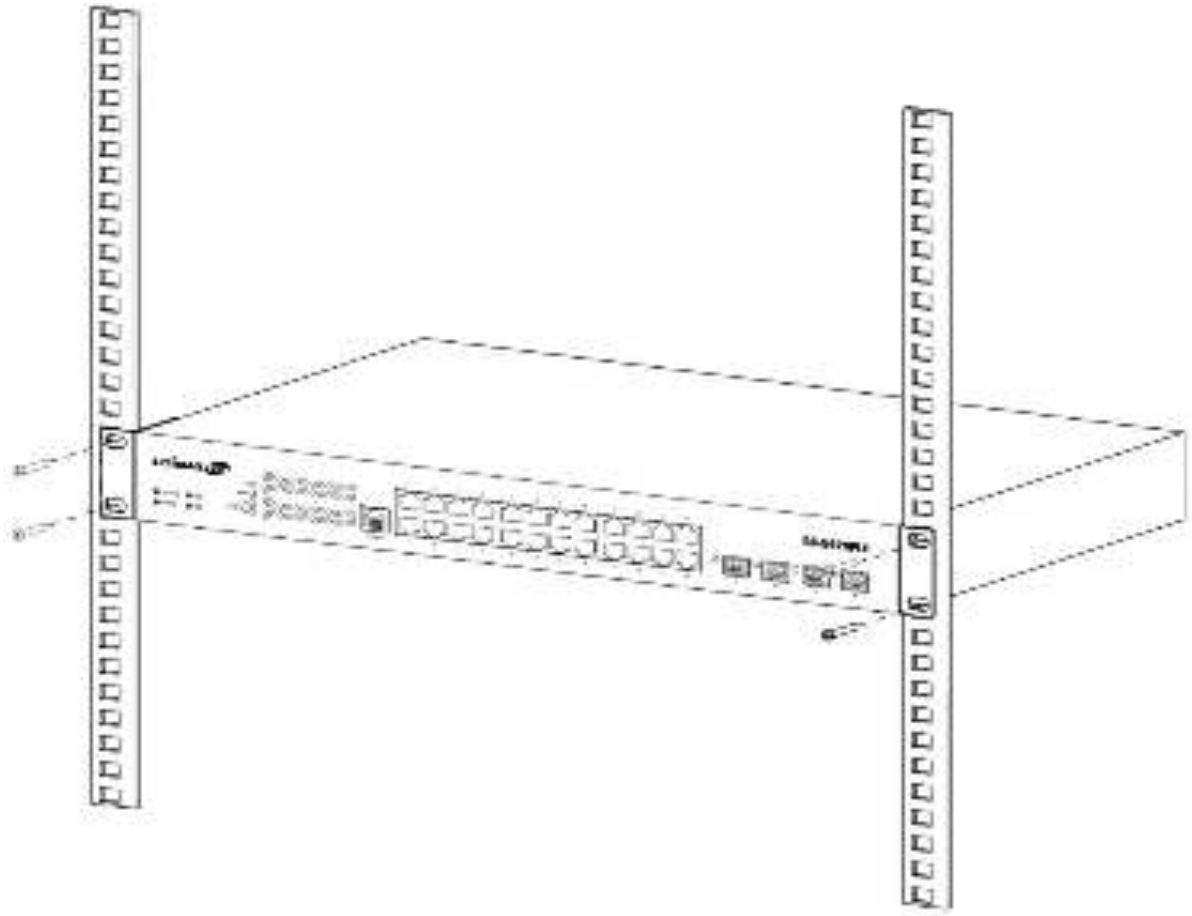


Figure 6 - Rack Installation

III Getting Started

This section provides an introduction to the web-based configuration utility, and covers the following topics:

- Powering on the device
- Connecting to the network
- Power over Ethernet (PoE) considerations
- Starting the web-based configuration utility

III-1 Power

III-1-1 Connecting to Power

Power down and disconnect the power cord before servicing or wiring a switch.

Do not disconnect modules or cabling unless the power is first switched off. The device only supports the voltage outlined in the type plate. Do not use any other power components except those specifically designated for the switch.
Disconnect the power cord before installation or cable wiring.

The switch is powered by the AC 100-240 V 50/60Hz internal high-performance power supply. It is recommended to connect the switch with a single-phase three-wire power source with a neutral outlet, or a multifunctional computer professional source.
Connect the AC power connector on the back panel of the switch to the external power source with the included power cord, and check the power LED is on.

Figure 7 - Rear View AC Power Socket

III-1-2 Connecting to Network

To connect the switch to the network:

1. Connect an Ethernet cable to the Ethernet port of a computer
2. Connect the other end of the Ethernet cable to one of the numbered Ethernet ports of the switch. The LED of the port lights if the device connected is active.
3. Repeat Step 1 and Step 2 for each device to connect to the switch.

We strongly recommend using CAT-5E or better cable to connect network devices. When connecting network devices, do not exceed the maximum cabling distance of 100 meters (328 feet). It can take up to one minute for attached devices or the LAN to be operational after it is connected. This is normal behavior.
Connect the switch to end nodes using a standard Cat 5/5e Ethernet cable (UTP/STP) to connect the switch to end nodes as shown in the illustration below.
Switch ports will automatically adjust to the characteristics (MDI/MDI-X, speed, duplex) of the device to which the switch is connected.

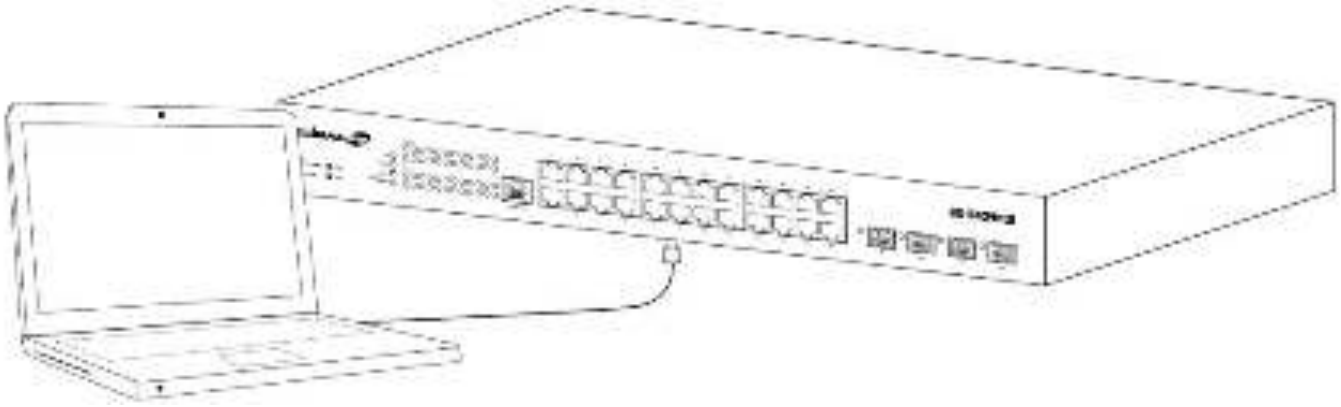


Figure 8 - PC Connect

III-1-3 Power over Ethernet (PoE) Considerations

For PoE switch models, consider the following information:
Devices considered a Power Sourcing Equipment (PSE), can support up to 30 Watts per PoE port to a Powered Device (PD).

Model	Power Dedicated to PoE	PoE Ports	PoE Standard Supported
GS-542PLX	400W	1 to 24	IEEE802.3at/af

Ports 1-24 provide PoE power supply functionality with a maximum output power up to 30W each port. This can supply power to PDs such as internet phones, network cameras, wireless access points. Connect the switch PoE port directly to the PD port using a network cable.

When connecting switches capable of supplying PoE, consider the following information:

- Switch models with PoE function are PSEs. These models are capable of supplying DC power to attached PDs, such as VoIP phones, IP cameras, and wireless access points (APs). PoE switches. Additionally, PoE switches are capable of detecting and supplying power to pre-standard legacy PoE Power Devices. Due to the support for legacy PoE, there is a possibility that PoE switches acting as a PSE may inadvertently detect and supply power an attached PSE, including other PoE switches. This false detection may result in a PoE switch operating improperly and unable to supply power to attached PDs.
- The prevention of a false detection can be easily remedied by disabling PoE on the ports that are used to connect PSEs. Another simple practice to prevent a false detection is to first power up a PSE device before connecting it to a PoE switch.
- When a device is falsely detected as a PD, disconnect the device from the PoE port and power recycle the device with AC power before reconnecting it to the PoE port.

III-1-4 Starting the Web-based Configuration Utility

This section describes how to navigate the web-based switch configuration utility.
Be sure to disable any pop-up blocker.

Browser Restrictions

- If you are using older versions of Internet Explorer, you cannot directly use an IPv6 address to access the device. You can, however, use the DNS (Domain Name System) server to create a domain name that contains the IPv6 address, and then use that domain name in the address bar in place of the IPv6 address.
- If you have multiple IPv6 interfaces on your management station, use the IPv6 global address instead of the IPv6 link local address to access the device from your browser.

Launching the Configuration Utility

To open the web-based configuration utility:

1. Open a Web browser.
2. Enter the IP address of the device you are configuring in the address bar on the browser (factory default IP address is 192.168.2.1) and then press Enter.

When the device is using the factory default IP address, its power LED flashes continuously. When the device is using a DHCP assigned IP address or an administrator-configured static IP address, the power LED is lit a solid color. Your computer's IP address must be in the same subnet as the switch. For example, if the switch is using the factory default IP address, your computer's IP address can be in the following range: 192.168.2.x (whereas x is a number from 2 to 254).
After a successful connection, the login window displays.

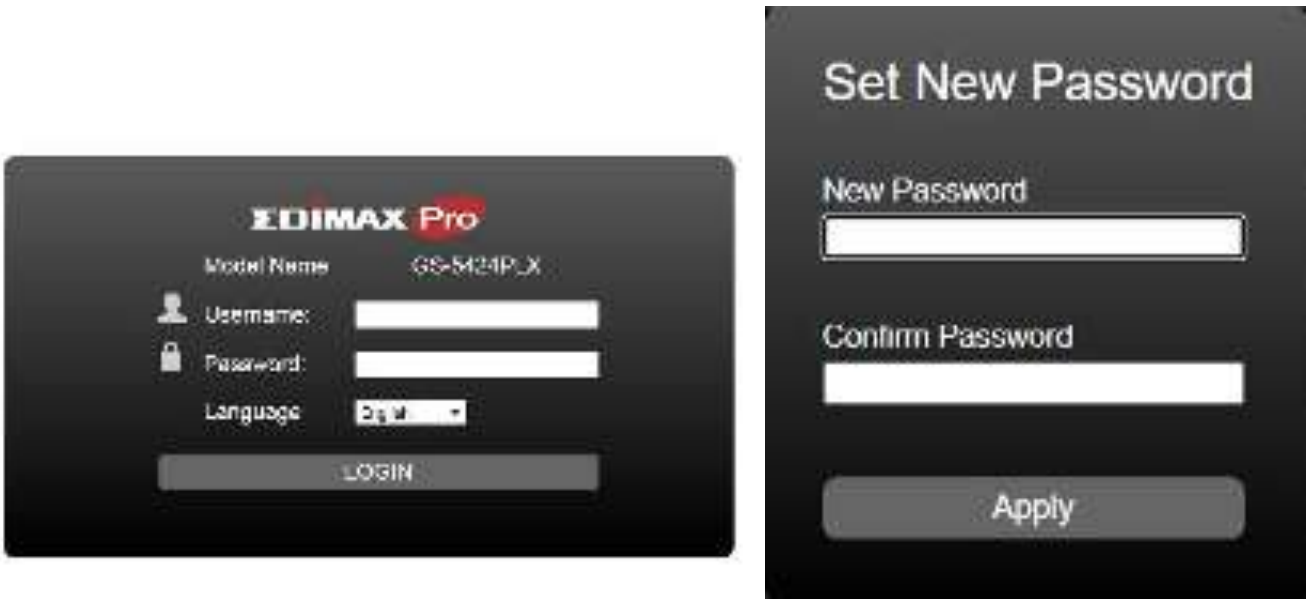


Figure 9 - Login Window

III-1-5 Logging In

The default username is admin and the default password is admin. The first time that you log in with the default username and password, you are required to enter a new password.

To log in to the device configuration utility:

1. Enter the default user ID (admin) and the default password (admin).
2. If this is the first time that you logged on with the default user ID (admin) and the default password (admin) it is recommended that you change your password immediately. See “4.9.3. Administrator” for additional information.

When the login attempt is successful, the System Information window displays.

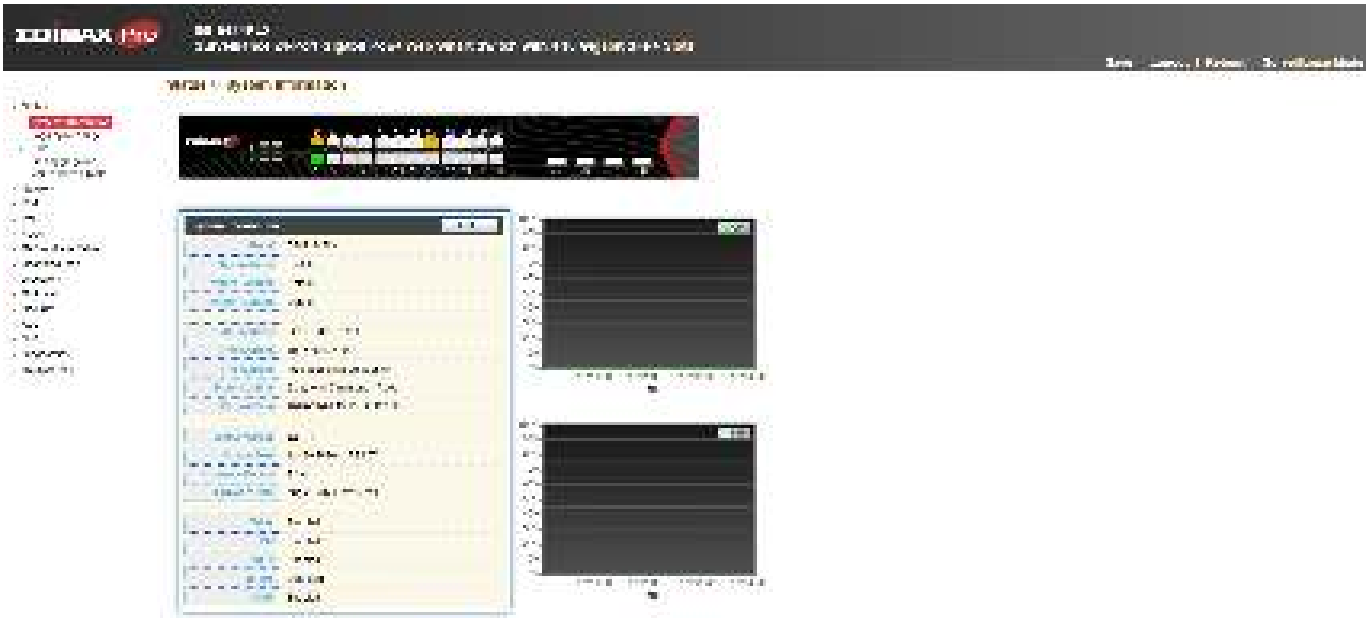


Figure 10 - System Information

If you entered an incorrect username or password, an error message appears and the Login page remains displayed on the window. If you are having problems logging in, please see the Launching the Configuration Utility section in the Administration Guide for additional information.

III-1-6 Logging Out

By default, the application logs out after ten minutes of inactivity.

To manually logout, click Logout in the top right corner of any page.

When a timeout occurs or you intentionally log out of the system, a message appears and the Login page appears, with a message indicating the logged-out state. After you log in, the application returns to the initial page.

IV Web-based Switch Configuration

The PoE smart switch software provides rich Layer 2 functionality for switches in your networks. This chapter describes how to use the web-based management interface (Web UI) to configure the switch's features.

For the purposes of this manual, the user interface is separated into four sections, as shown in the following figure:

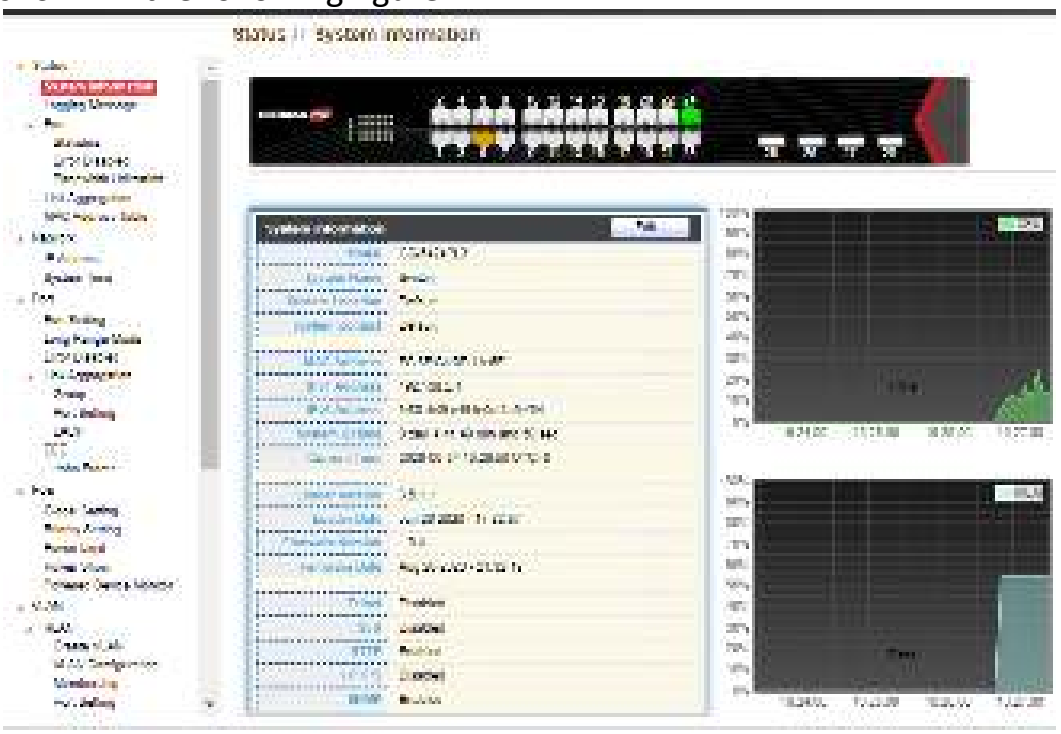


Figure 11 - User Interface

No.	Name	Description
1	Configuration menu	Navigate to locate specific switch functions.
2	Configuration settings	Edit specific function settings.
3	Switch's current link status	Green squares indicate the port link is up, while black squares indicate the port link is down.
4	Common toolbar	Provides access to frequently used settings.

IV-1 Status

Use the Status pages to view system information and status.

IV-1-1 System Information

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

To display the Device Information web page, click **Status > System Information**.

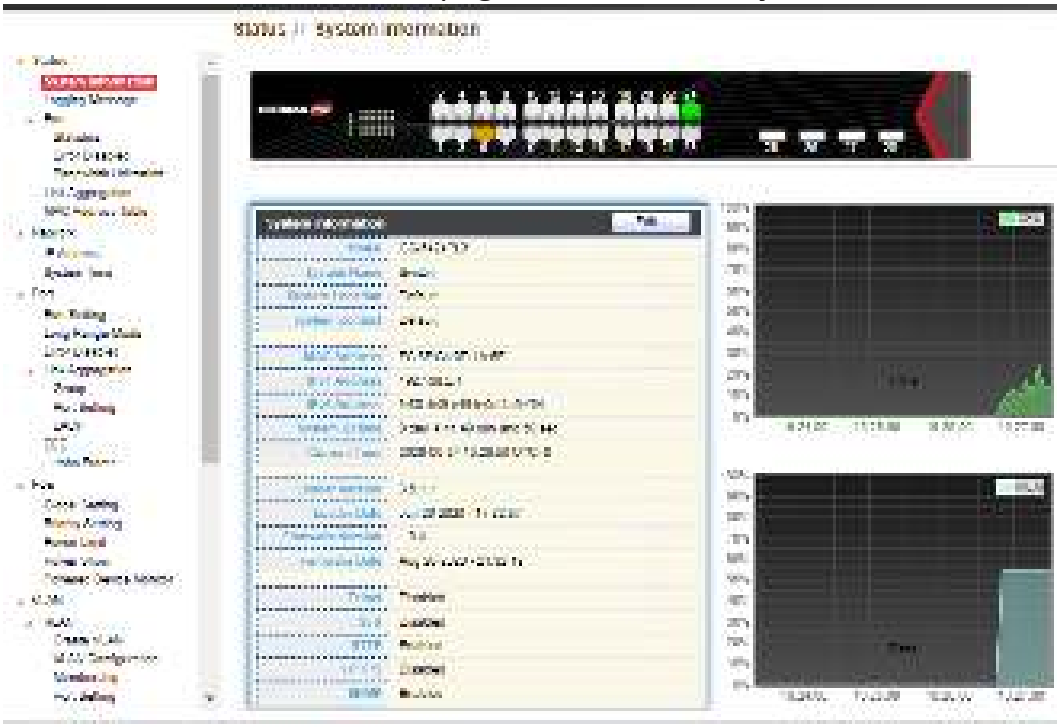


Figure 12 - Status > System Information

Item	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.
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.

Click “Edit” button on the table title to edit following system information.

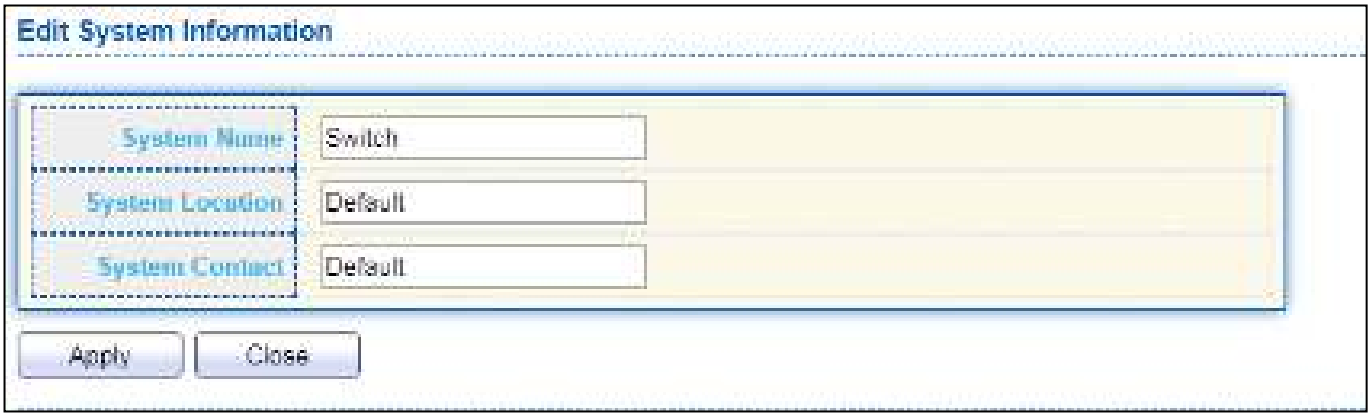


Figure 13 - Status > System Information > Edit System Information

Item	Description
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.

IV-1-2 Logging Message

To view the logging messages stored on the RAM and Flash, click **Status > Logging Message**.

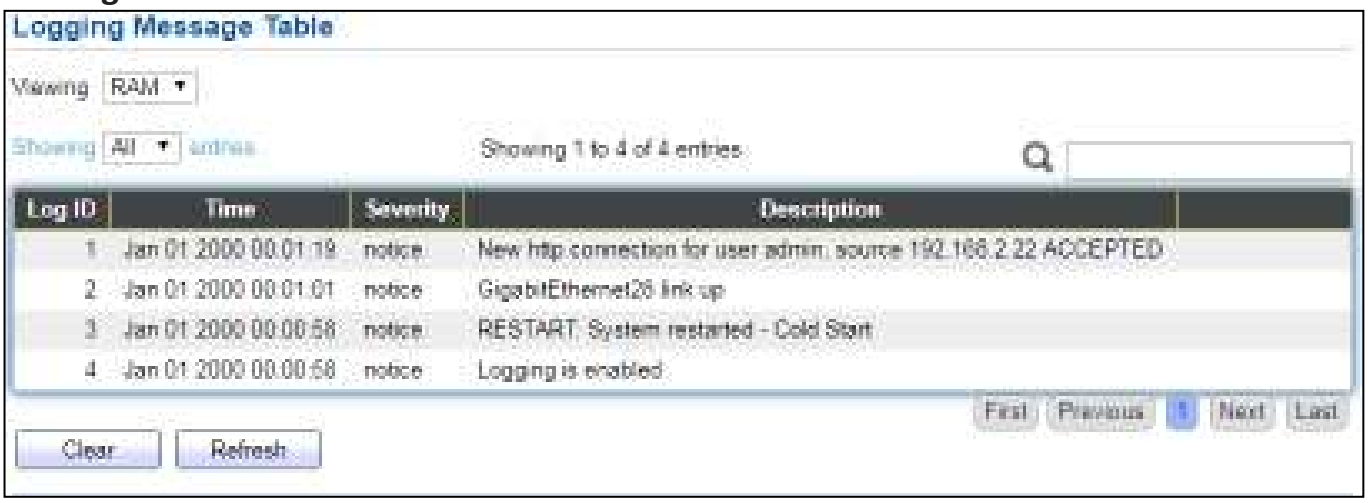


Figure 14 - Status > Logging Message

Item	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.
Viewing	The logging view including: ● RAM: Show the logging messages stored on the RAM. ● Flash: Show the logging messages stored on the Flash.
Clear	Clear the logging messages.
Refresh	Refresh the logging messages.

IV-1-3 Port

IV-1-3-1 Statistics

This page displays standard counters on network traffic form the Interfaces, Ethernet -like and RMONMIB. 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.

To display the Port Flow Chart web page, click **Status > Port > Statistics**.

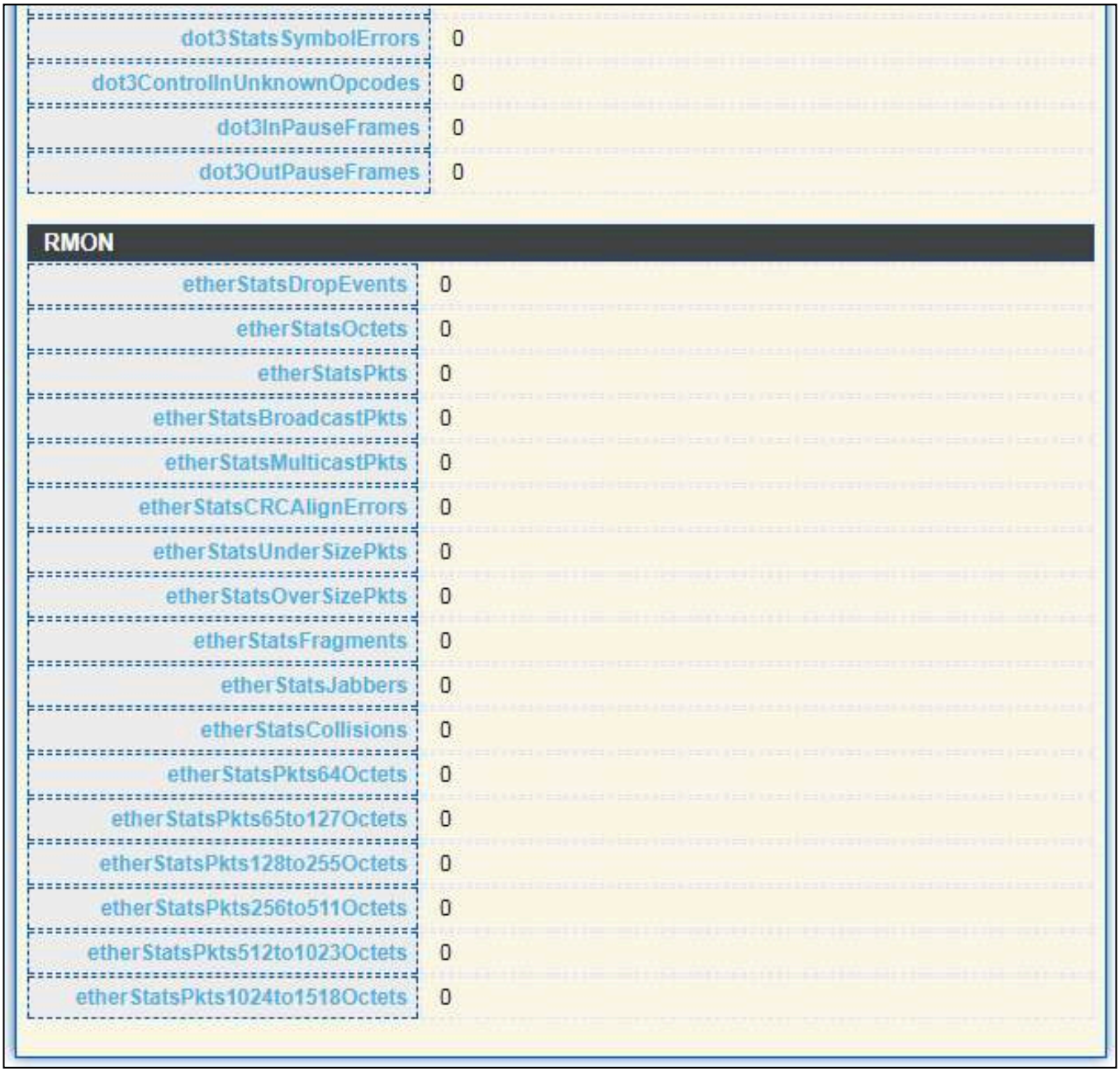


Figure 15 - Status > Port > Statistics

Item	Description
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 seconds to get new counter of specified port.

IV-1-3-2 Error Disabled

To display the Error Disabled web page, click **Status > Port > Error Disabled**.

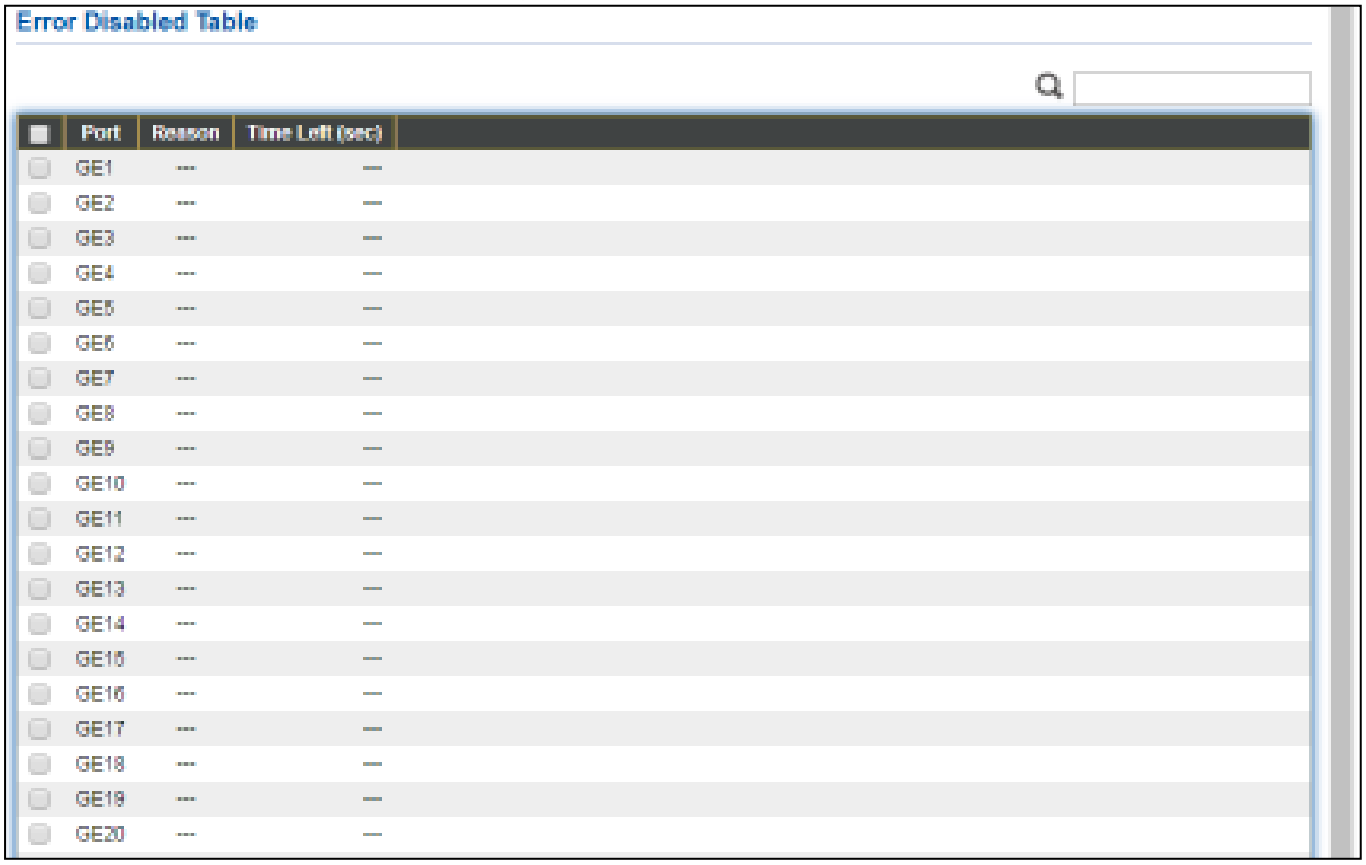


Figure 16 - Status > Port > Error Disabled

Item	Description
□	Select one or more port to operate.
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.
Refresh	Refresh the current page.
Recover	Recover the selected port status.

IV-1-3-3 Bandwidth Utilization

This page allow user to browse ports' bandwidth utilization in real time. This page will refresh automatically in every refresh period.

To display Bandwidth Utilization web page, click **Status > Port > Bandwidth Utilization**.

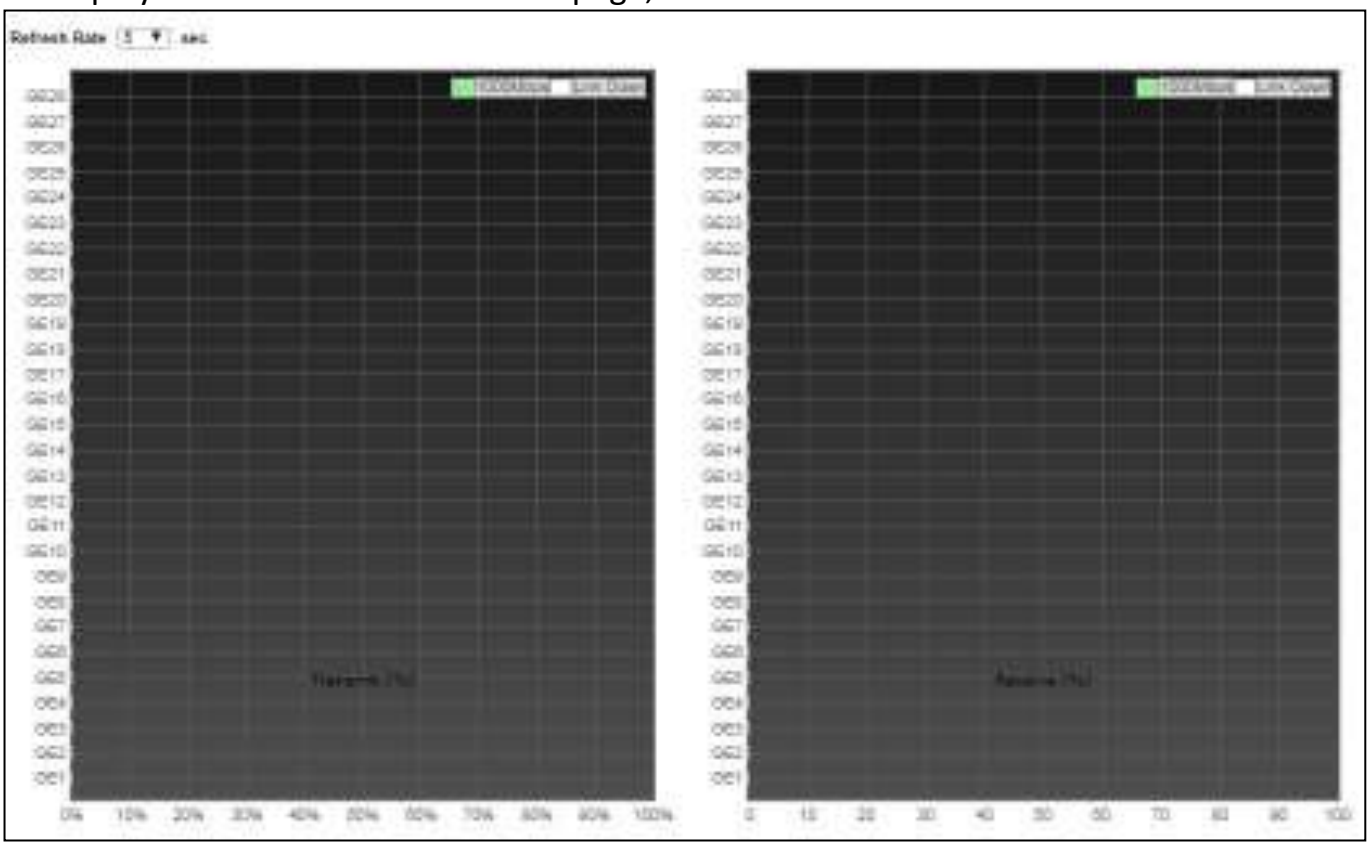


Figure 17 - Status > Port > Bandwidth Utilization

Item	Description
Refresh Rate	Refresh the web page every period of seconds to get new bandwidth utilization data.

IV-1-4 Link Aggregation

To display the Link Aggregation web page, click **Status > Link Aggregation**.

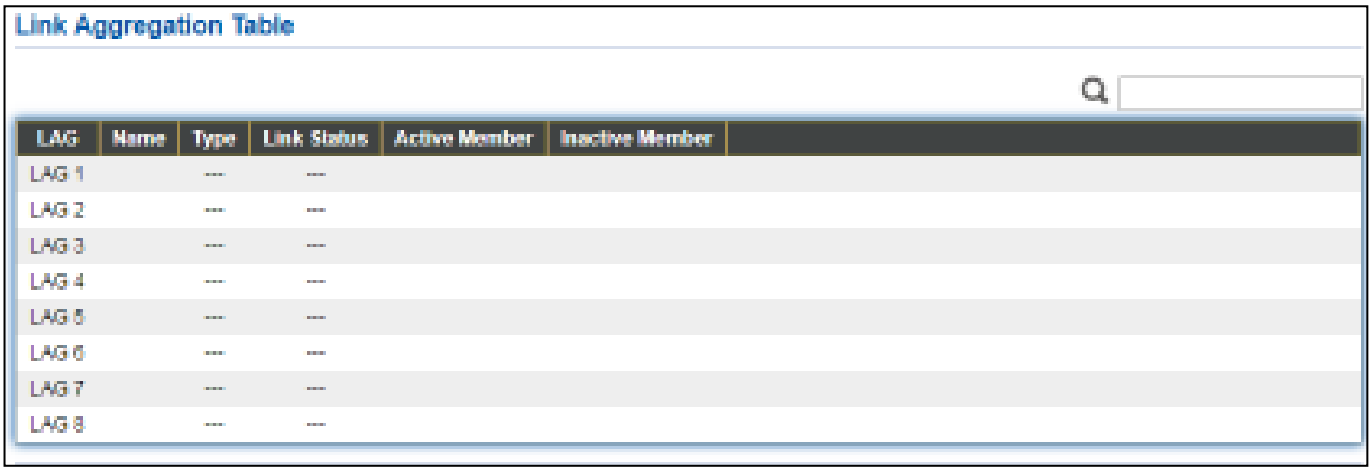


Figure 18 - Status > Link Aggregation

Item	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.

IV-1-5 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.

To display the MAC Address Table web page, click **Status > MAC Address Table**.

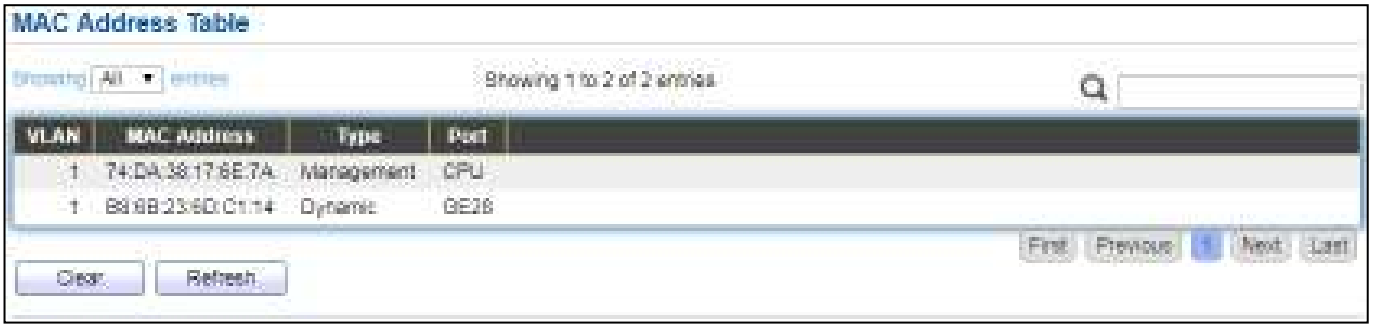


Figure 19 - Status > MAC Address Table

Item	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.

IV-2 Network

Use the Network pages to configure settings for the switch network interface and how the switch connects to a remote server to get services.

IV-2-1 IP Address

This section allows you to edit the IP address, Netmask, Gateway and DNS server of the switch.

To view the IP Address menu, navigate to **Network > IP Address**.

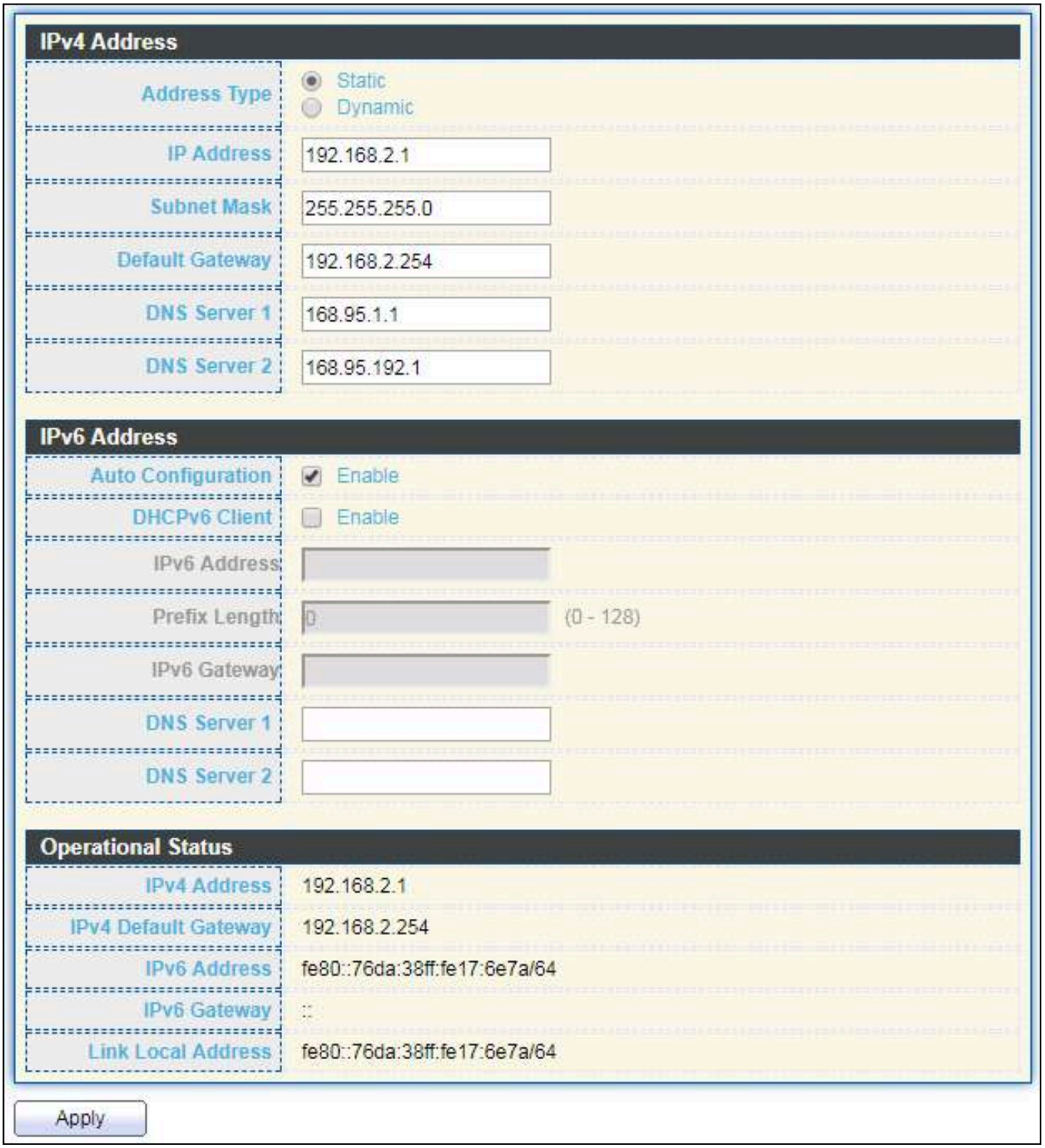


Figure 20 - Network > IP Address

Item	Description
Address Type	The address type of switch IP configuration including ● Static: Static IP configured by users will be used. ● Dynamic: Enable the DHCP to obtain the IP address from a DHCP server.
IP Address	Specify the switch static IP address on the static configuration.
Subnet Mask	Specify the switch subnet mask on the static configuration.
Default Gateway	Specify the default gateway on the static configuration. The

	default gateway must be in the same subnet with switch IP address configuration.
DNS Server 1	Specify the primary user-defined IPv4 DNS server configuration.
DNS Server 2	Specify the secondary user-defined IPv4 DNS server configuration.
Table 3-2: IPv6 Address fields	
IPv4 Address	The operational IPv4 address of the switch.
IPv4 Gateway	The operational IPv4 gateway of the switch.
IPv6 Address v6	The operational IPv6 address of the switch.
IPv6 Gateway	The operational IPv6 gateway of the switch.
Link Local Address	The IPv6 link local address for the switch.

IV-2-2 System Time

This page allow user to set time source, static time, time zone and daylight saving settings. Time zone and daylight saving takes effect both static time or time from SNTP server.

To display System Time page, click **Network > System Time**.

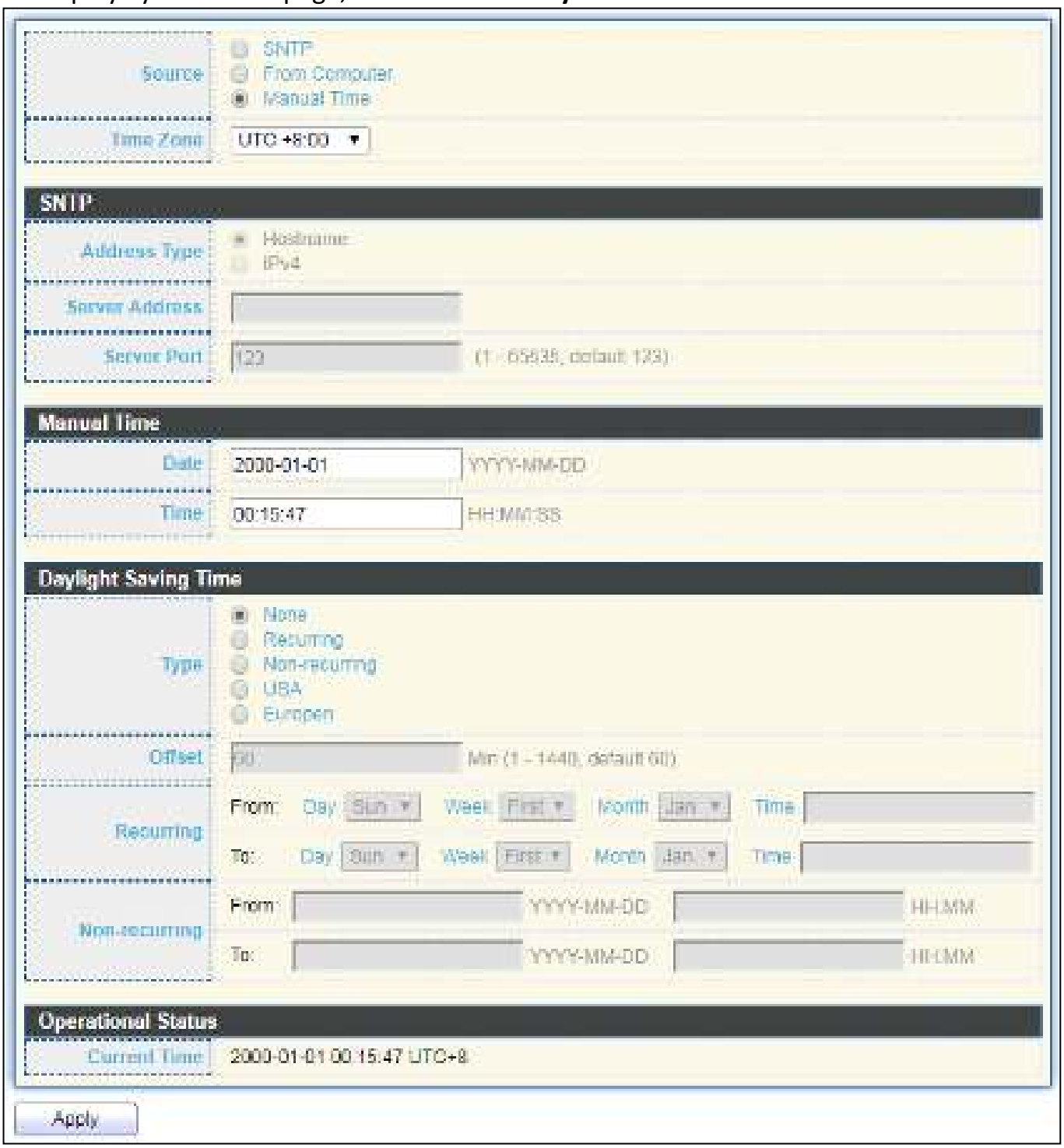


Figure 21 - Network > System Time

Item	Description
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.
Server Port	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	
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 Sunday in October.
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.
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.

IV-3 Port

Use the Port pages to configure settings for switch port related features.

IV-3-1 Port Setting

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

To display Port Setting web page, click **Port > Port Setting**.

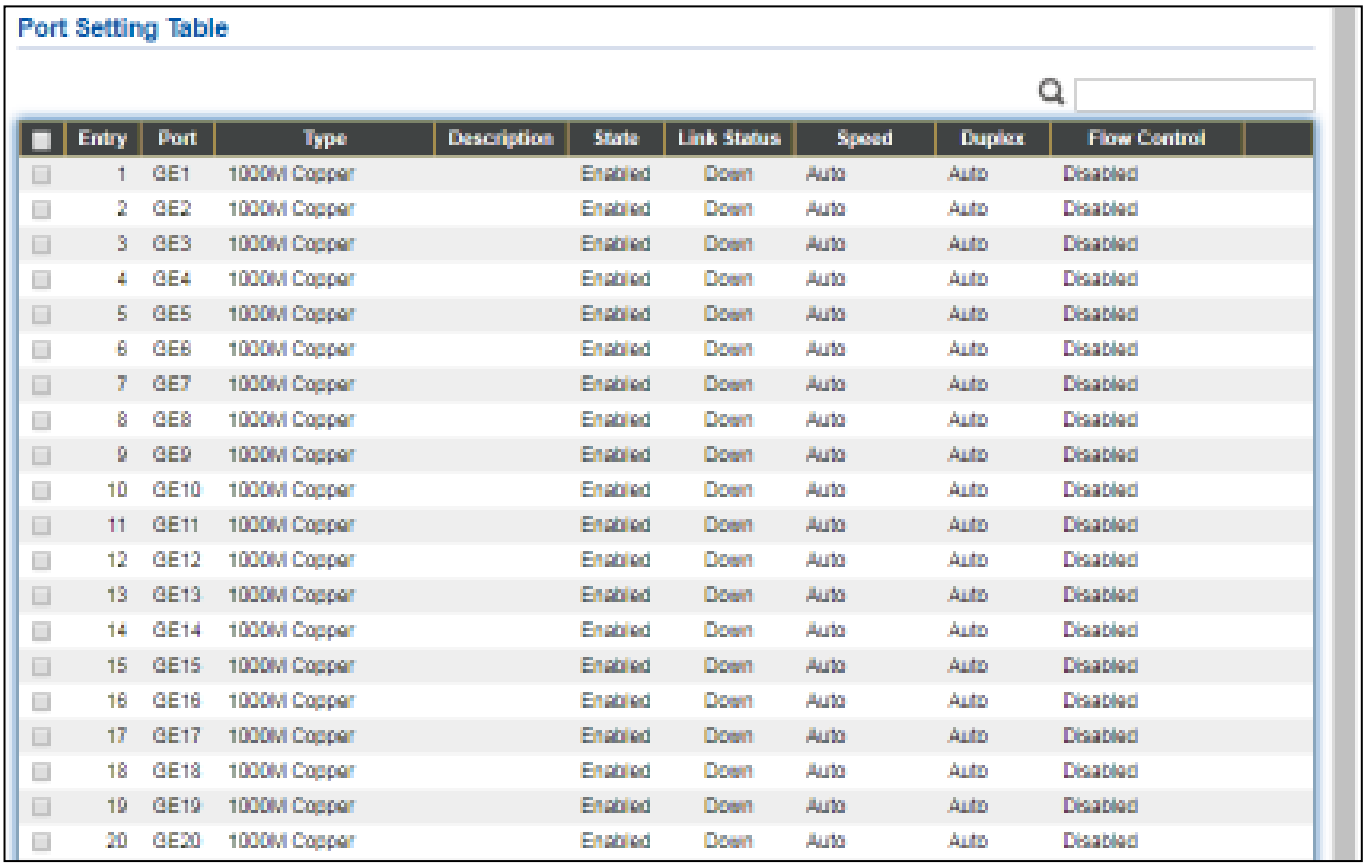


Figure 22 - Port > Port Setting

Item	Description
Port	Port Name.
Type	Port media type.
Description	Port Description.
State	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.

Click "**Edit**" button to edit Port Setting menu

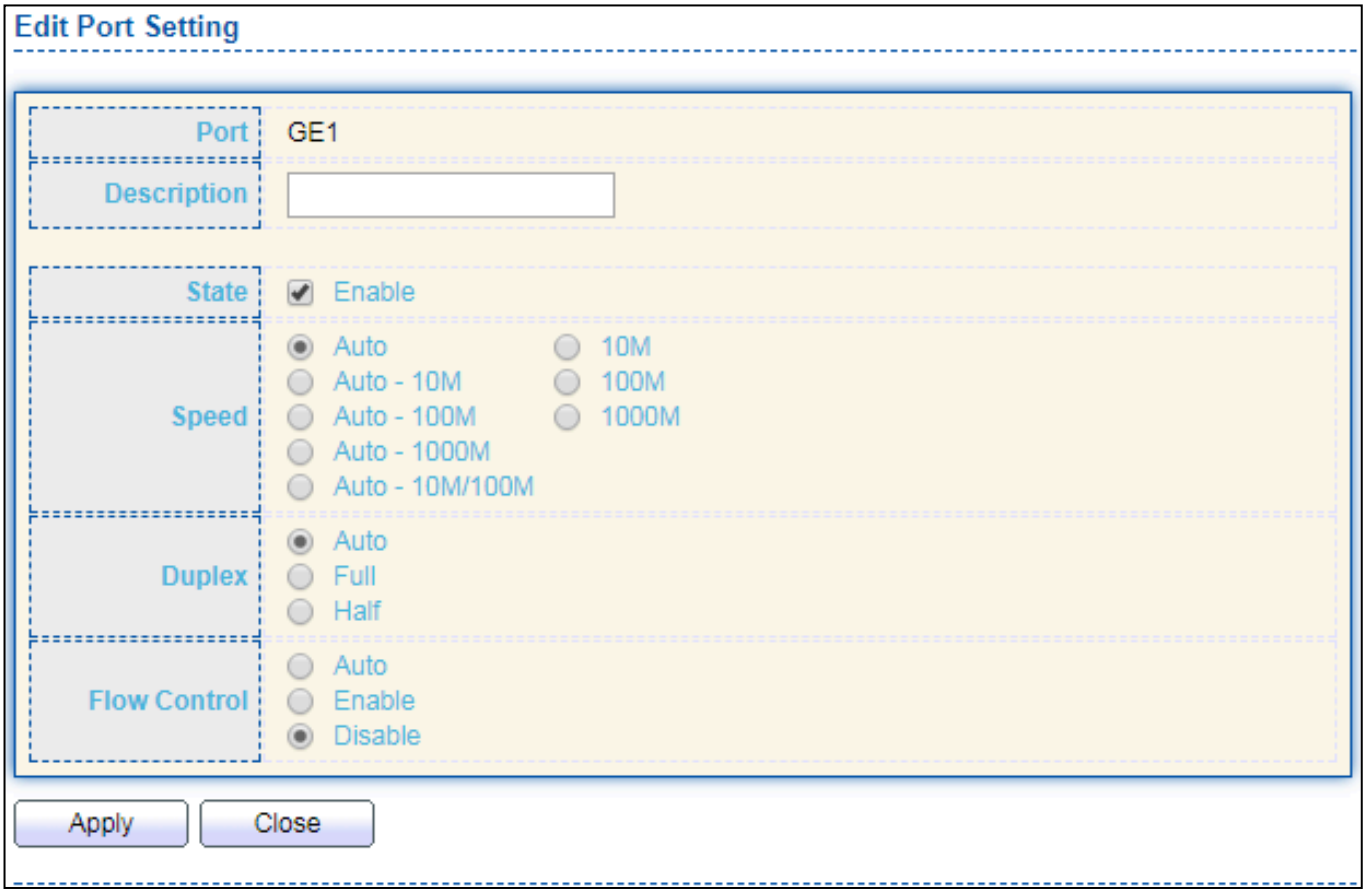


Figure 23 - Port > Port Setting > Port Setting

Item	Description
Port	Selected Port list.
Description	Port media type.
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.

IV-3-2 Long Range Mode

This page shows port current status and Enable long range mode will double the cabling distance but reduce the speed to 10Mbps.

To display Long Range Mode web page, click **Port > Long Range Mode Setting**.

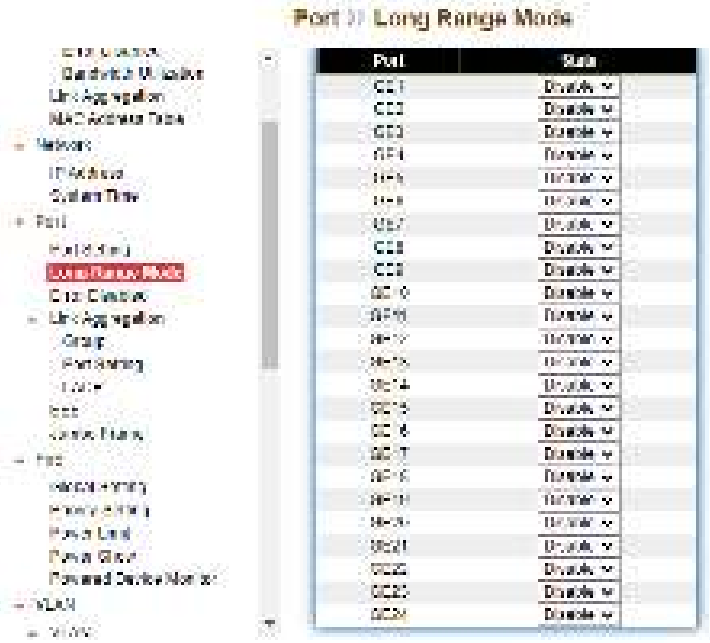


Figure 24 - Port > Long Range Mode

IV-3-3 Error Disable

To display Error Disabled web page, click **Port > Error Disabled**

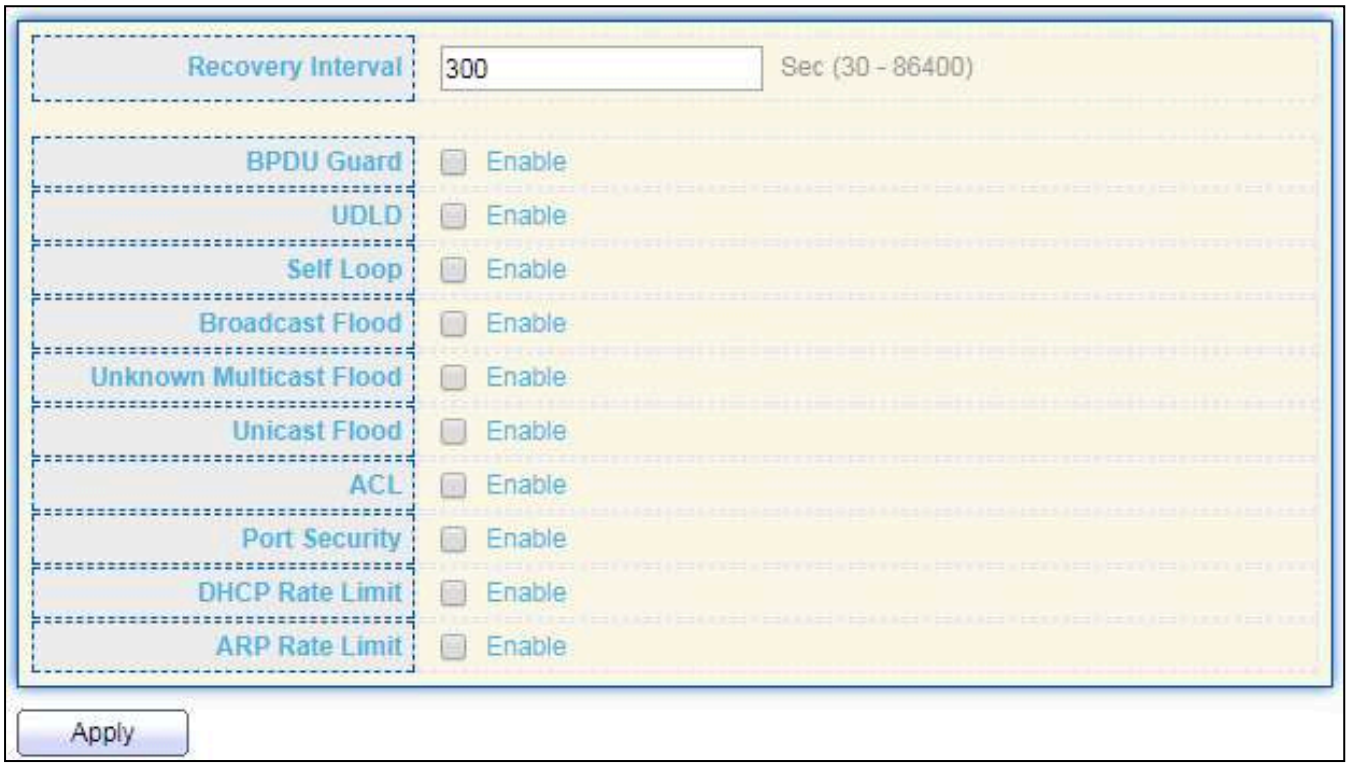


Figure 25 - Port > Error disable

Item	Description
Recover 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.

IV-3-4 Link Aggregation

IV-3-4-1 Group

This page allow user to configure link aggregation group load balance algorithm and group member.
To view the Group menu, navigate to **Port > Link Aggregation > Group**.

Figure 26 - Port > Link Aggregation > Group

Item	Description
Load Balance Algorithm	LAG load balance distribution algorithm ● src-dst-mac: Based on MAC address. ● src-dst-mac-ip: Based on MAC address and IP address.
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.

Click “**Edit**” to edit Link Aggregation Group menu.

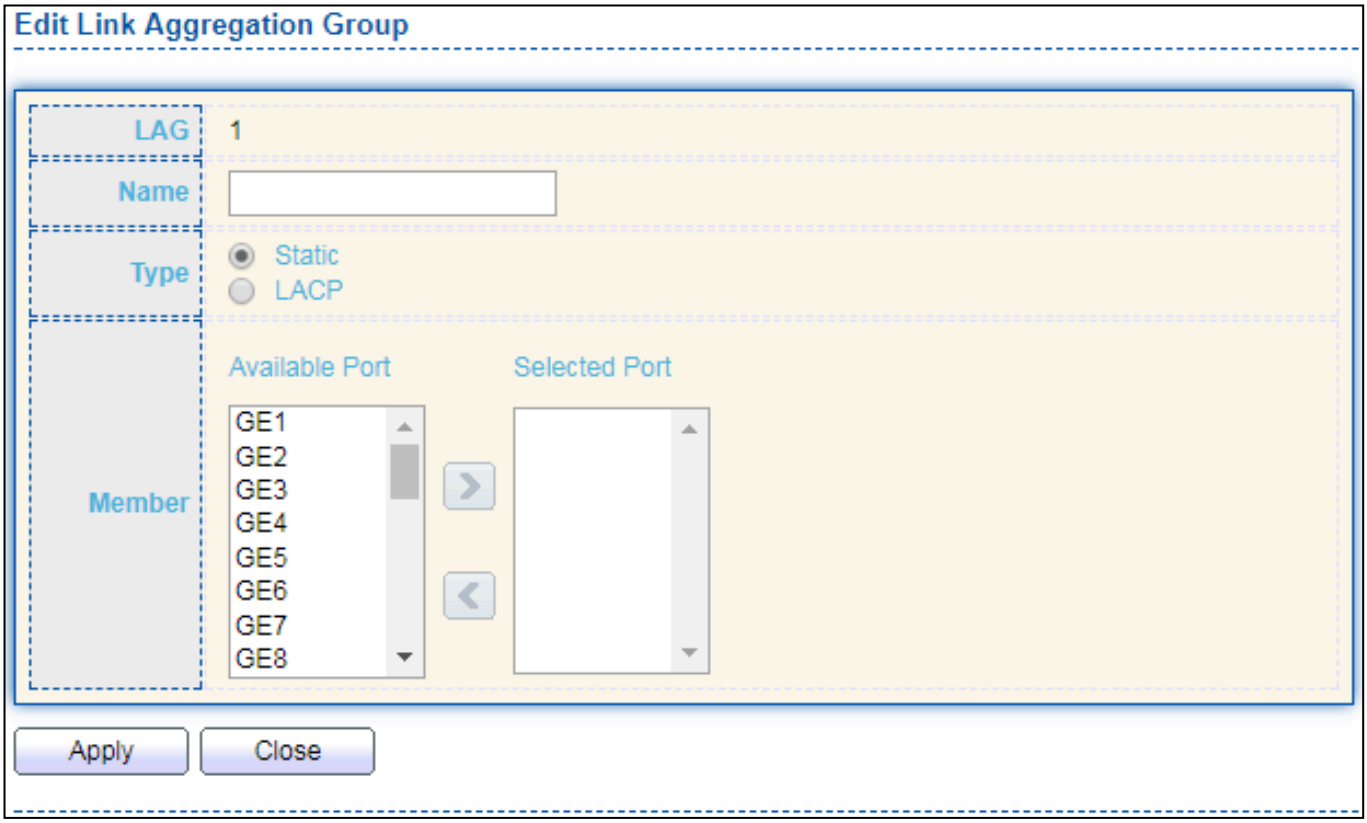


Figure 27 - Port > Link Aggregation > Group > Edit Link Aggregation Group

Item	Description
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.

IV-3-4-2 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.

To display LAG Port Setting web page, click **Port > Link Aggregation > Port Setting**.

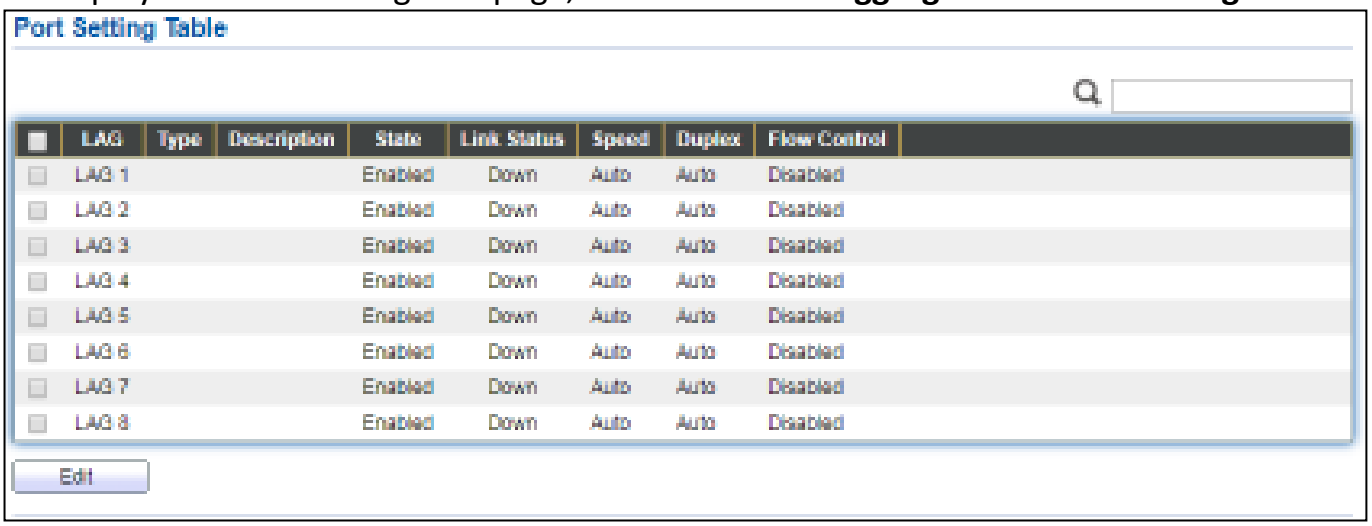


Figure 28 - Port > Link Aggregation > Port Setting

Item	Description
LAG	LAG Port Name.
Type	LAG Port media type.
Description	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.

Click “**Edit**” to view Edit Port Setting menu.

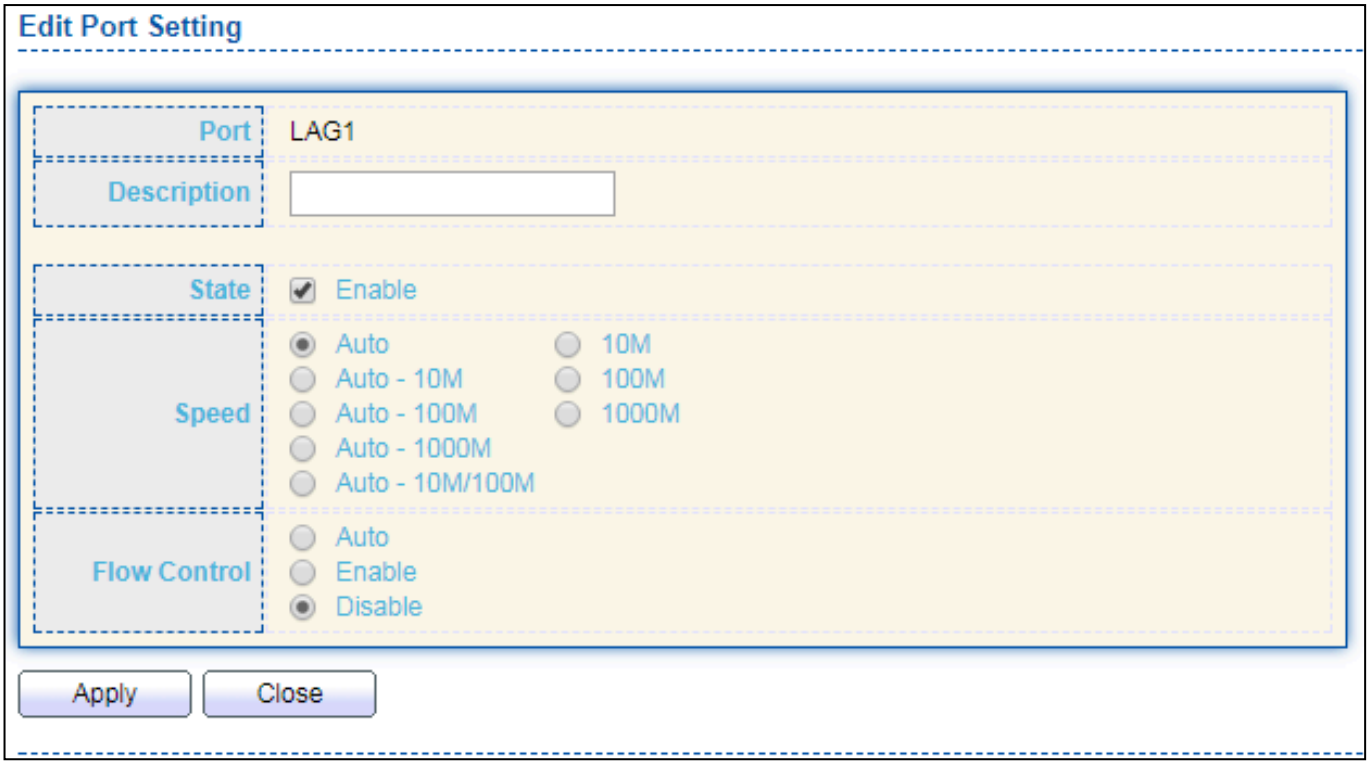


Figure 29 - Port > Link Aggregation > Port Setting > Edit Port Setting

Item	Description
Port	Selected Port list.
Description	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.

IV-3-4-3 LACP

This page allow user to configure LACP global and port configurations. Select ports and click "**Edit**" button to edit port configuration.

To display the LACP Setting web page , click **Port > Link Aggregation > LACP**.

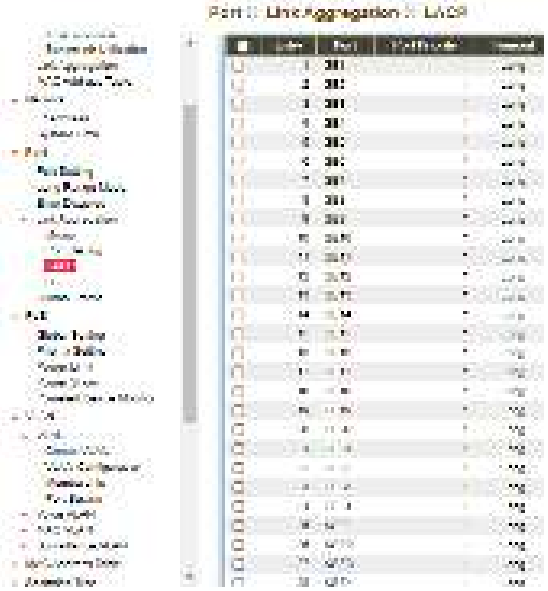


Figure 30 - Port > Link Aggregation > LACP

Item	Description
System Priority	Configure the system priority of LACP. This decides the system priority field in LACP PDU.
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).

Click "**Edit**" button to view Edit LACP Port Setting menu.

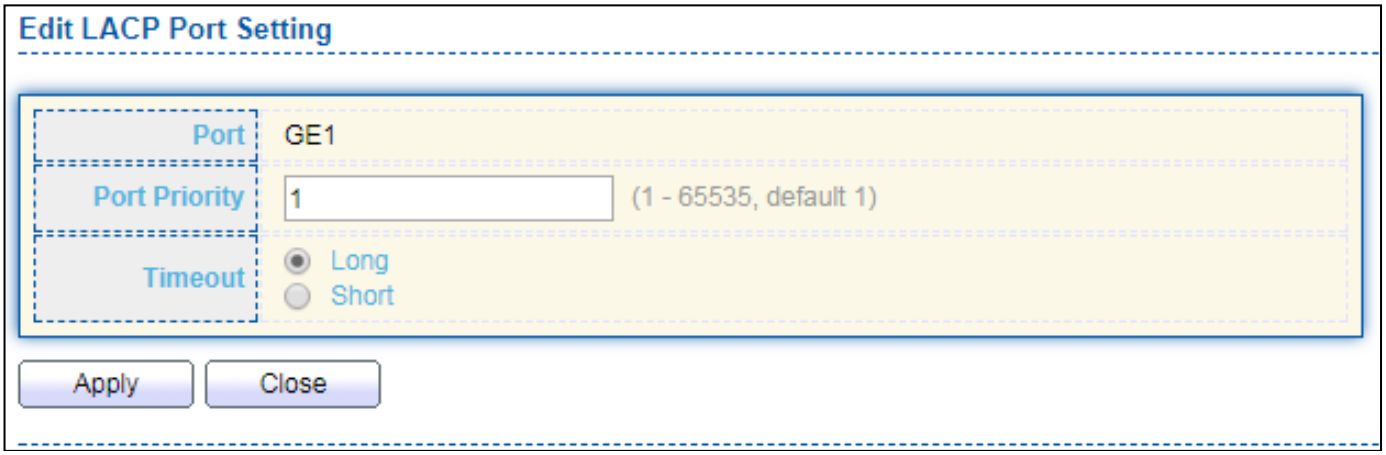


Figure 31 - Port > Link Aggregation > LACP > Edit LACP Port Setting

Item	Description
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).

IV-3-4-4 EEE

This page allow user to configure Energy Efficient Ethernet settings.

To display the EEE web page, click **Port > EEE**.

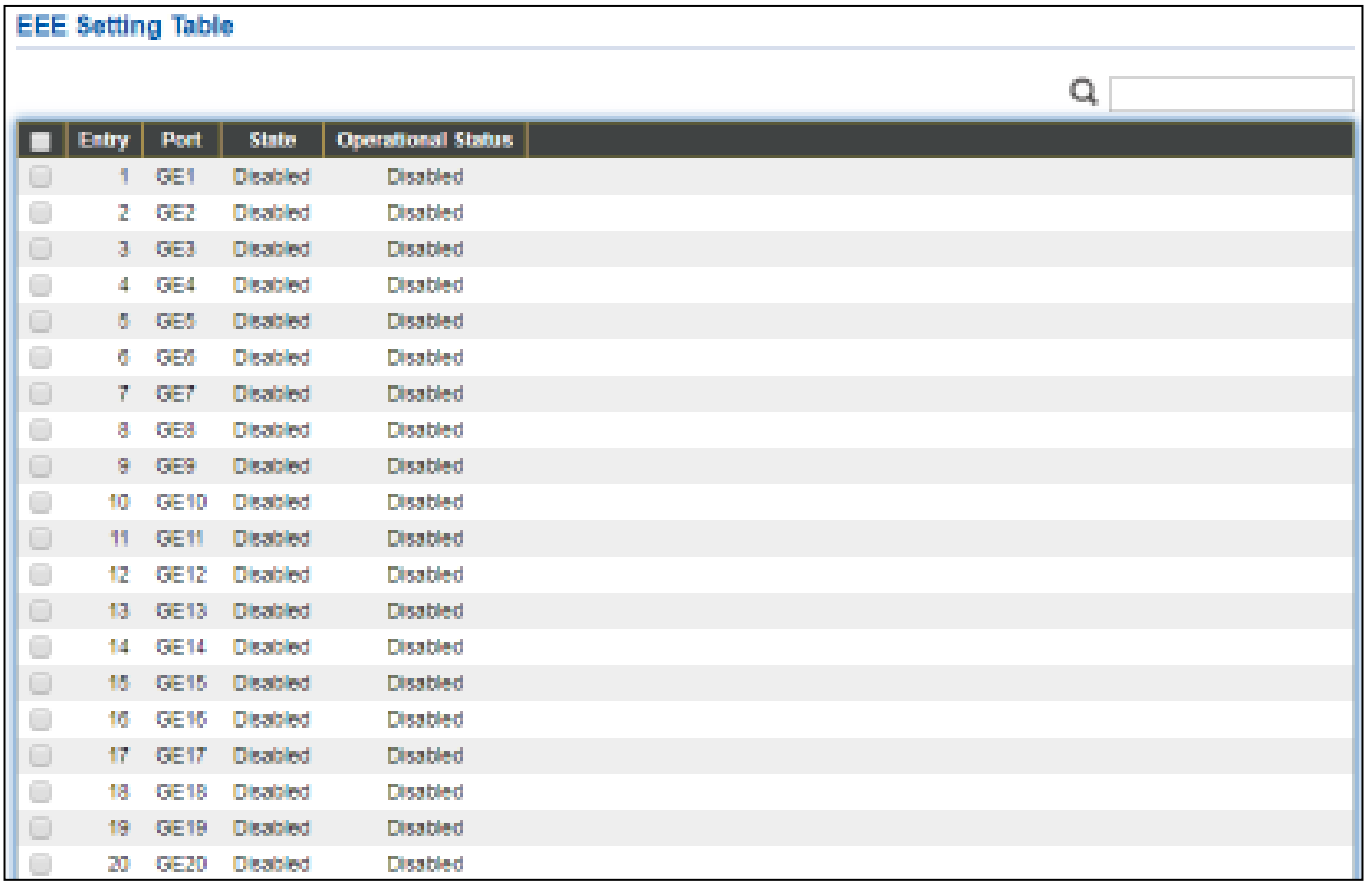


Figure 32 - Port > EEE

Item	Description
Port	Port Name.
State	Port EEE admin state ● Enabled: EEE is enabled. ● Disabled: EEE is disabled.
Operational Status	Port EEE operational status ● Enabled: EEE is operating. ● Disabled: EEE is no operating.

Click “**Edit**” to edit the EEE menu.

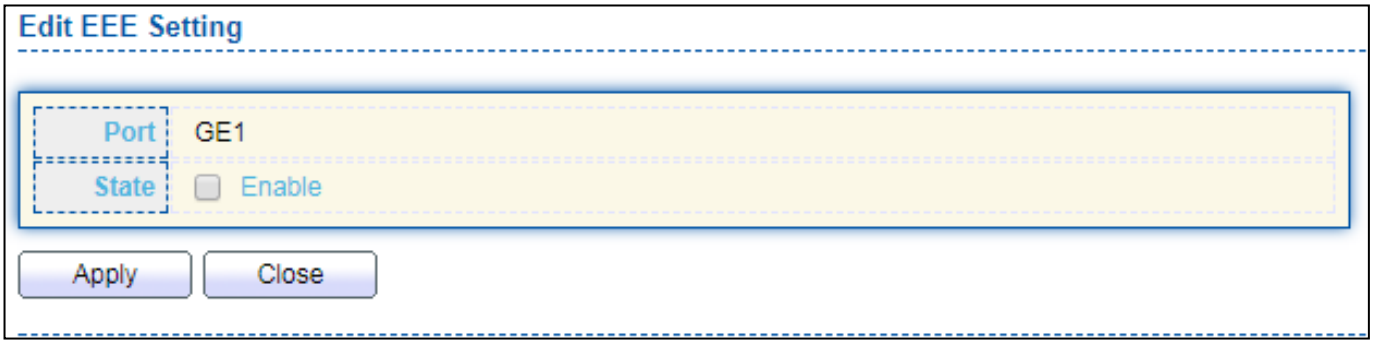


Figure 33 - Port > EEE > Edit EEE Setting

Item	Description
Port	Port Name
State	Port EEE admin state ● Enabled: EEE is enabled. ● Disabled: EEE is disabled.

IV-3-5 Jumbo Frame

This page allow user to configure switch jumbo frame size.

To display Jumbo Frame web page, click **Port > Jumbo Frame**.

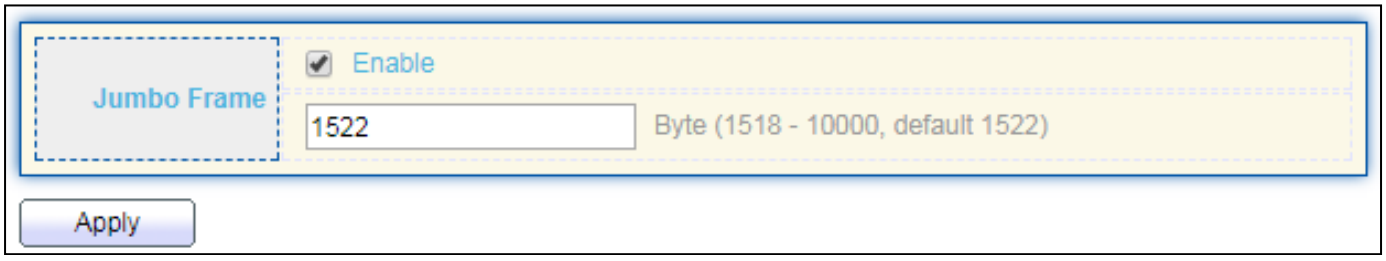


Figure 34 - Port > Jumbo Frame

Item	Description
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.

IV-4 PoE

Port security can set port isolation and specific behavior.

IV-4-1 Global Setting

To display the Global web page, click **PoE > Global Setting**.

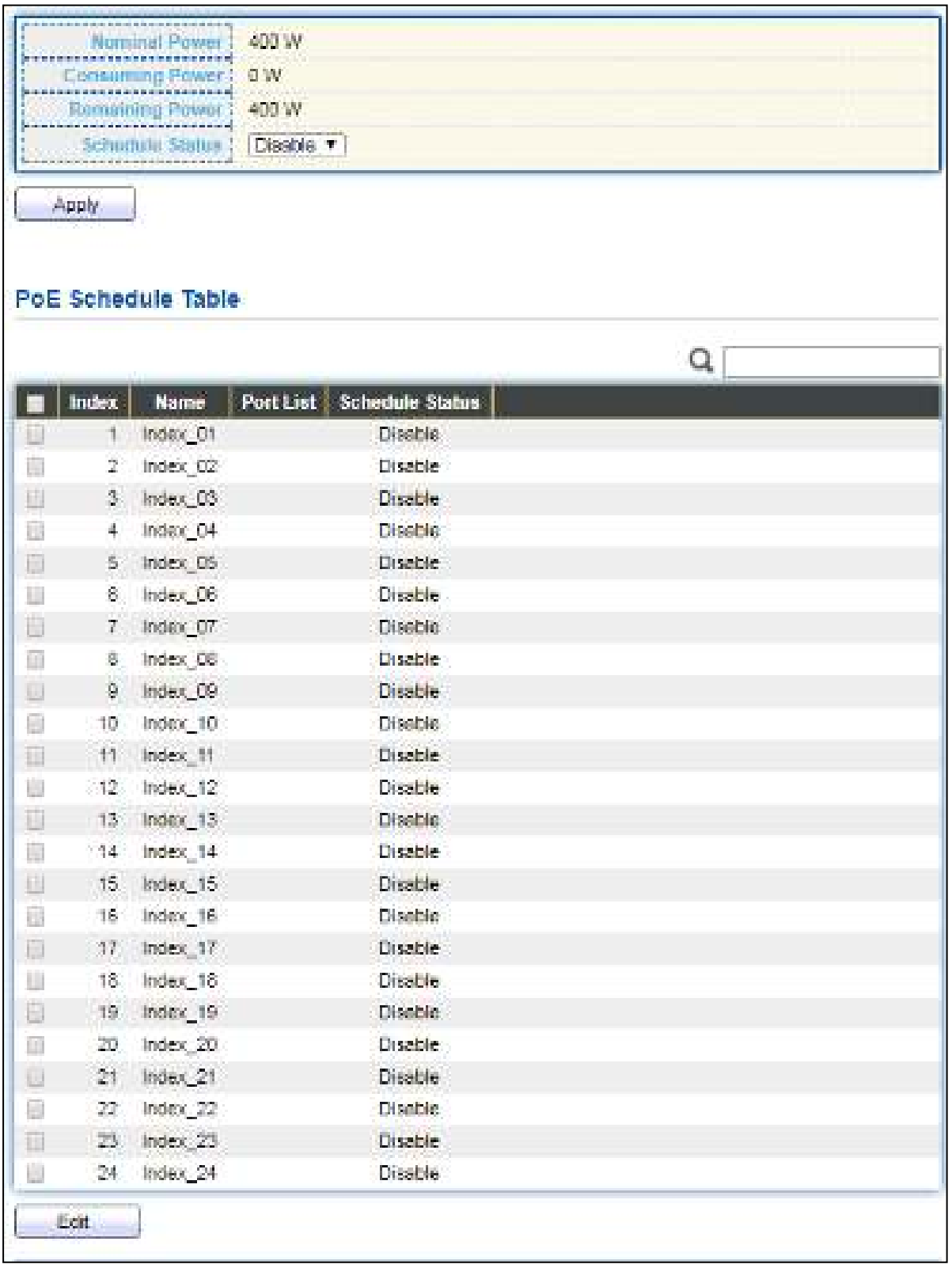


Figure 35 - PoE > Global Setting

Item	Description
Nominal Power	Maximum supply power.
Consuming Power	Current consumed power.
Remaining Power	Remaining available power.
Schedule Status	Schedule status global switch.
Name	PoE Schedule Name.
Port List	The ports provide power in designated schedule index.
Schedule Status	The current schedule status.

Click “**Edit**” to view PoE Schedule List menu.

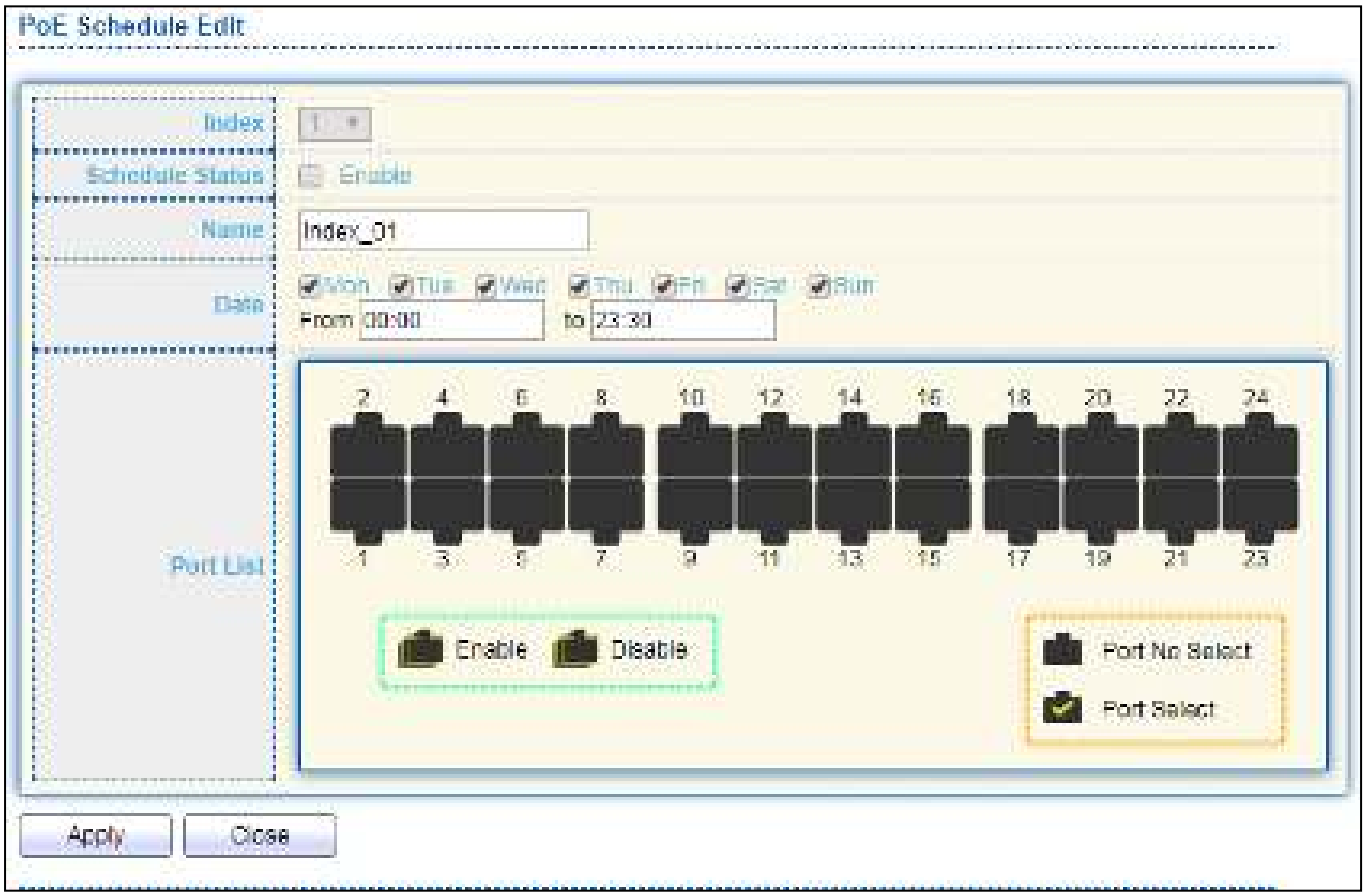


Figure 36 - PoE > Priority Setting > Edit PoE Schedule Edit

Item	Description
Index	The serial number of schedule list.
Schedule Status	Schedule Status ● Checked: Schedule status is enabled. ● Unchecked: Schedule status is disabled.
Name	Enter the PoE schedule name.
Date	Select a valid time for this schedule.
Port List	Select the port provide power.

IV-4-2 Priority Setting

Use this section to set the power supply priority of PoE ports. Individual ports can be assigned critical, high, or low power supply priority.

To display the Priority Setting web page, click **PoE > Priority Setting**.

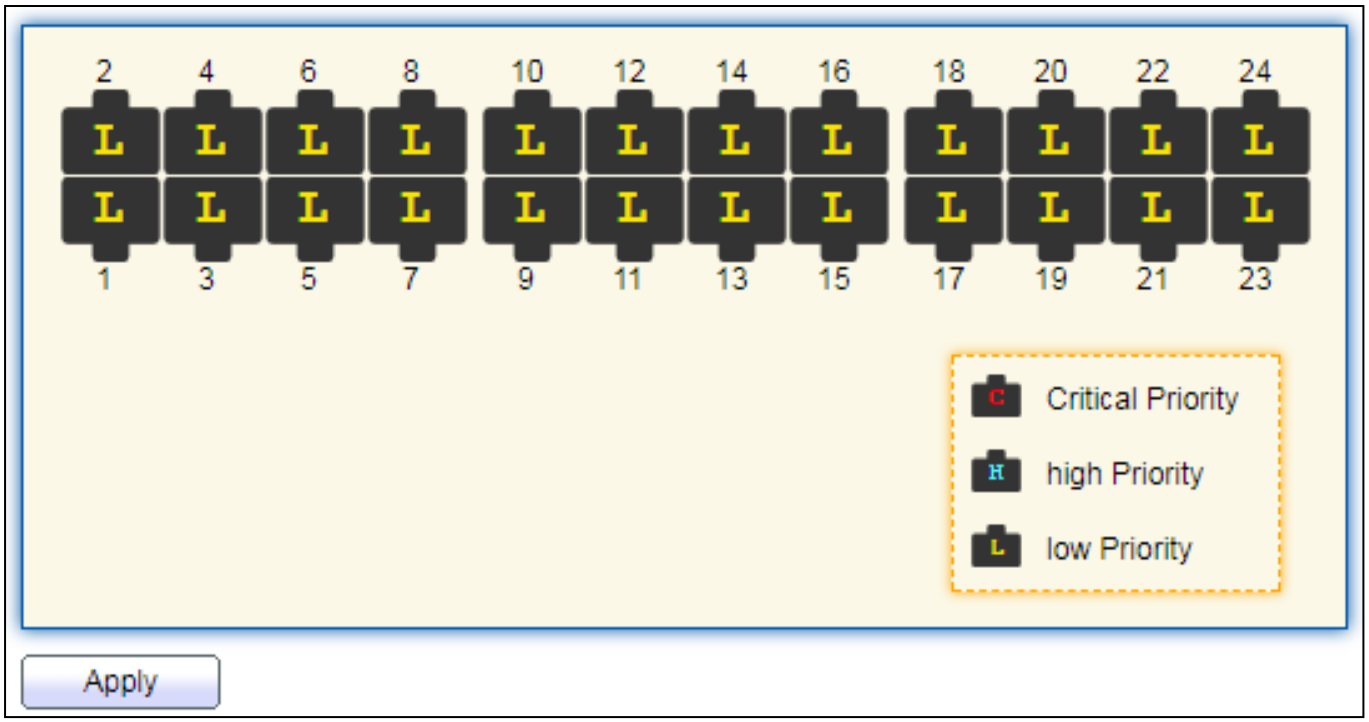


Figure 37 - PoE > Priority Setting

Click the port to change its priority status according to the bottom right hand chart.

IV-4-3 Power Limit

To display the Power Limit web page, click **PoE > Power Limit**.

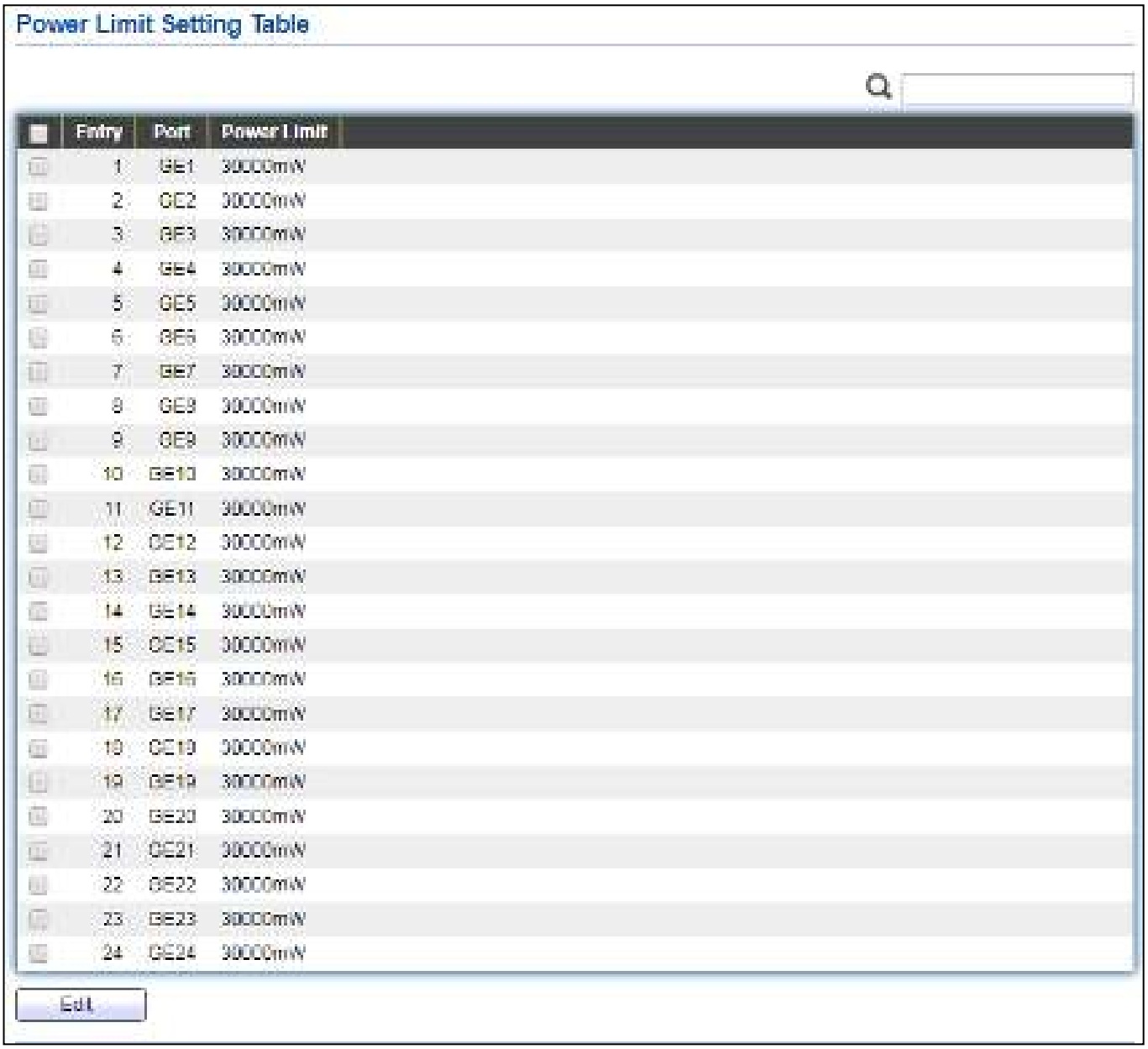


Figure 38 - PoE > Power Limit

Item	Description
Port	Port name.
Power Limit	The max supply power for this port.

Click “**Edit**” to view Power Limit Setting menu.

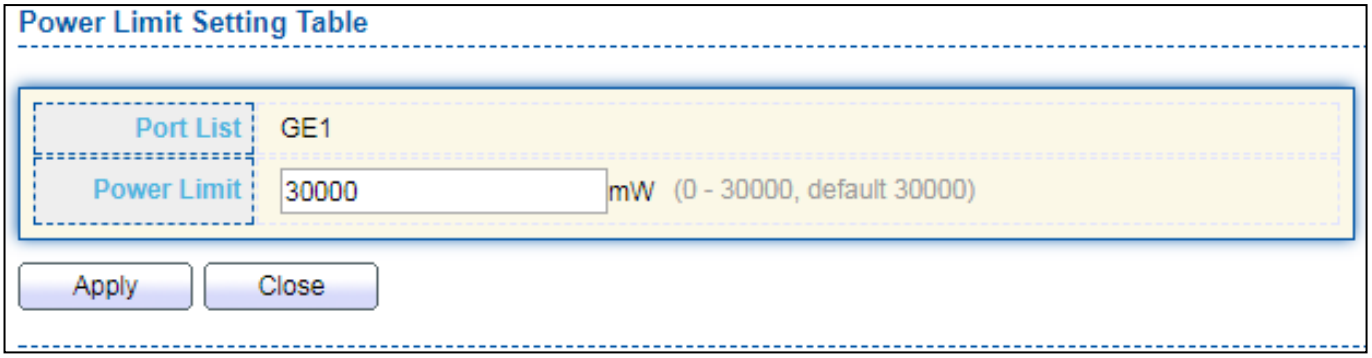


Figure 39 - PoE > Power Setting > Power Limit Setting Table

Item	Description
Port List	Selected port list.
Power Limit	Enter max supply power value for the selected port list.

IV-4-4 PoE Show

To display the PoE Status web page, click **PoE > Power Status**.

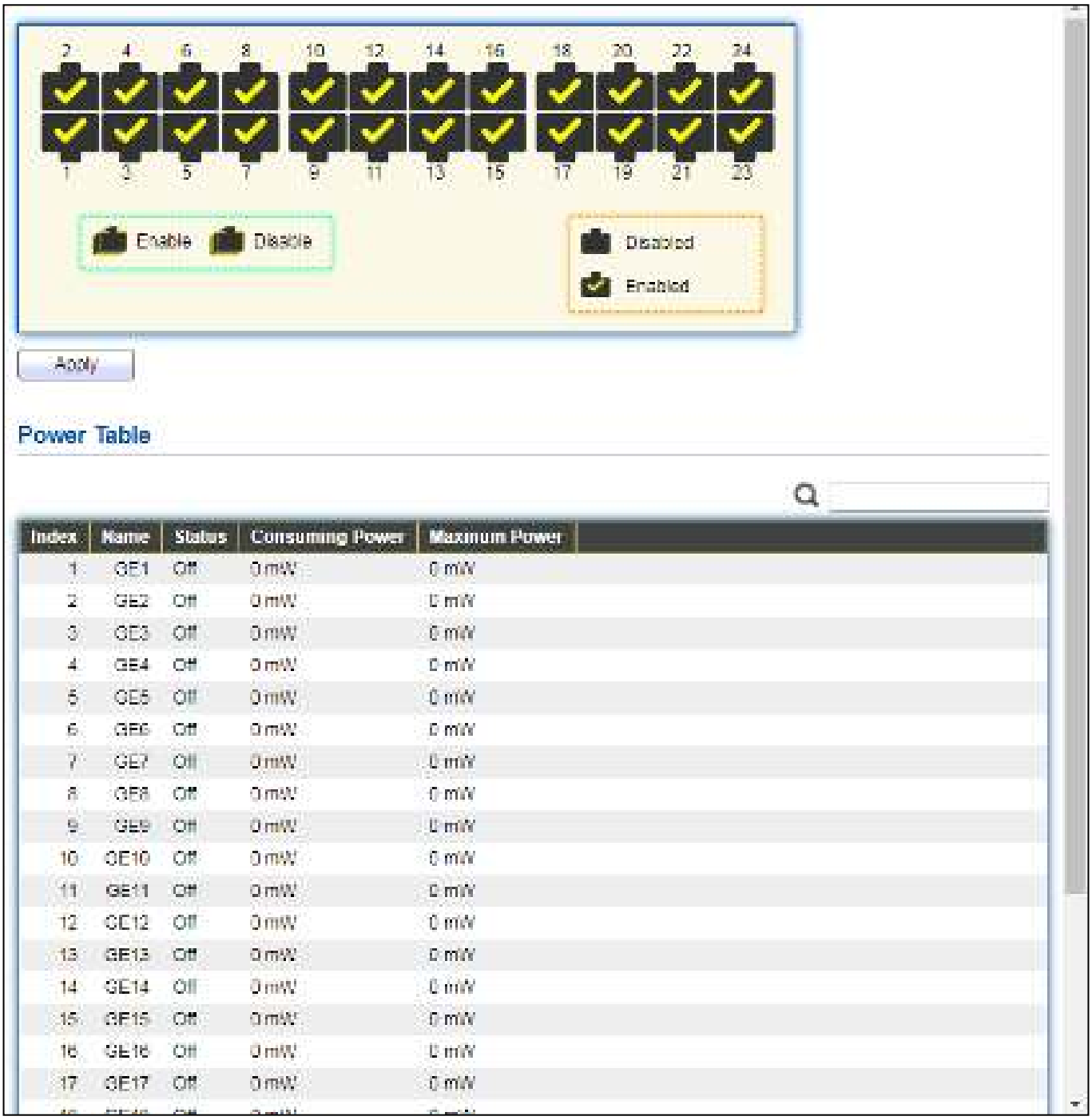
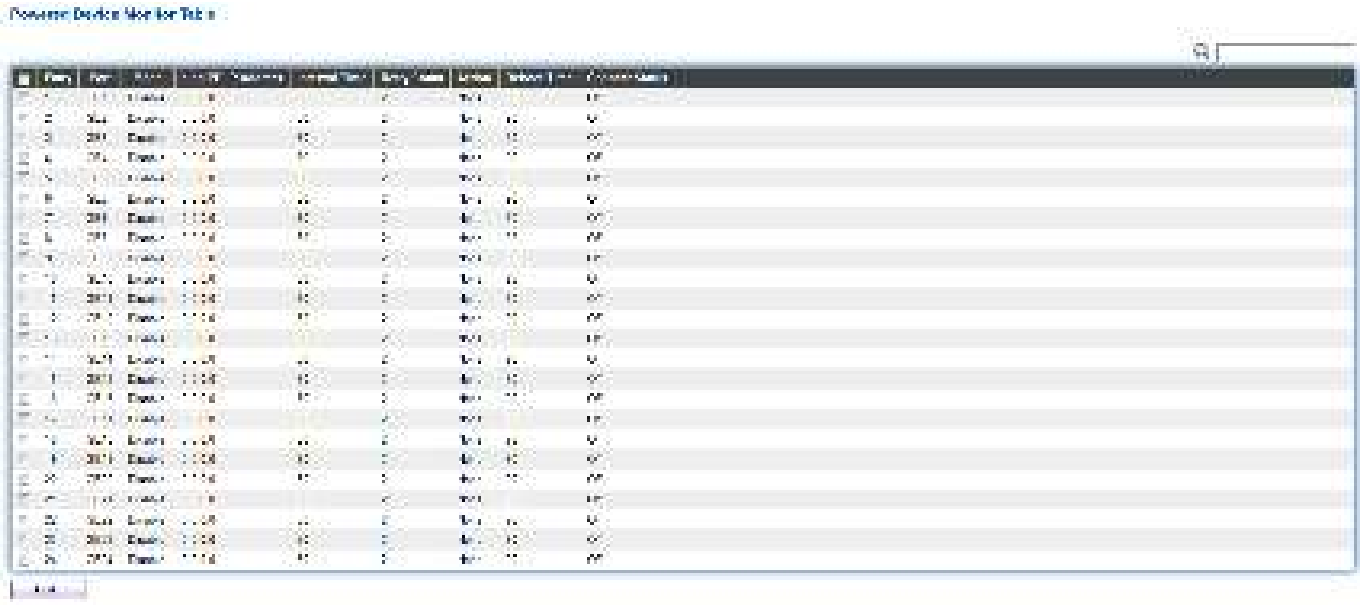


Figure 40 - PoE > Power Stauts

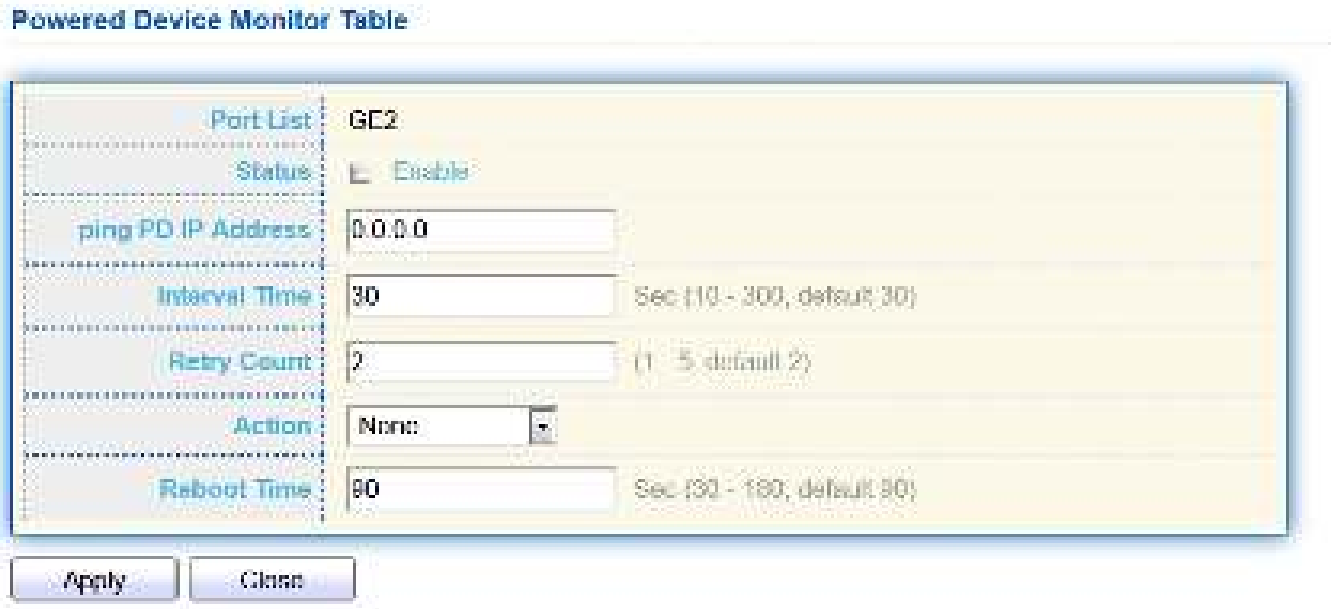
Per Port PoE Status
Checked: Port PoE status is enabled.
Unchecked: Port PoE status is disabled.

IV-4-5 Power Device Monitor

This page shows the information of each ports, including mode, ping PD IP Address, interval time, retry count, action, reboot time and connect status.



To display port setting page, please click the “Edit” button.



Item	Description
Port list	Display the interface of port entry.
Status	Enable/Disable
Ping PD IP Address	Input IP address of the PD
Internal Time	The default setting about Interval (30 seconds) will make switch detect the PD status by performing ping requests every 30 seconds.
Retry Count	If there is no ping reply from the PD, retry count starts to count from 1. Once retry count is reached to 2 times, the switch will perform the action in which you defined.
Action	The Action including none, PD reboot, Reboot & Alarm and Alarm

IV-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 togeth-er even if they are not located on the same network switch. VLAN membership can be configured through software instead of physically relocating devices or connections.

IV-5-1 VLAN

Use the VLAN pages to configure settings of VLAN.

IV-5-1-1 Create VLAN

This page allows user to add or delete VLAN ID entries and browser all VLAN entries that add statically or dynamic learned by GVRP. Each VLAN entry has a unique name, user can edit VLAN name in edit page.

To display Create VLAN page, click **VLAN > VLAN > Create VLAN**.

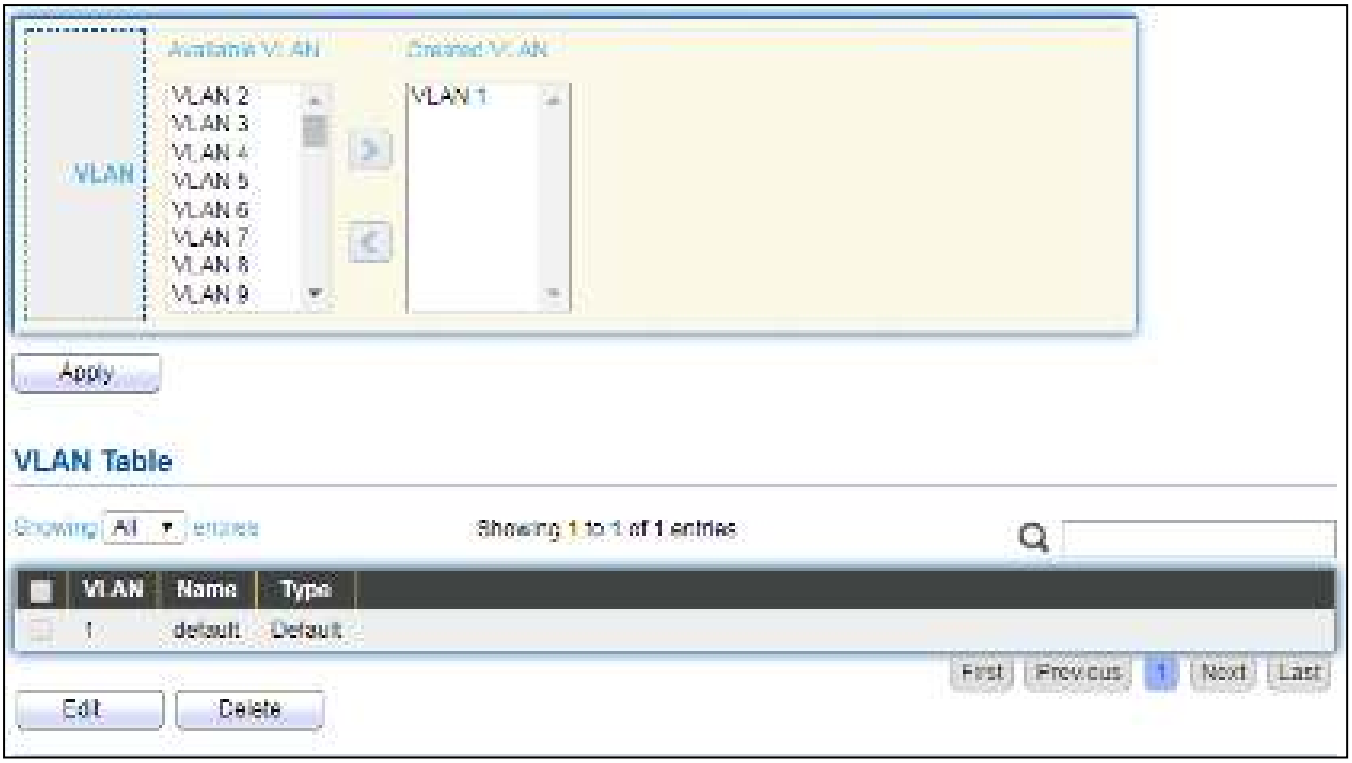


Figure 41 - VLAN > VLAN > Create VLAN

Item	Description
Available VLAN	VLAN has not created yet. Select available VLANs from left box then move to right box to add.
Created VLAN	VLAN had been created. Select created VLANs from right box then move to left box to delete
VLAN	The VLAN ID.
Name	The VLAN Name.
Type	The VLAN Type. ● Static: Port base VLAN. ● Dynamic: 802.1q VLAN.

Click "**Edit**" button to view Edit VLAN Name menu.

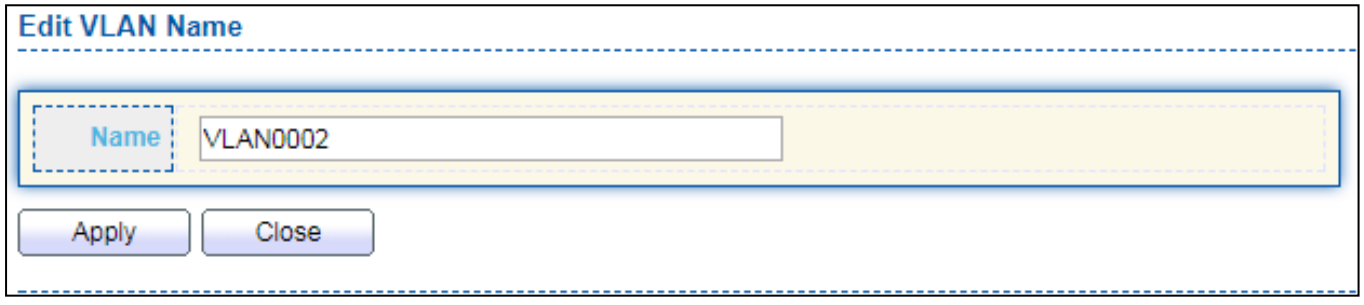


Figure 42 - VLAN > VLAN > Create VLAN > Edit VLAN Name

Item	Description
Name	Input VLAN name.

IV-5-1-2 VLAN Configuration

This page allow user to configure the membership for each port of selected VLAN.

To display VLAN Configuration page, click **VLAN > VLAN > VLAN Configuration**.

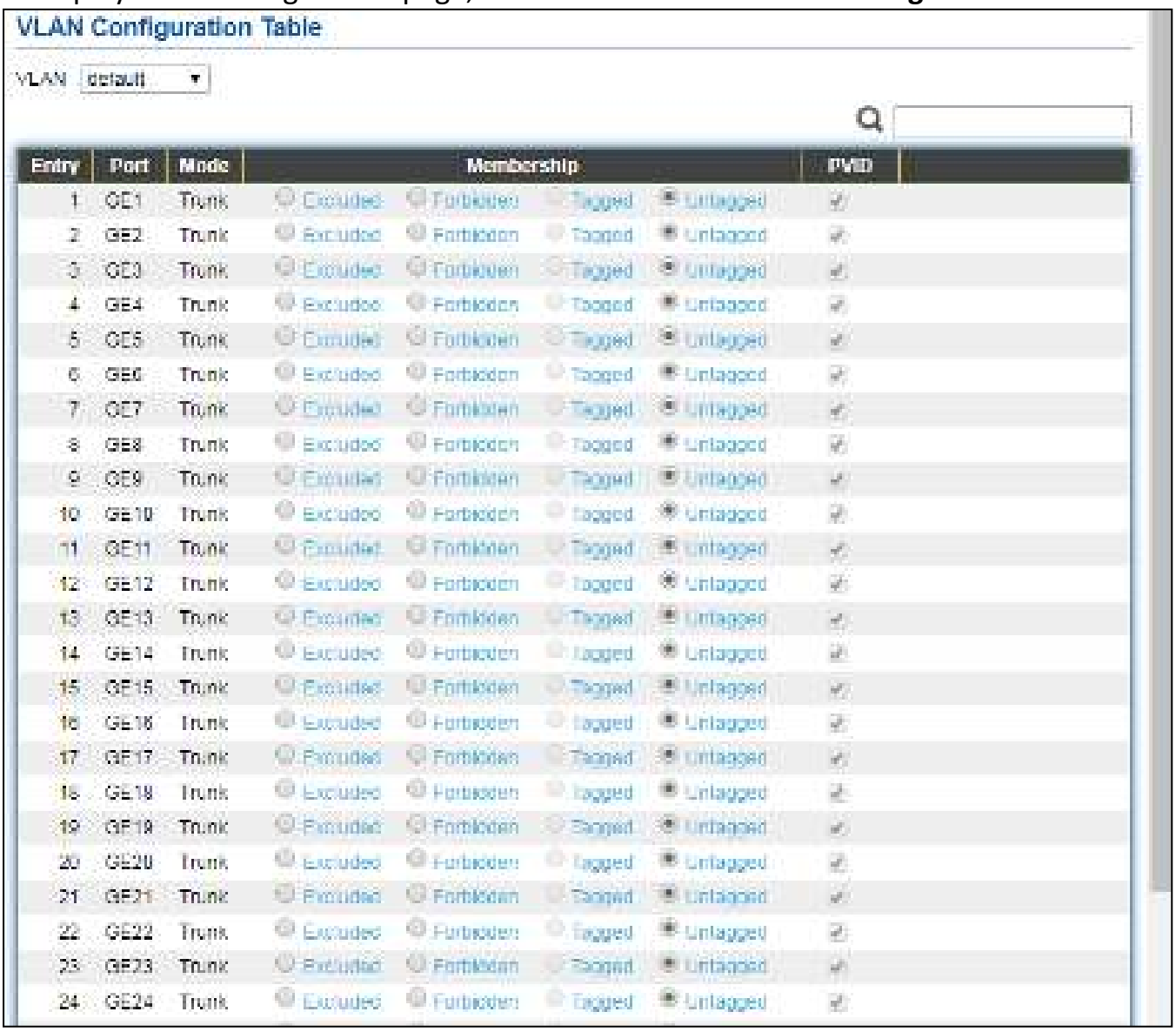


Figure 43 - VLAN > VLAN > VLAN Configuration

Item	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.

IV-5-1-3 Membership

This page allow user to view membership information for each port and edit membership for specified interface.

To display Membership page, click **VLAN > VLAN > Membership**.

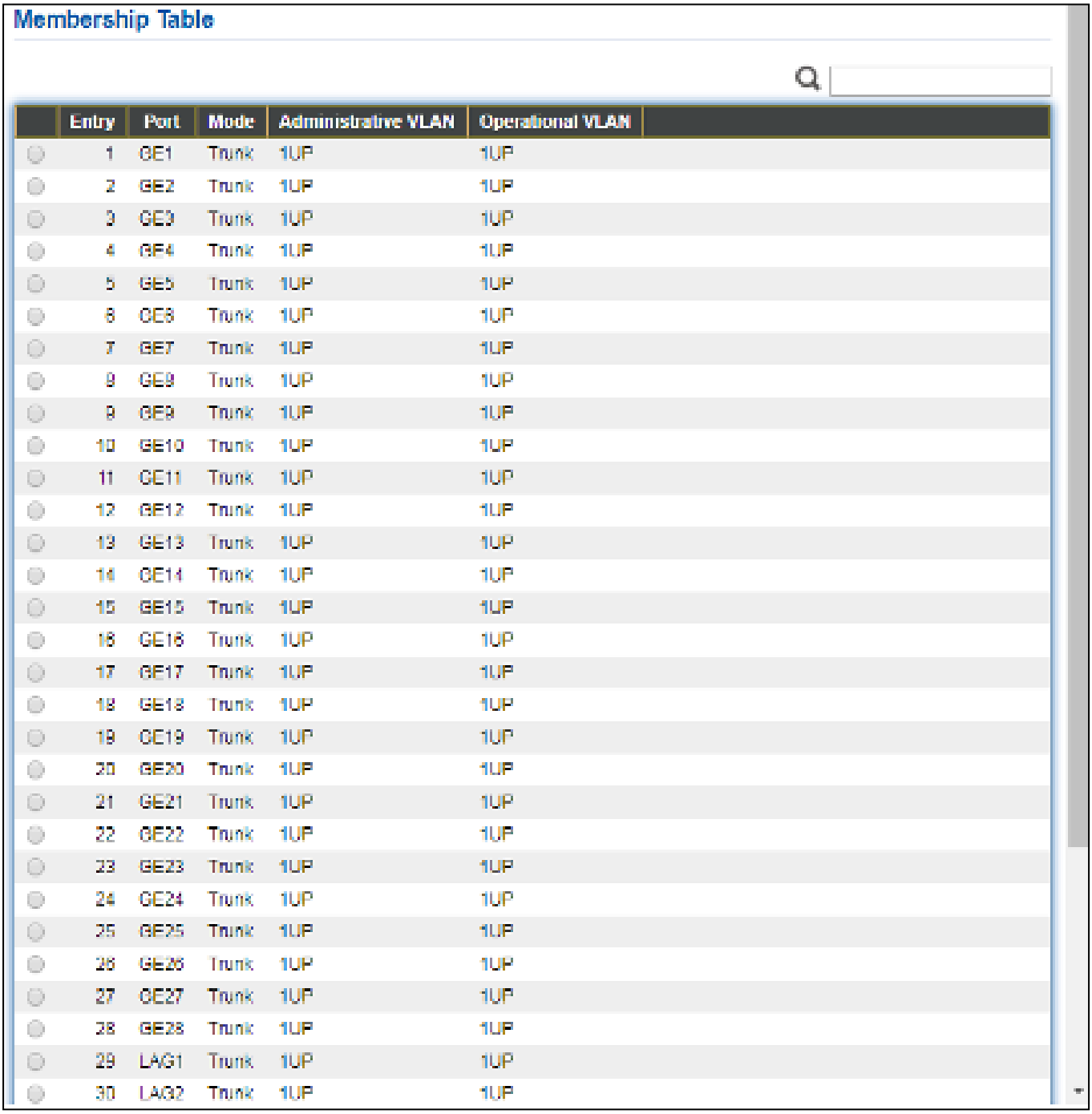


Figure 44 - VLAN > VLAN > Membership

Item	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.

Click "**Edit**" button to view the Edit Port Setting menu

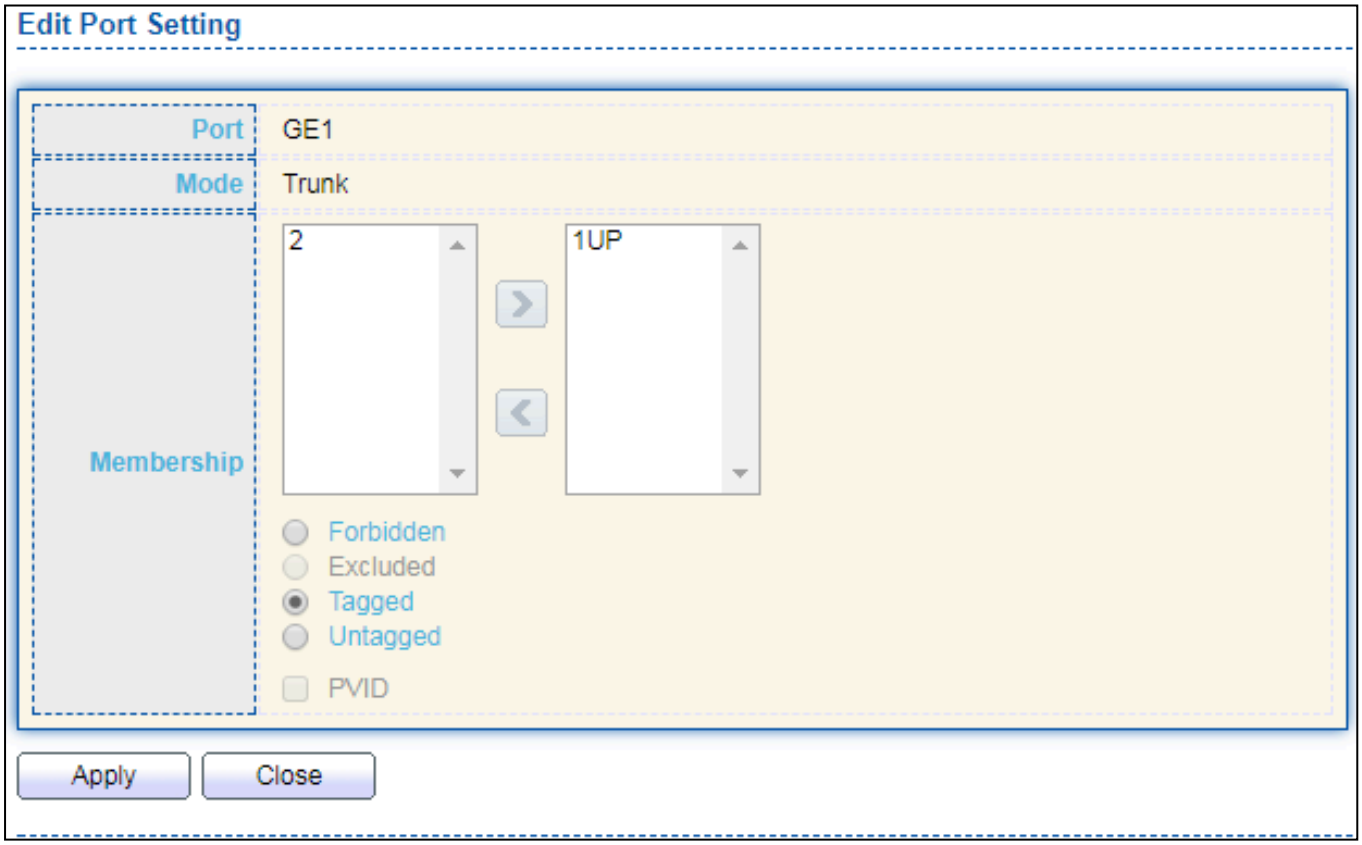


Figure 45 - VLAN > VLAN > Membership > Edit Port Setting

Item	Description
Port	Display the interface.
Mode	Display the VLAN mode of interface.
Membership	Select VLANs of left box and select one of following membership then move to right box to add membership. Select VLANs of right box then move to left box to remove membership. Tagging membership may not choose in differ VLAN port mode. Select the time source. ● Forbidden: Set VLAN as forbidden VLAN. ● Excluded: This option is always disabled. ● Tagged: Set VLAN as tagged VLAN. ● Untagged: Set VLAN as untagged VLAN. ● PVID: Check this checkbox to select the VLAN ID to be the port-based VLAN ID for this port. PVID may auto select or can't select in differ settings.

IV-5-1-4 Port Setting

This page allow user to configure ports VLAN settings such as VLAN port mode, PVID etc…The attributes depend on different VLAN port mode.

To display Port Setting page, click **VLAN > VLAN > Port Setting**.

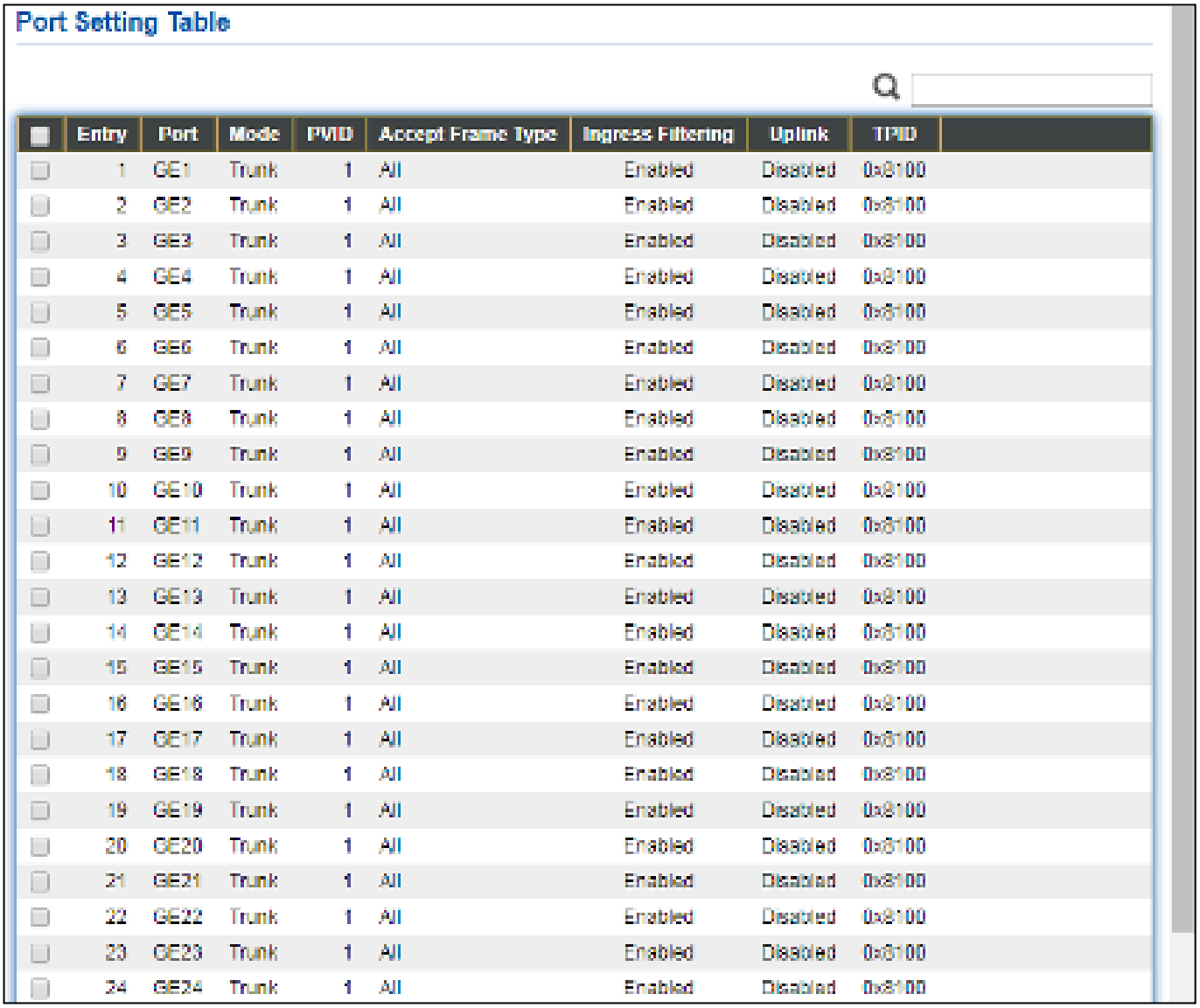


Figure 46 - VLAN > VLAN > Port Setting

Item	Description
Port	Display the interface.
Mode	Display the VLAN mode of interface.
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.

Click “**Edit**” button to Edit Port Setting menu.

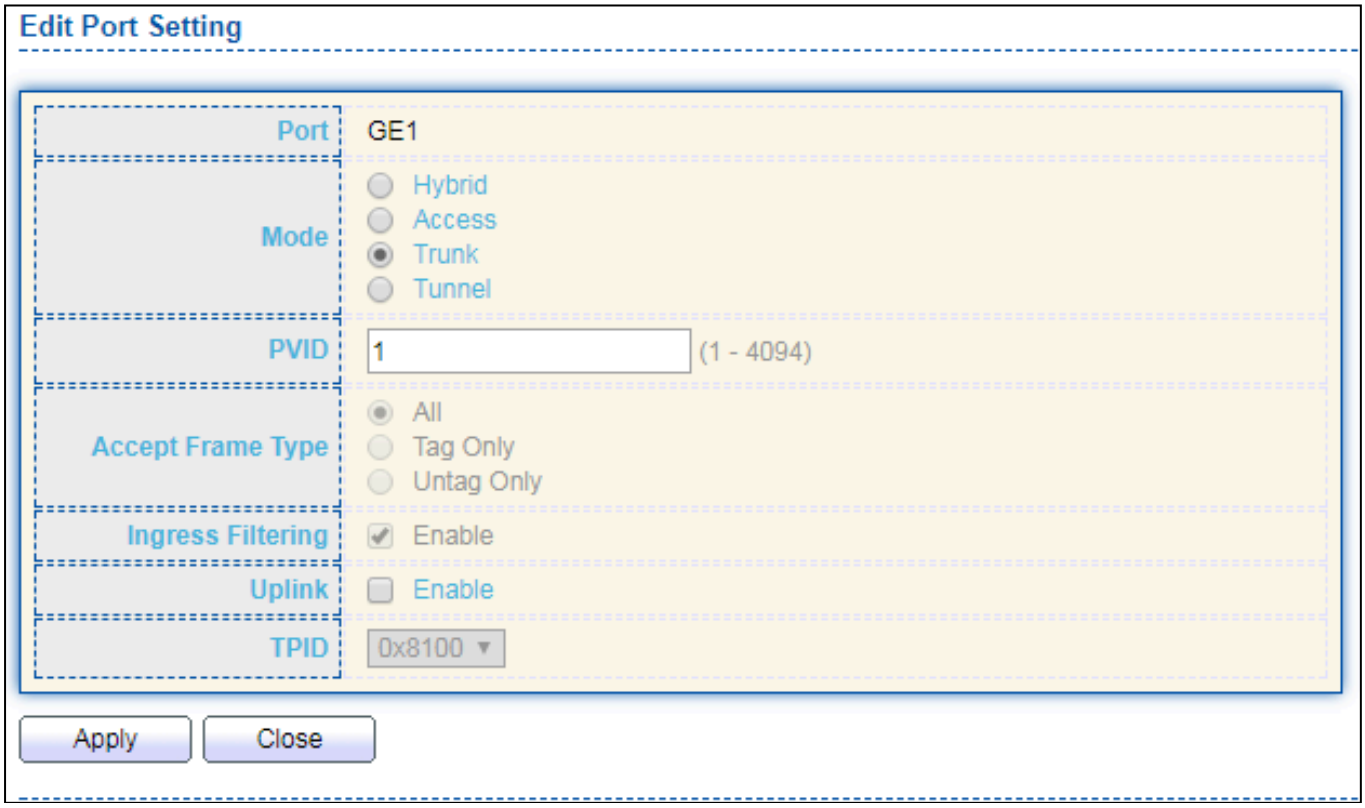


Figure 47 - VLAN > VLAN > Port Setting > Edit Port Setting

Item	Description
Port	Display selected port to be edited.
Mode	Select the VLAN mode of the interface. ● Forbidden: Set VLAN as forbidden VLAN. ● Hybrid: Support all functions as defined in IEEE 802.1Q specification. ● Access: Accepts only untagged frames and join an untagged VLAN. ● Trunk: An untagged member of one VLAN at most, and is a tagged member of zero or more VLANs.
PVID	Specify the port-based VLAN ID (1-4094). It's only available with Hybrid and Trunk mode.
Accepted Type	Specify the acceptable-frame-type of the specified interfaces. It's only available with Hybrid mode.
Ingress Filtering	Set checkbox to enable/disable ingress filtering. It's only available with Hybrid mode.
Uplink	Set checkbox to enable/disable uplink mode. It's only available with trunk mode.
TPID	Select TPID used of interface. It's only available with trunk mode.

IV-5-2 Voice VLAN

Use the Voice VLAN pages to configure settings of Voice VLAN.

IV-5-2-1 Property

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

To display Property Web page, click **VLAN> Voice VLAN> Property**.

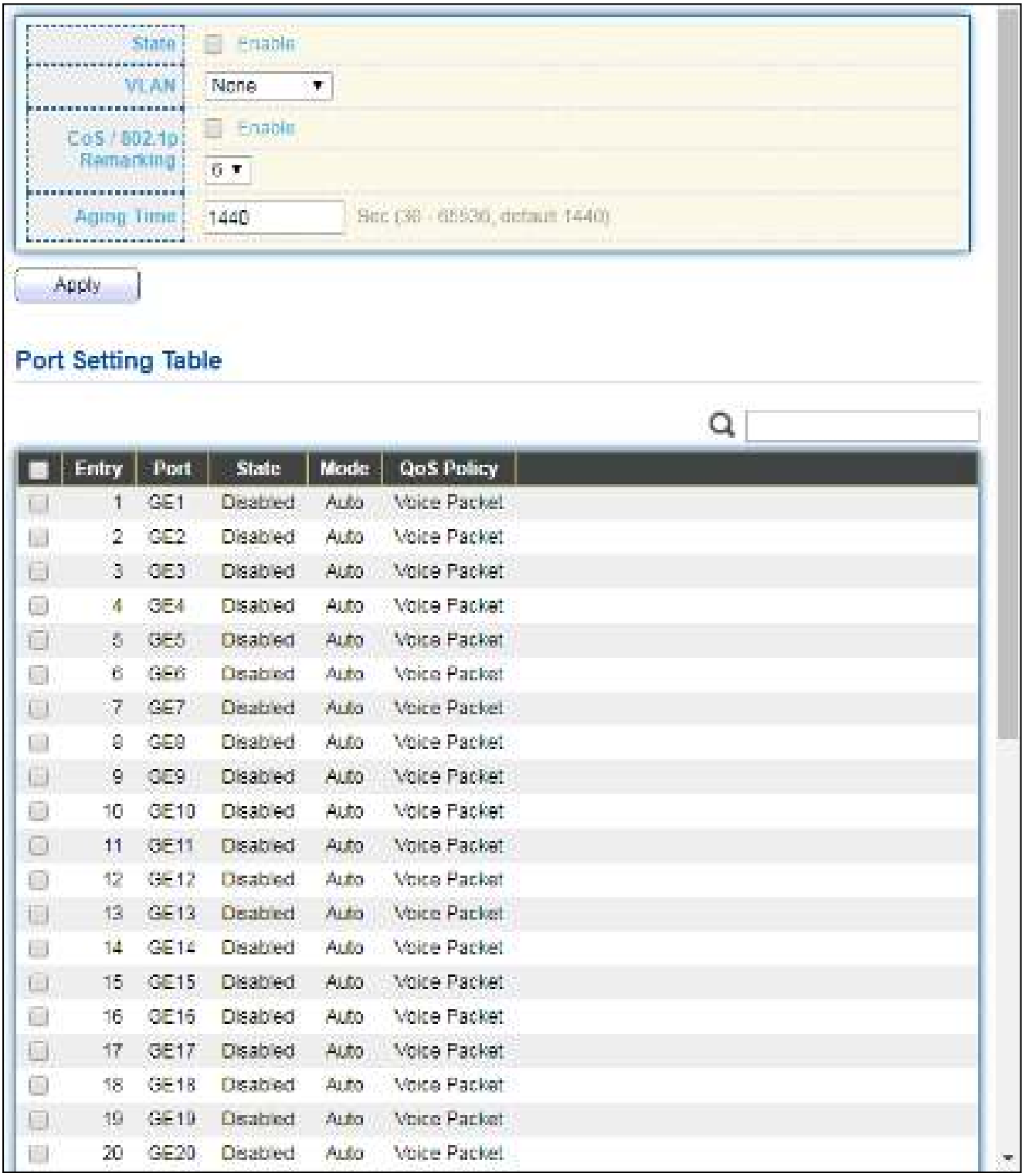


Figure 48 - VLAN > Voice VLAN > Property

Item	Description
State	Set checkbox to enable or disable voice VLAN function.
VLAN	Select Voice VLAN ID. Voice 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 voice VLAN entry will be age out after this time if without any packet pass through.
Port Setting Table	
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.

Click "**Edit**" button to view Edit Port Setting menu.

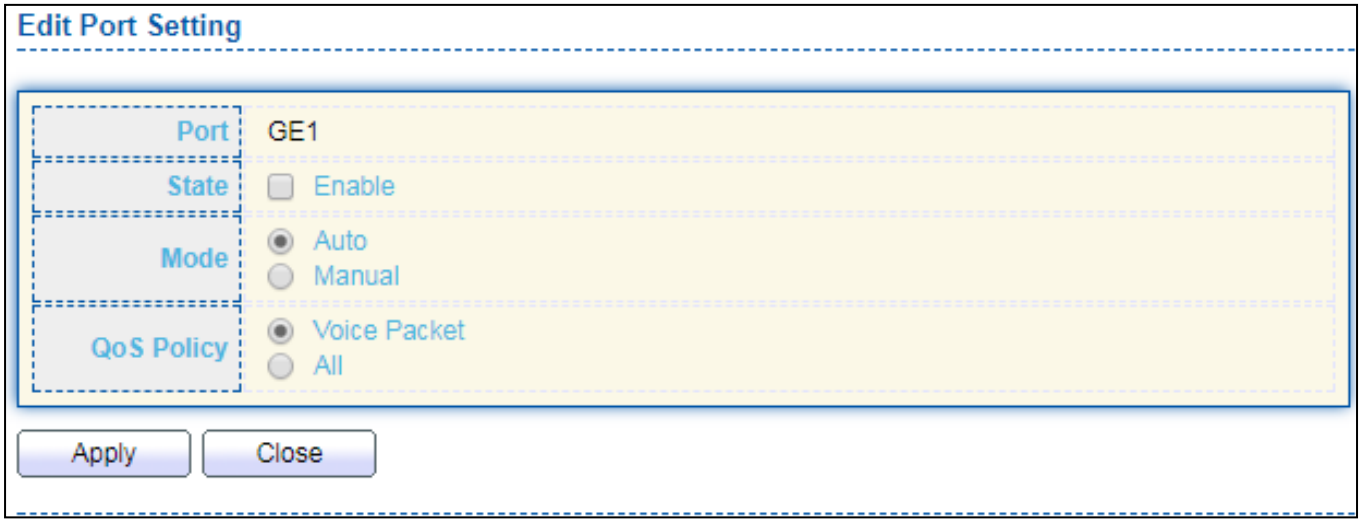


Figure 49 - VLAN > Voice VLAN > Property > Edit Port Setting

Item	Description
Port	Display selected port to be edited.
State	Set checkbox to enable/disabled voice VLAN function of interface.
Mode	Select port voice VLAN mode ● Auto: Voice VLAN auto detect packets that match OUI table and add received port into voice VLAN ID tagged member. ● Manual: User need add interface to VLAN ID tagged member manually.
QoS Policy	Select port QoS Policy mode ● Voice 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 Voice VLAN.

IV-5-2-2 Voice OUI

This page allow user to add, edit or delete OUI MAC addresses. Default has 8 pre-defined OUI MAC.

To display the Voice OUI Web page, click **VLAN > Voice VLAN > Voice OUI**.

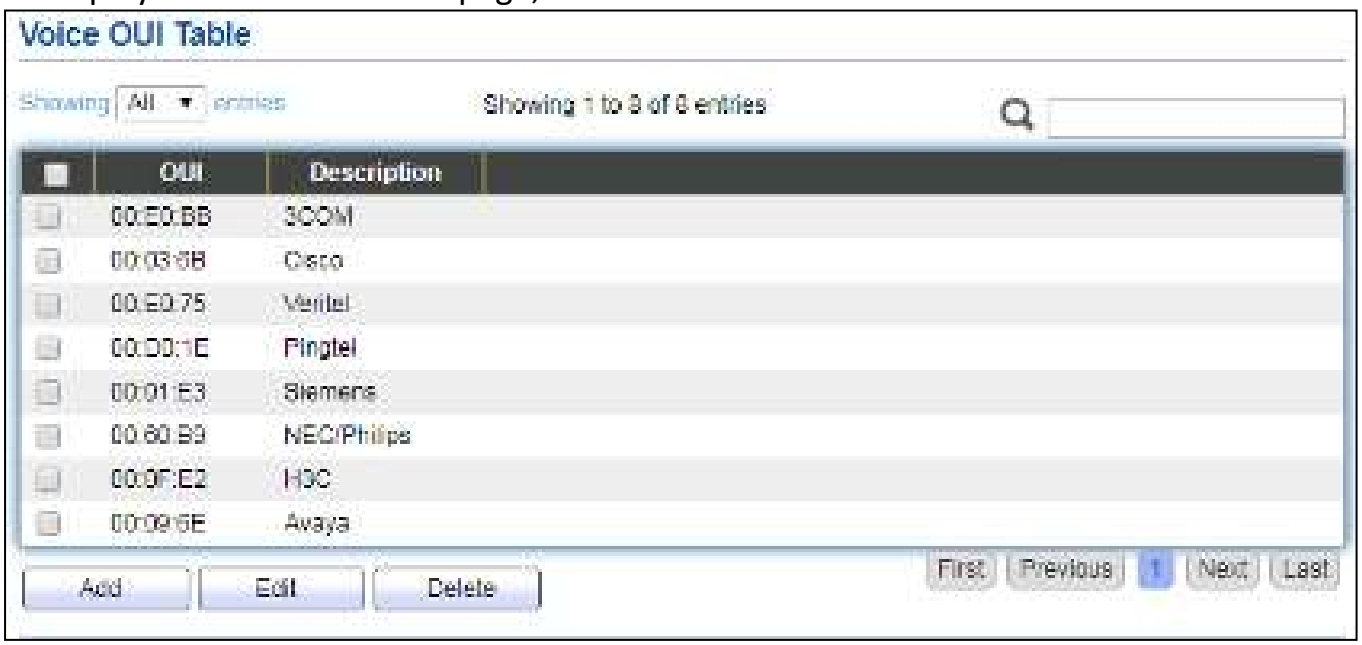


Figure 50 - VLAN > Voice VLAN > Voice OUI

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

Click “Add” or “Edit” button to Add/Edit Voice OUI menu.

Figure 51 - VLAN > Voice VLAN > Voice OUI > Add/Edit Voice OUI

Item	Description
OUI	Input OUI MAC address. Can’t be edited in edit dialog.
Description	Input description of the specified MAC address to the voice VLAN OUI table.

IV-5-3 MAC VLAN

Use the MAC VLAN pages to configure settings of MAC VLAN.

IV-5-3-1 MAC Group

This page allow user to add or edit groups settings of MAC VLAN.

To display the MAC page , click **VLAN > MAC VLAN > MAC Group**.

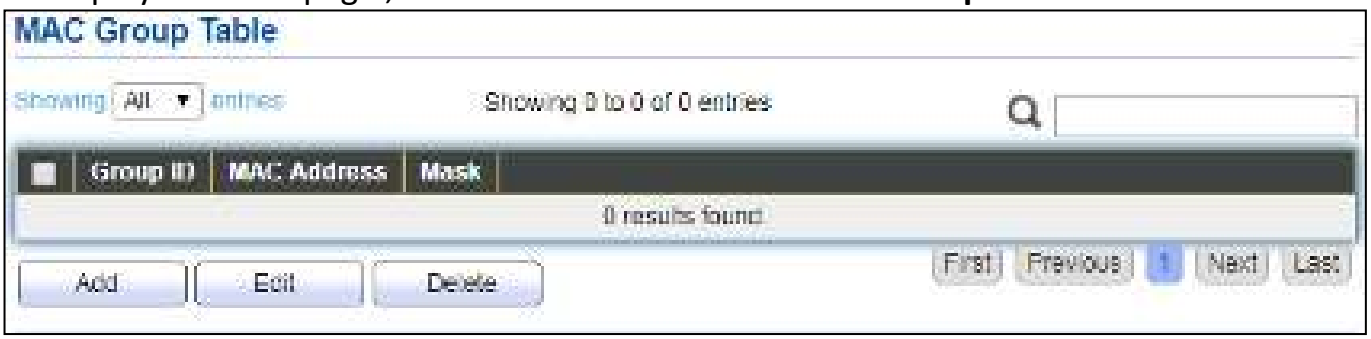


Figure 52 - VLAN > MAC VLAN > MAC Group

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

Click “**Add**” button or "**Edit**" button to view Add/Edit MAC menu.

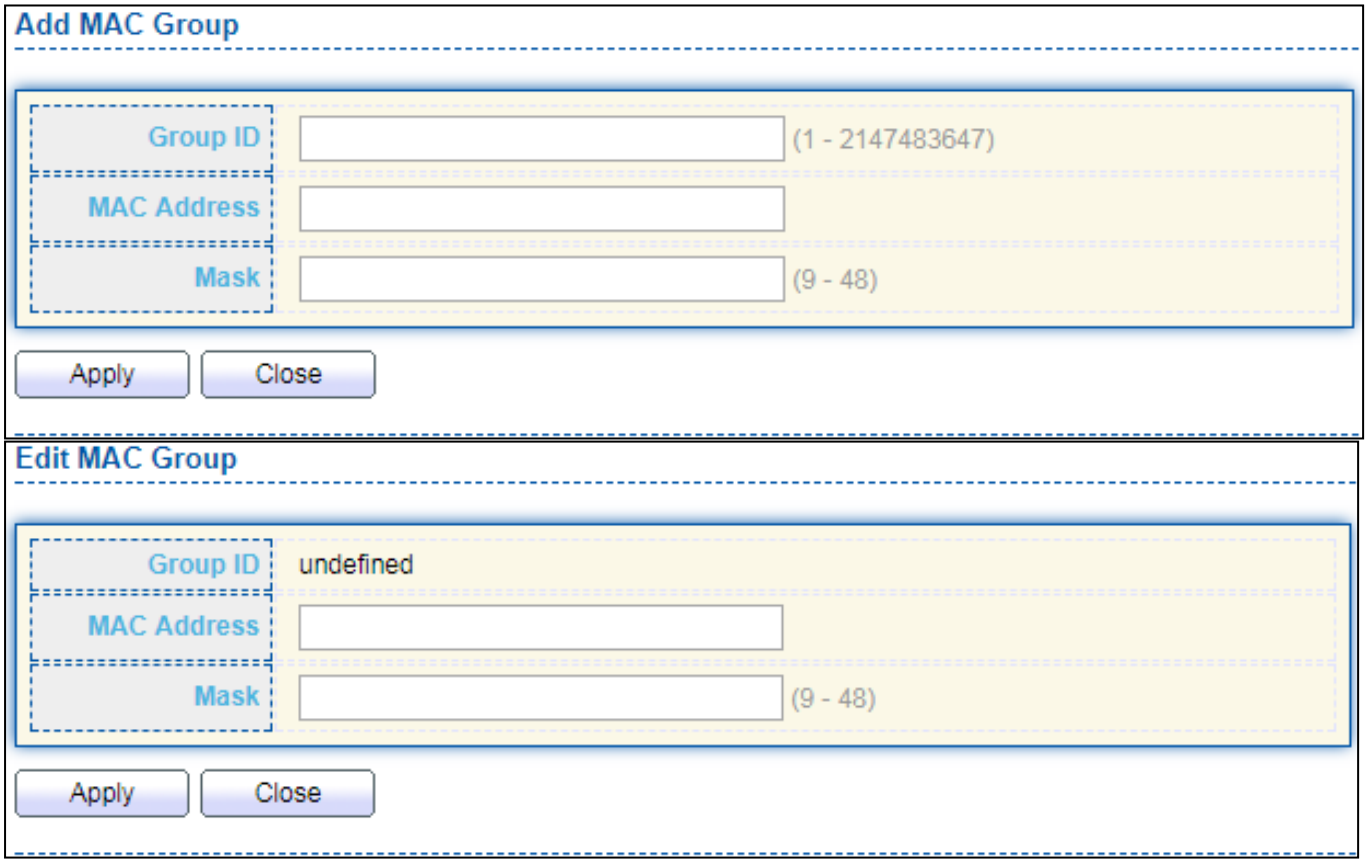


Figure 53 - VLAN > MAC VLAN > MAC Group > Add/Edit MAC

Item	Description
Group ID	Input group ID that is a unique ID of mac group entry. The range from 1 to 2147483647. Only available on Add Dialog.
MAC Address	Input mac address for classifying packets.
Mask	Input mask of mac address.

IV-5-3-2 Group Binding

This page allow user to bind MAC VLAN group to each port with VLAN ID.

To display Group Binding page, click **VLAN> MAC VLAN > Group Binding**.

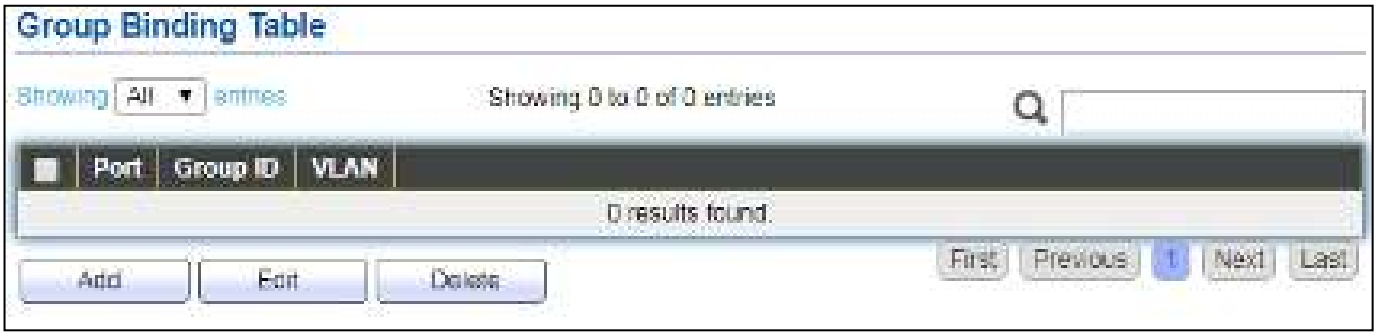


Figure 54 - VLAN > MAC VLAN > Group Binding

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

Click “**Add**” or “**Edit**” button to view the Add/Edit Group Binding menu.

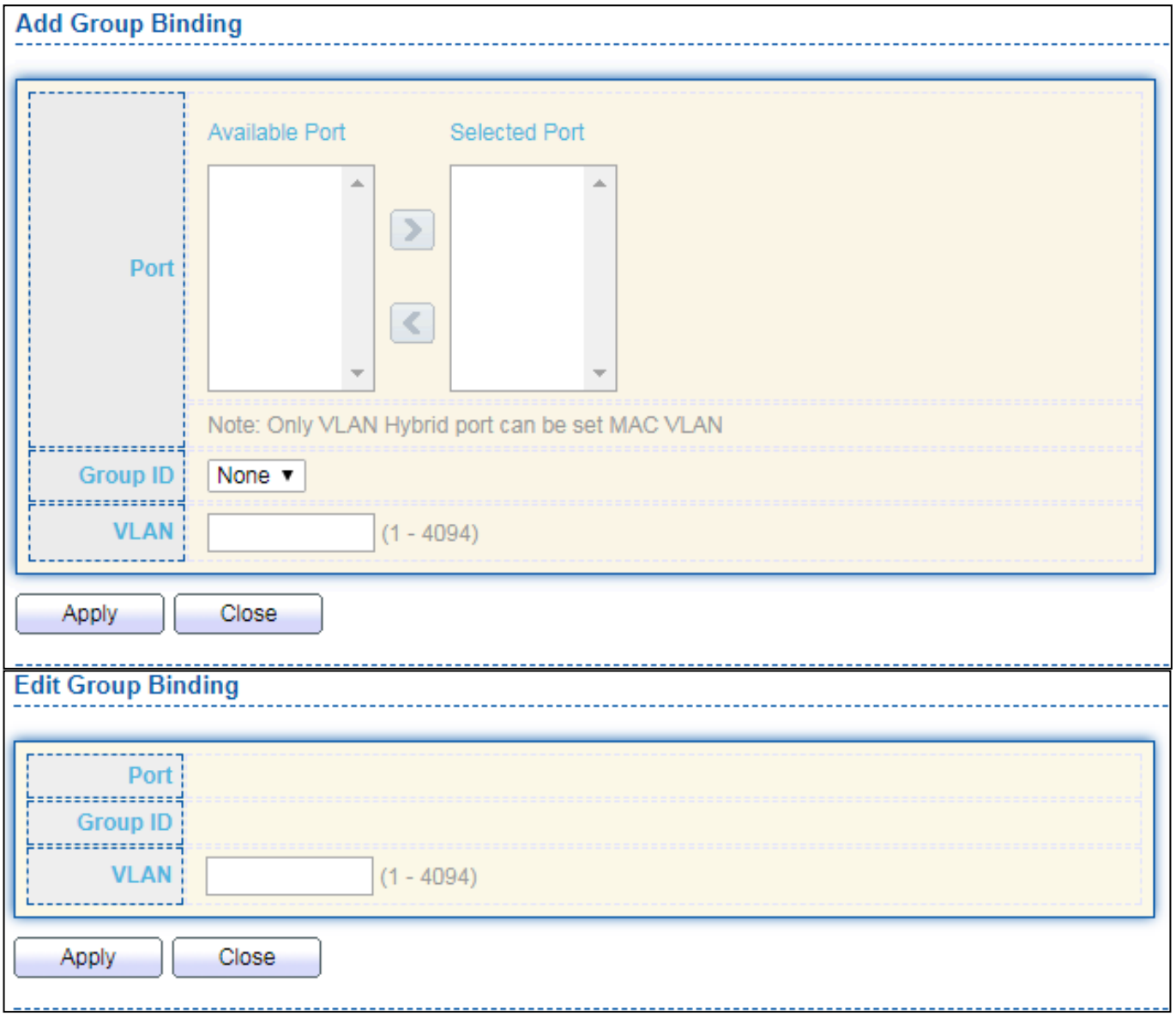


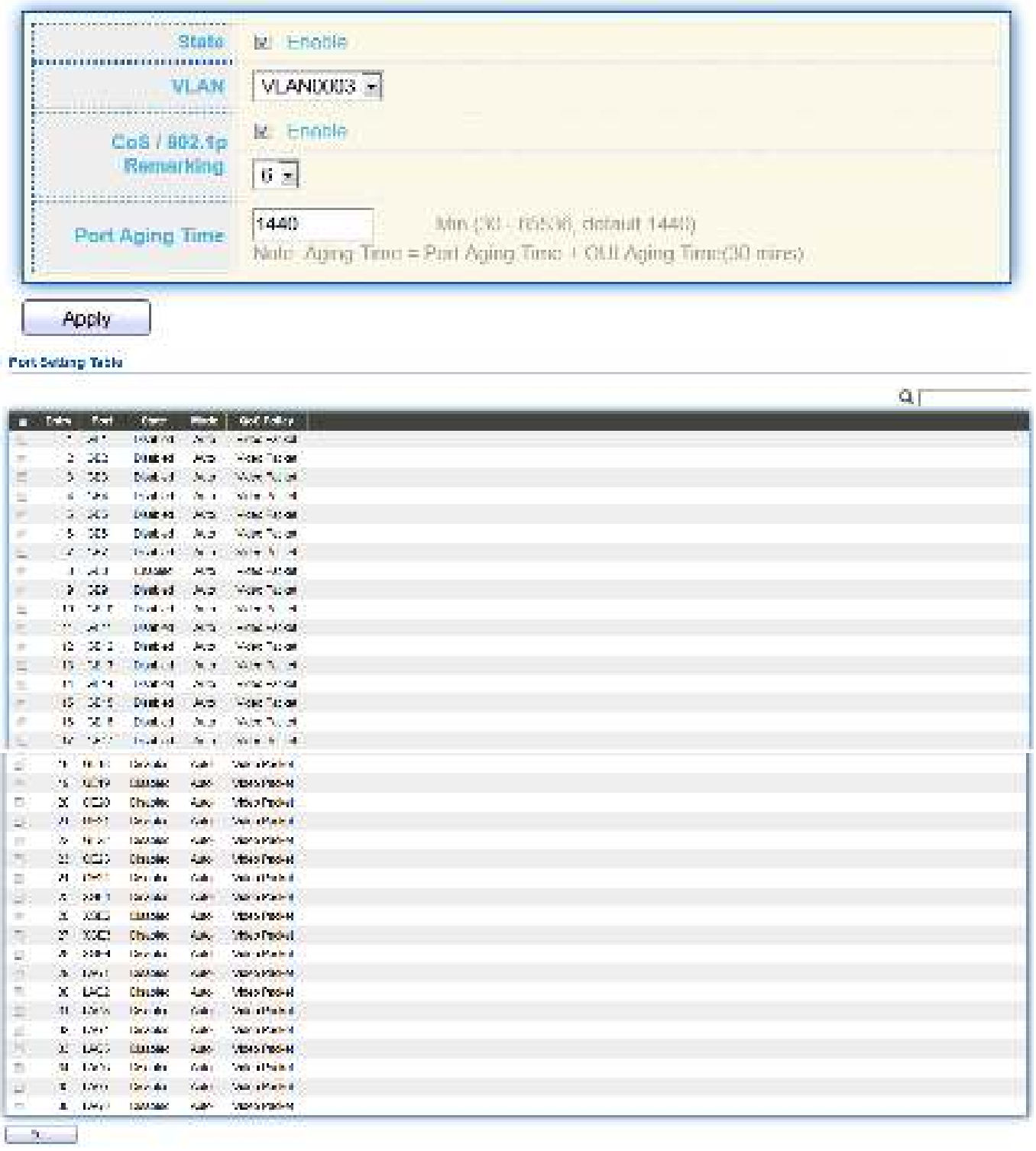
Figure 55 - VLAN > MAC VLAN > Add/Edit Group Binding

Item	Description
Port	Select ports in left box then move to right to binding with MAC group. Or select ports in right box then move to left to unbind with MAC 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 MAC group.

IV-5-4 Surveillance VLAN

Use the Surveillance VLAN pages to configure settings of Surveillance VLAN.

IV-5-4-1 Property



Item	Description
State	Enable/Disable
VLAN	Choose none or indicate VLAN
CoS/802.1p Remarking	The 802.1p standard defines seven levels of CoS from 0 through to 7 (highest priority). 802.1p is a sub-set of the 802.1q standard which added additional fields into the header of a standard Ethernet frame allowing it to contain VLAN identifiers as well as the priority values.
Port Aging Time	When aging is configured on an interface that's using port security, all the dynamically learned secure addresses age out when the aging time expire

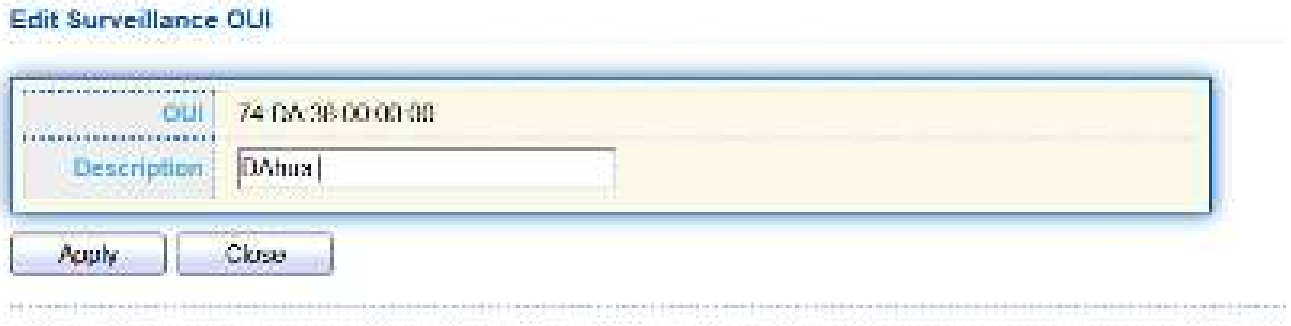
To display Port Setting page, click the “Edit” button.

Item	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.

IV-5-4-2 Surveillance OUI

Item	Description
OUI	An organizationally unique identifier (OUI) is a 24-bit number that uniquely identifies a vendor, manufacturer, or other organization. ... In MAC addresses, the OUI is combined with a 24-bit number (assigned by the assignee of the OUI) to form the address.
OUI Mask	Specifies a set of MAC addresses using a bit mask to indicate the bits of the MAC addresses that must fit to the specified MAC address attribute.

To change the description of your IP camera, click the “Edit” button.



IV-6 MAC Address Table

Use the MAC Address Table pages to show dynamic MAC table and configure settings for static MAC entries.

IV-6-1 Dynamic Address

To display the Dynamic Address web page, click **MAC Address Table > Dynamic Address**.

Figure 56 - MAC Address Table > Dynamic Address

Item	Description
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.

IV-6-2 Static Address

To display the Static Address web page, click **MAC Address Table > Static Address**.

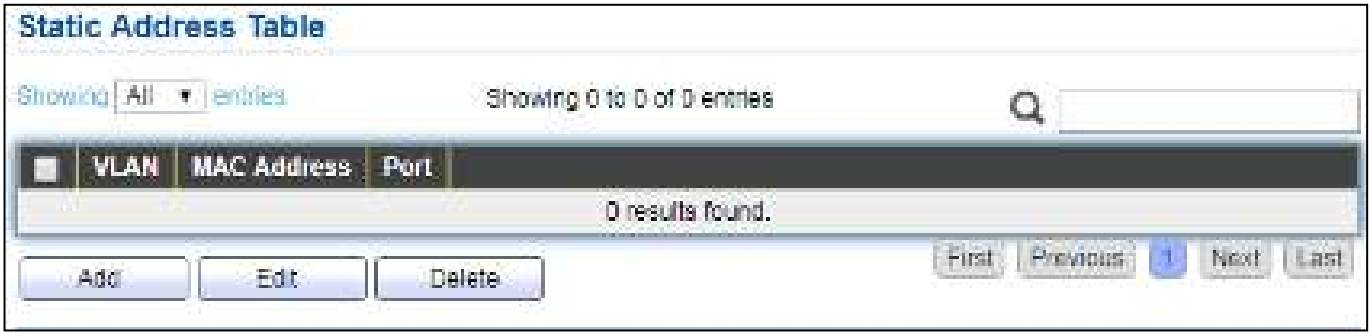


Figure 57 - MAC Address Table > Static Address.

Item	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.

IV-6-3 Filtering Address

To display the Filtering Address web page, click **MAC Address Table > Filtering Address**.

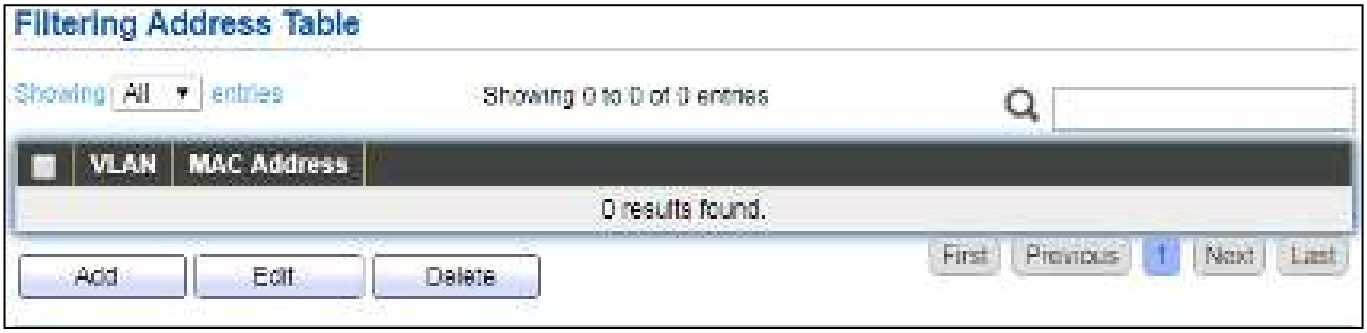


Figure 58 - MAC Address Table > Filtering Address.

Item	Description
MAC Address	Specify unicast MAC address in the packets to be dropped.
VLAN	Specify the VLAN to show or clear MAC entries.

IV-7 Spanning Tree

The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network.

IV-7-1 Property

To display the Property web page, click **Spanning Tree > Property**.

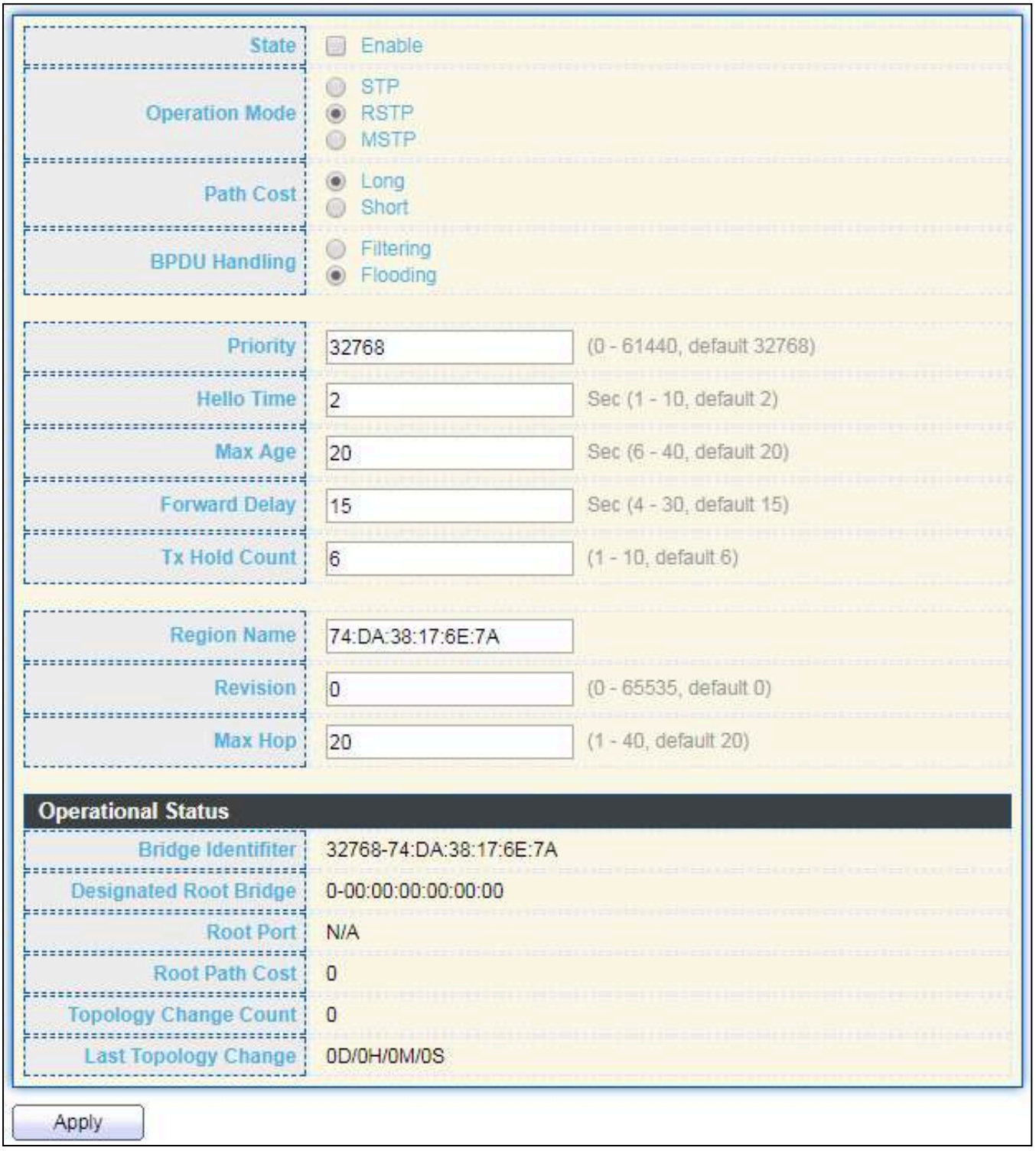


Figure 59 - Spanning Tree > Property

Item	Description
State	Enable/disable the STP on the switch.
Operation Mode	Specify the STP operation mode. ● STP: Enable the Spanning Tree (STP) operation. ● RSTP: Enable the Rapid Spanning Tree (RSTP) operation. ● MSTP: Enable the Multiple Spanning Tree (MSTP) operation.
Path Cost	Specify the path cost method. ● 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	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	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	Specify the STP hello time in second to broadcast its hello message to other bridges by Designated Ports. Its valid range is from 1 to 10 seconds.
Max Age	Specify 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	The MSTP revision number. Its valid rage is from 0 to 65535.
Max Hop	Specify the number of hops in an MSTP region before the BPDU is discarded. The valid range is 1 to 40.
Operational Status	
Bridge Identifier	Bridge identifier of the switch.
Designated Root Identifier	Bridge identifier of the designated root bridge.
Root Port	Operational root port of the switch.
Root Path Cost	Operational root path cost.
Topology Change Count	Numbers of the topology changes.

Last Topology Change	The last time for the topology change.

IV-7-2 Port Setting

To configure and display the STP port settings, click **STP > Port Setting**.

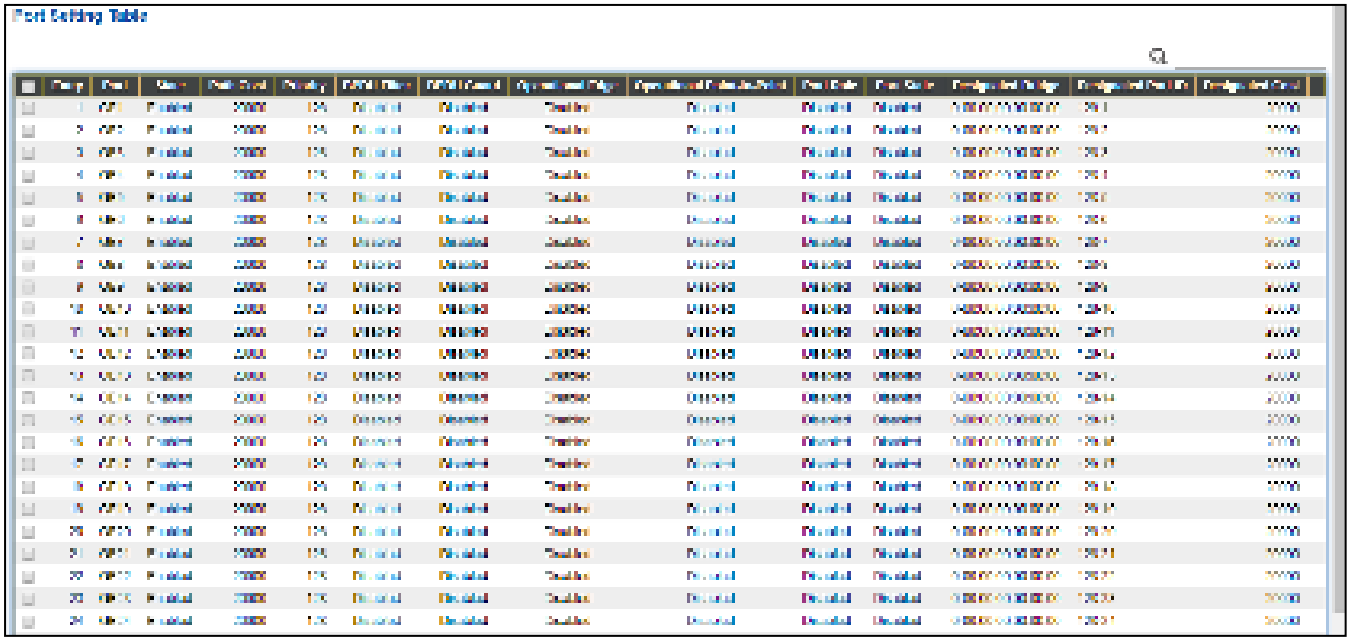


Figure 60 - Spanning Tree > Port Setting

Item	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.

Protocol Migration Check	Restart the Spanning Tree Protocol (STP) migration process (re-negotiate with its neighborhood) on the specific interface.

Click "**Edit**" button to view Edit Port Setting menu.

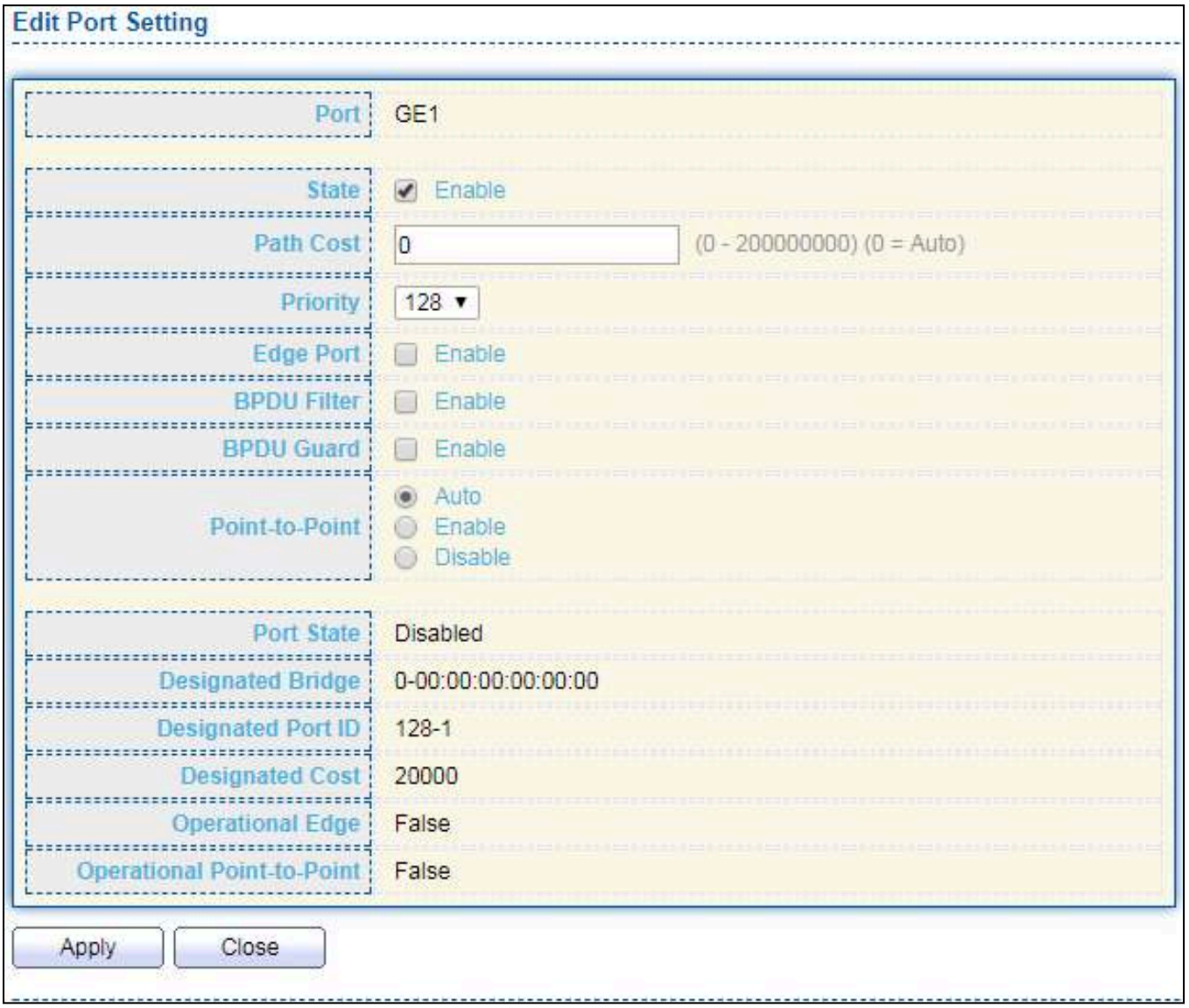


Figure 61 - Spanning Tree > Port Setting > Edit Port Setting

Item	Description
Port	Selected port ID.
State	Enable/Disable the STP on the specified port.
Path Cost	Specify the STP path cost on the specified port.
Priority	Specify the STP path cost on the specified port.
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 Guard	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

IV-7-3 MST Instance

To configure MST instance setting, click **STP > MST Instance**.

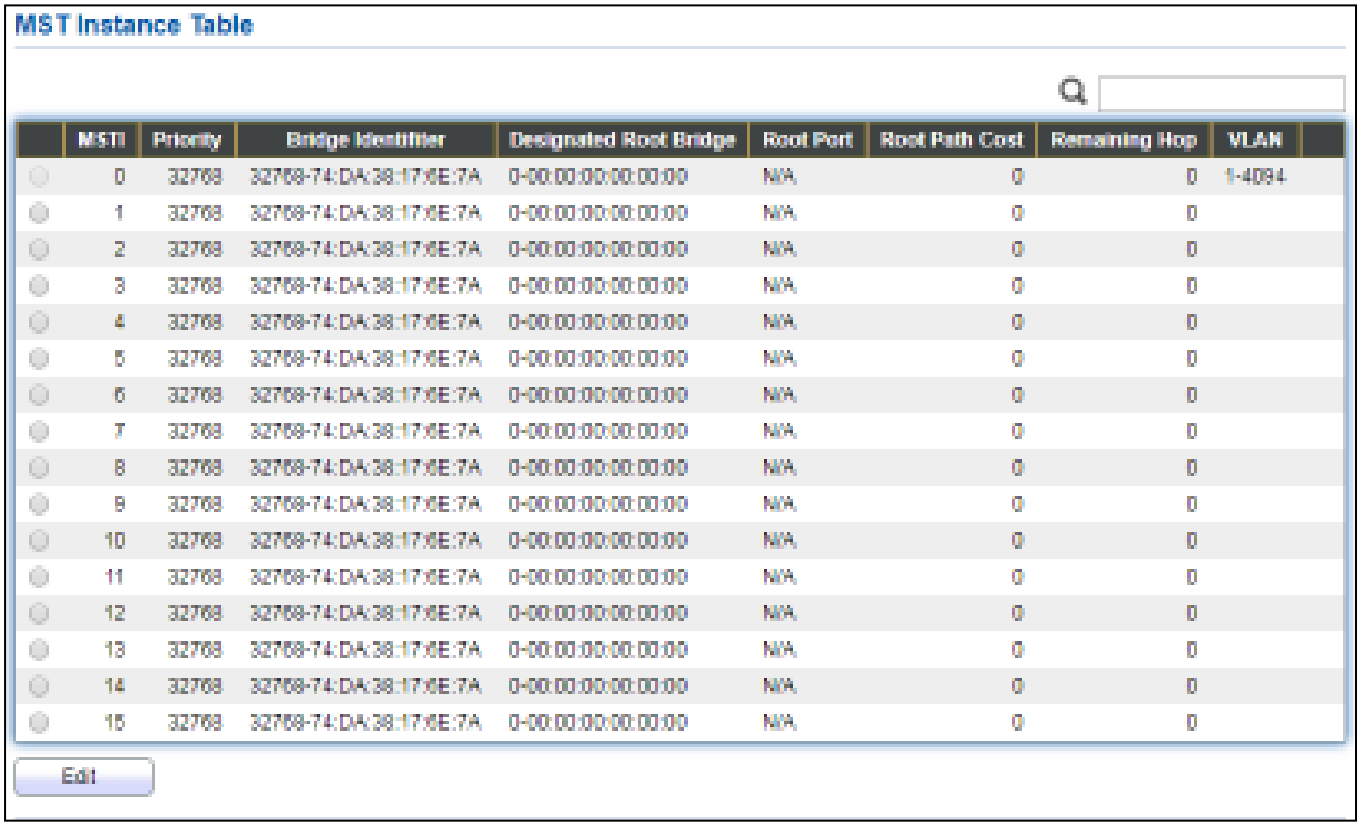


Figure 62 - Spanning Tree > MST Instance

Item	Description
MSTI	Designated port number.
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.

Click "**Edit**" button to view Edit MST Instance menu.

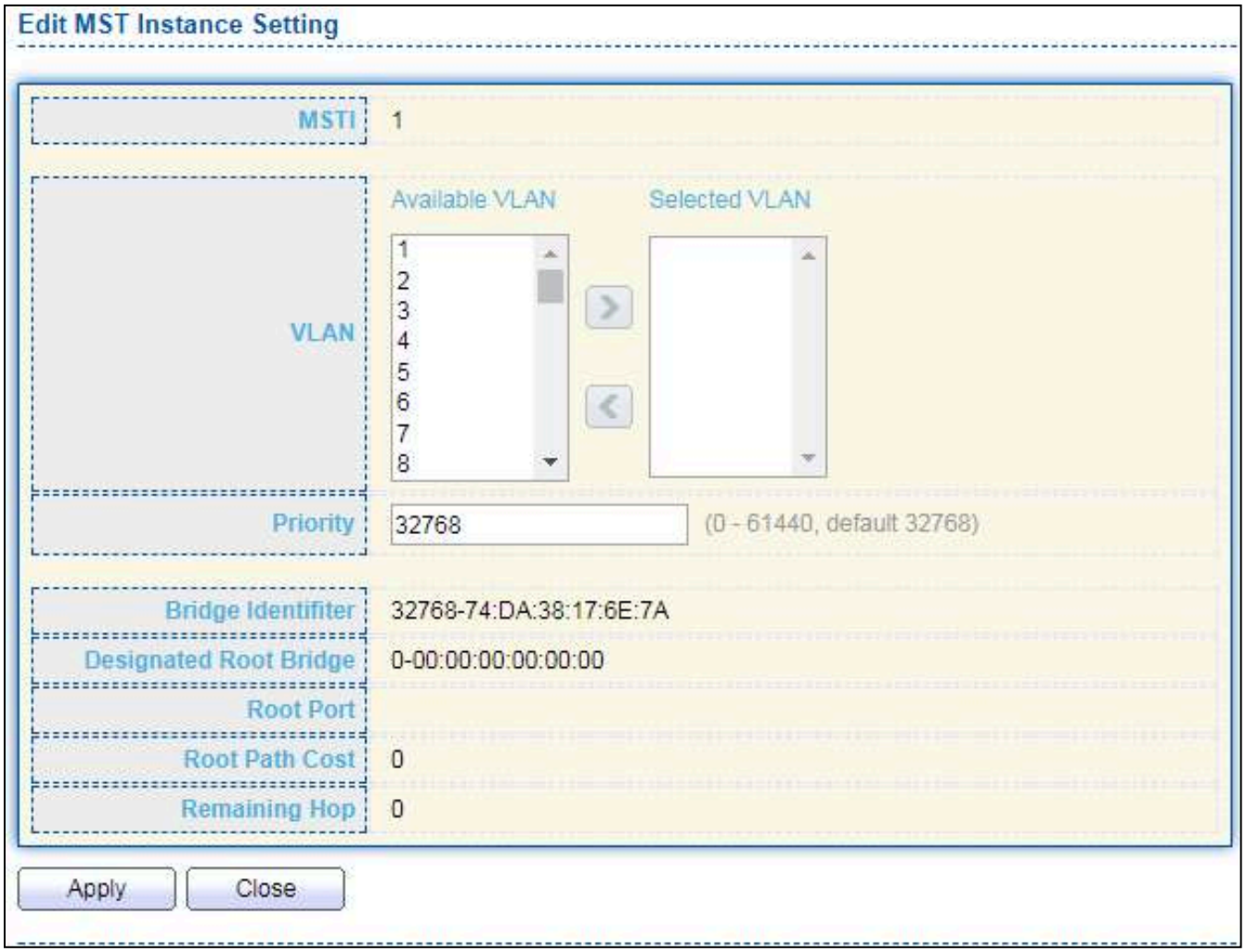


Figure 63 - Spanning Tree > MST Instance > Edit MST Instance Setting

Item	Description
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.

IV-7-4 MST Port Setting

To configure and display MST port setting, click **STP > MST Port Setting**.

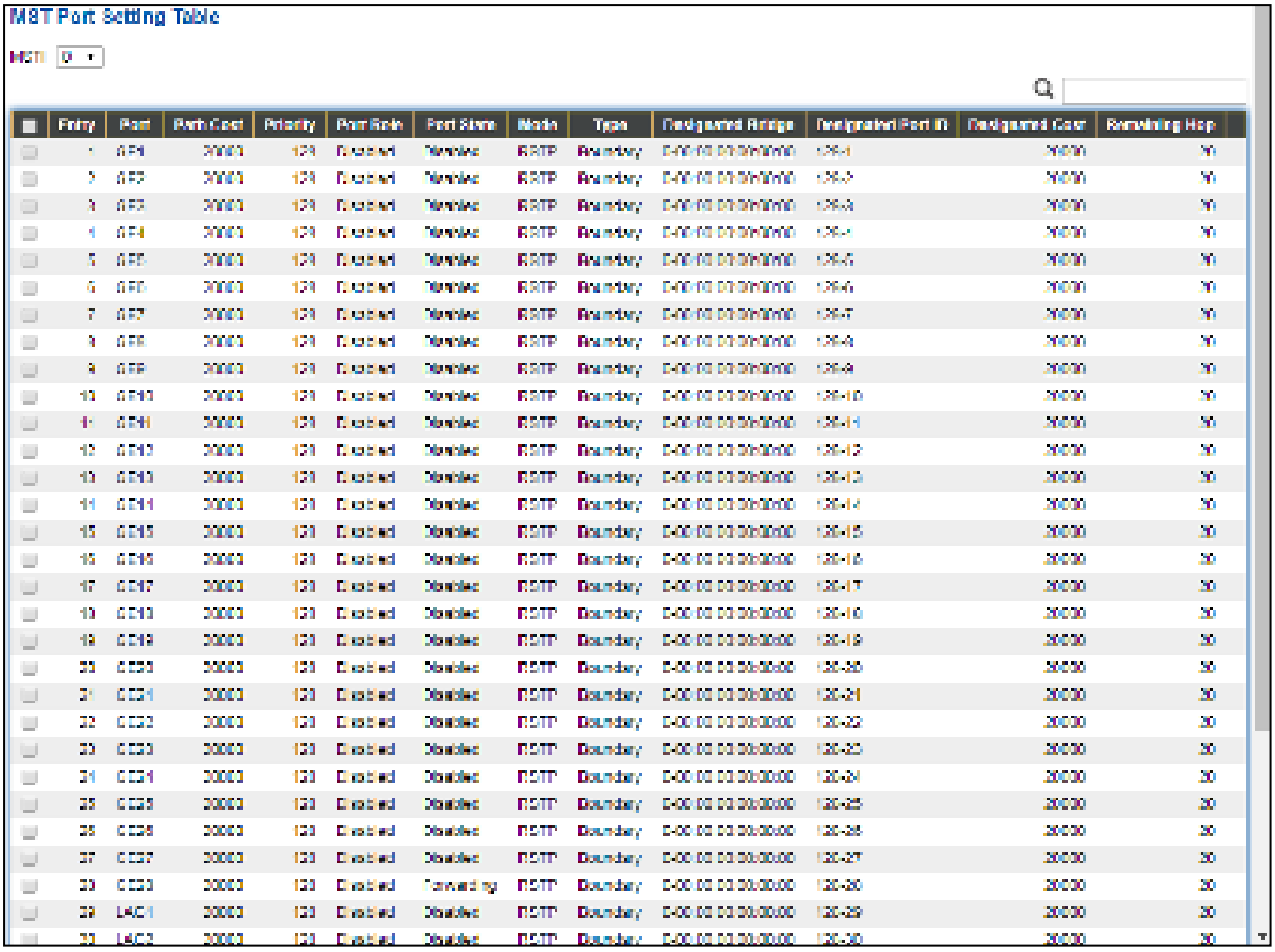


Figure 64 - Spanning Tree > MST Port Setting

Item	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.

Click "**Edit**" button to view Edit MST Port Setting menu.

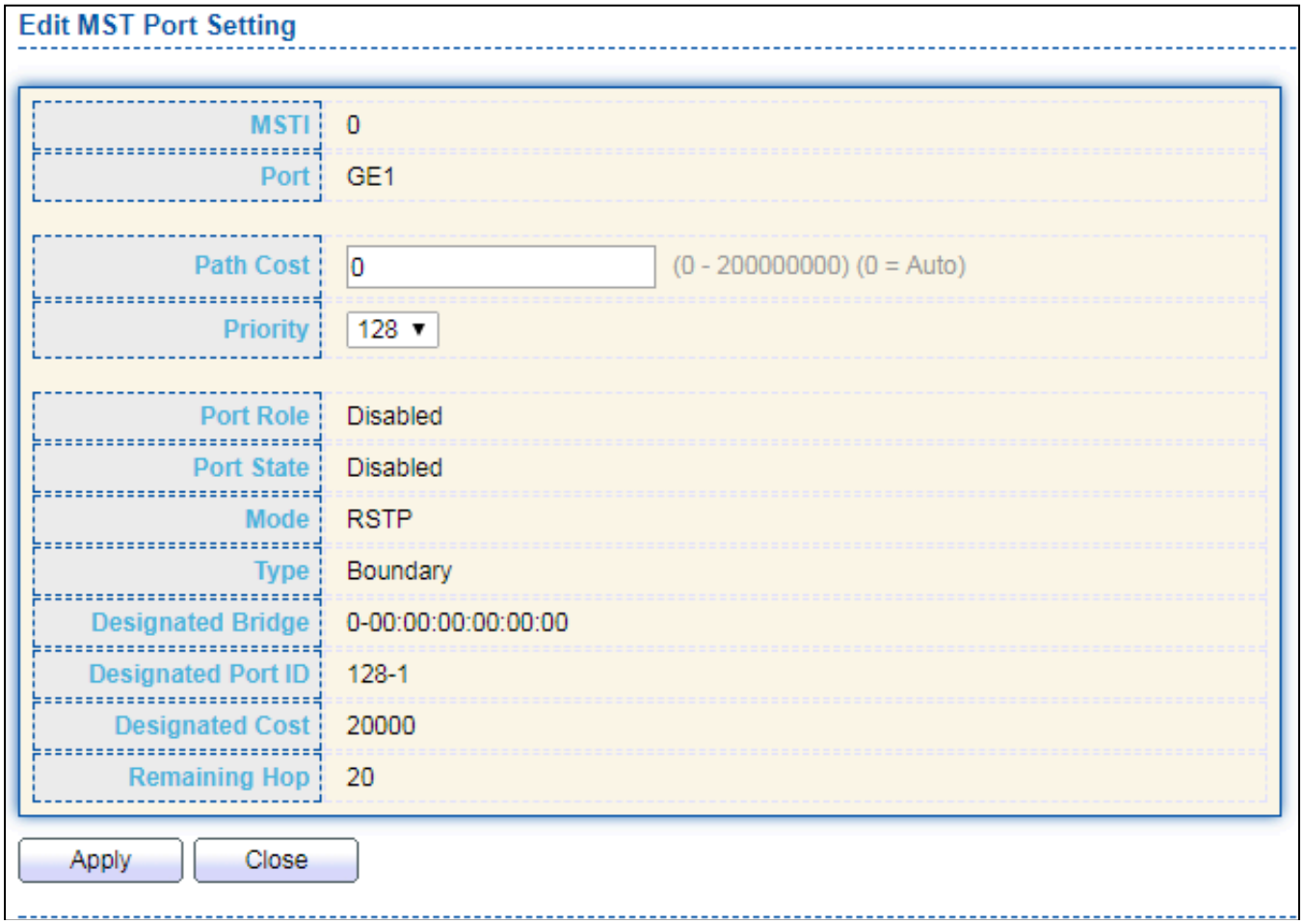


Figure 65 - Spanning Tree > MST Port Setting > Edit MST Port Setting

Item	Description
Path Cost	Specify the STP port path cost on the specified MSTI.
Priority	Specify the STP port priority on the specified MSTI.

IV-7-5 Statistics

To display the STP statistics, click **STP > Statistics**.

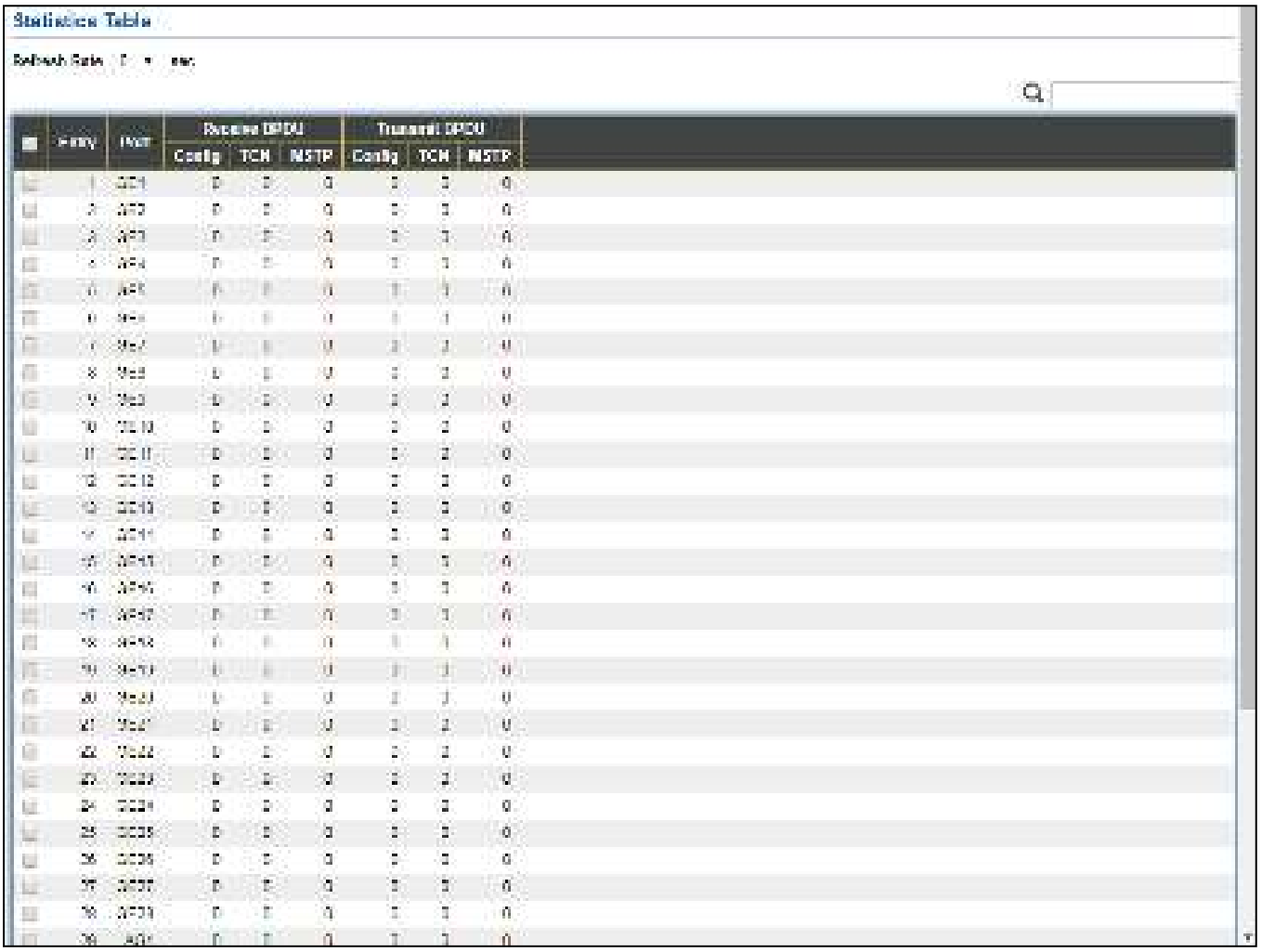


Figure 66 - Spanning Tree > Statistics

Item	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.

Click "**View**" button to view the STP Port Statistic menu.

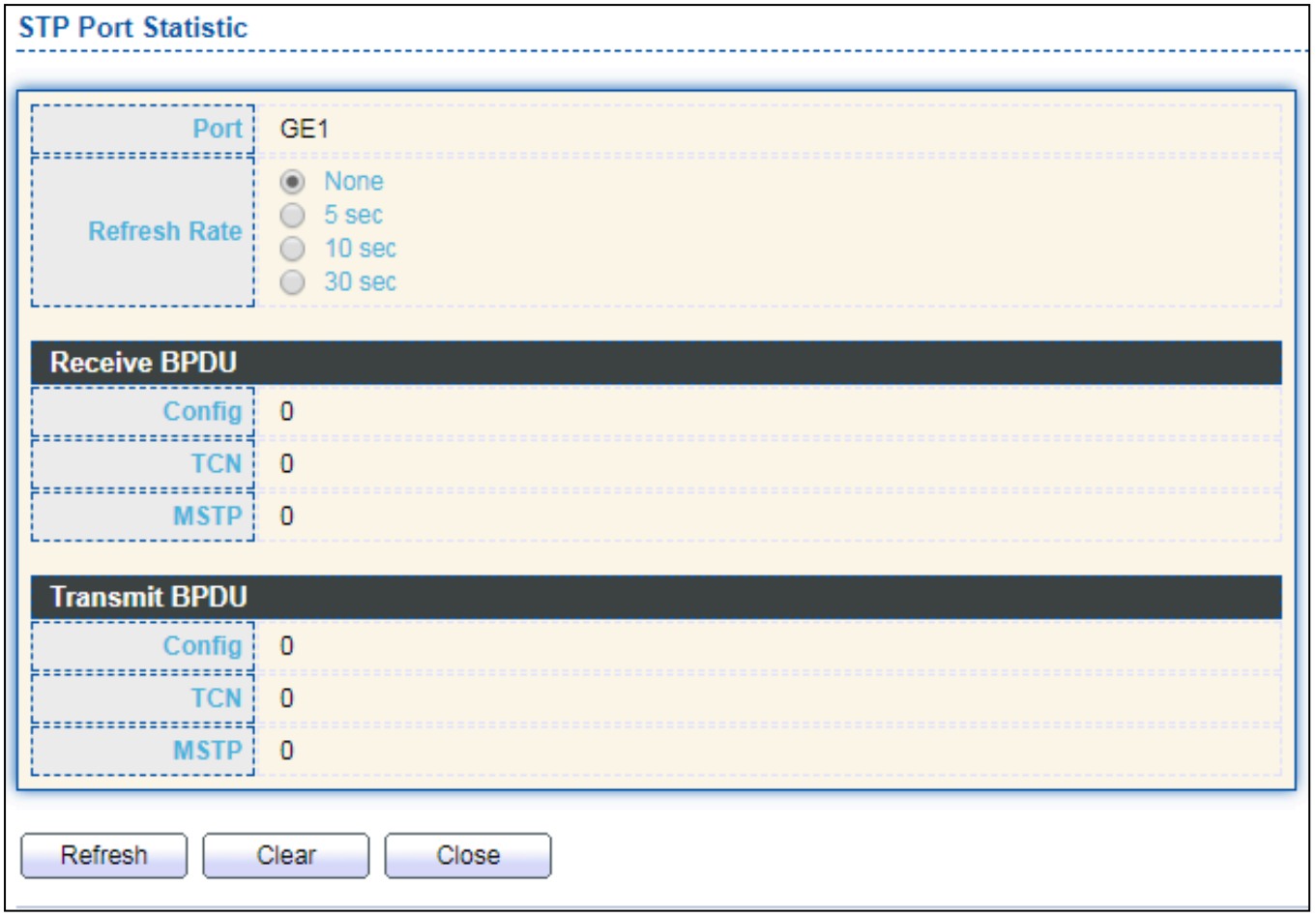


Figure 67 - Spanning Tree > Statistics > STP Port Statistic

Item	Description
Refresh Rate	The option to refresh the statistics automatically.
Clear	Clear the statistics for the selected interfaces.

IV-8 Discovery

Use this section to configure LLDP.

IV-8-1 LLDP

LLDP is a one-way protocol; there are no request/response sequences. Informa-tion is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function. The LLDP category contains LLDP and LLDP-MED pages.

IV-8-1-1 Property

To display LLDP Property Setting web page, click **Discovery > LLDP > Property**.

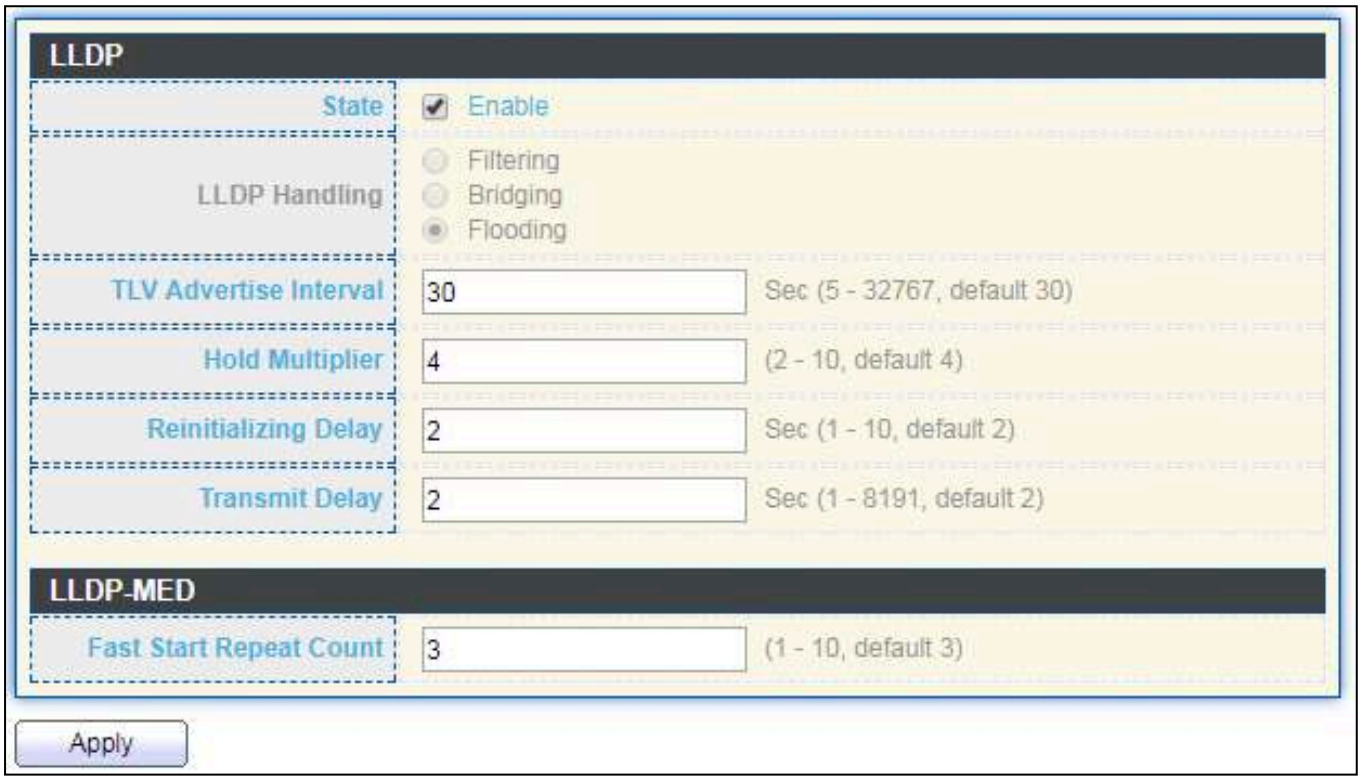


Figure 68 - Discovery > LLDP > Property

Item	Description
State	Enable/ Disable LLDP protocol on this switch.
LLDP Handling	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	Select the interval at which frames are transmitted. The default is 30

Interval	seconds, and the valid range is 5–32767 seconds.
Holdtime Multiplier	Select the multiplier on the transmit interval to assign to TTL (range 2–10, default = 4).
Reinitialization Delay	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	Select fast start repeat count when port link up (range 1–10, default = 3).

IV-8-1-2 Port Setting

To display LLDP Port Setting, click **Discovery > LLDP > Port Setting**.

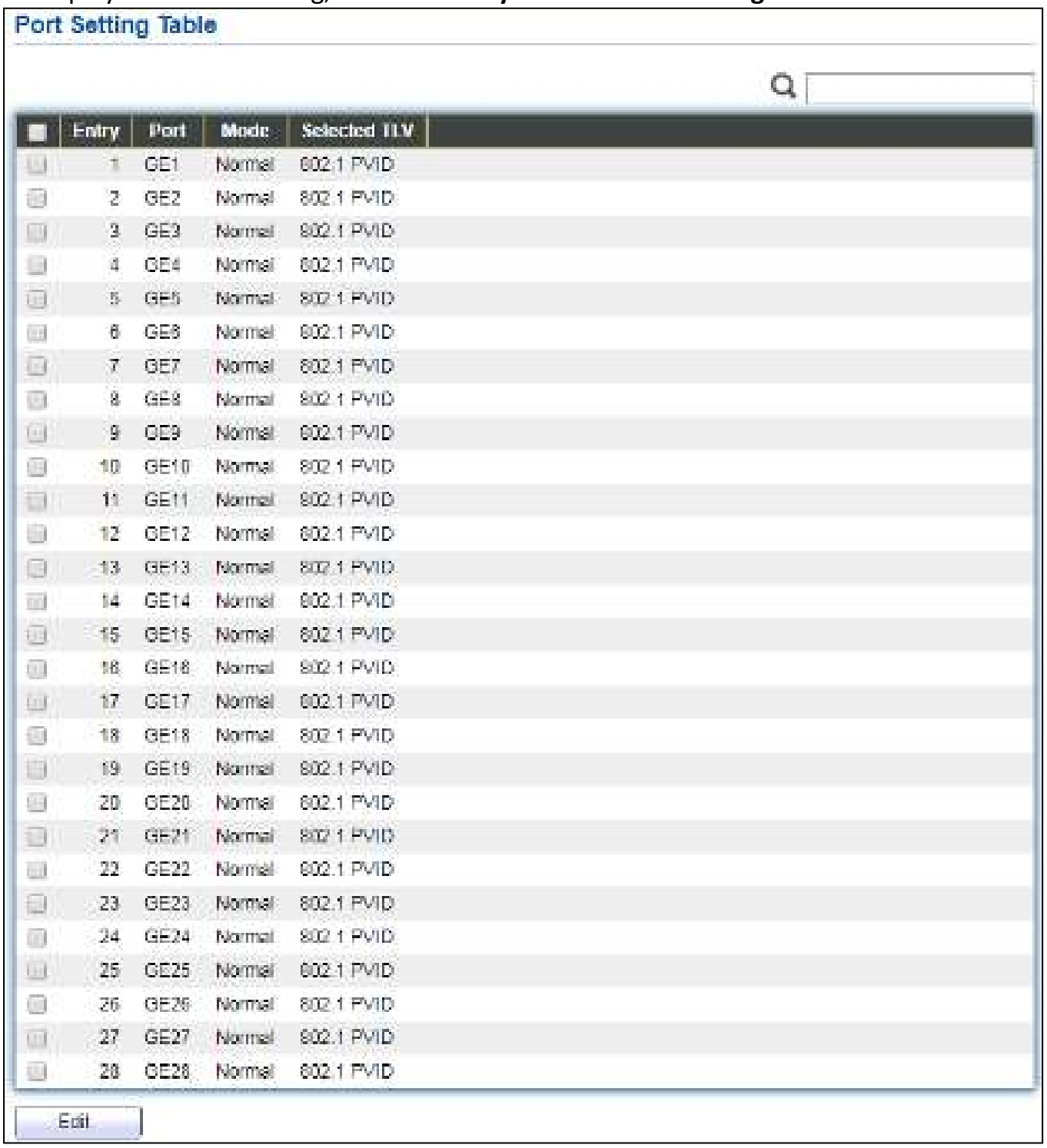


Figure 69 - Discovery > LLDP > Port Setting

Item	Description
Port	Port Name.
Mode	The port LLDP mode.
Selectde TLV	The Selected LLDP TLV.

Click "**Edit**" button to view Edit Port Setting menu.

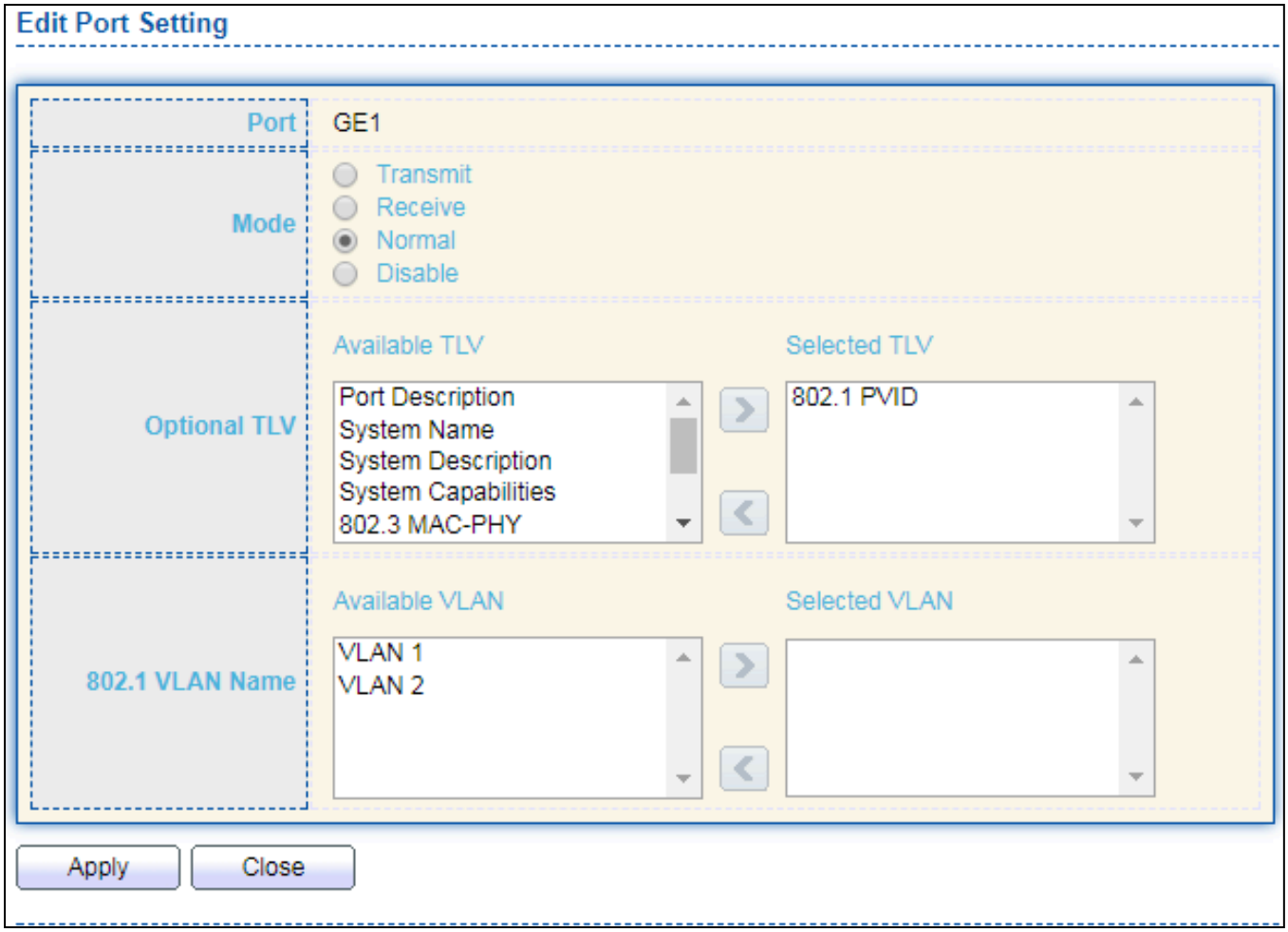


Figure 70 - Discovery > LLDP > Port Setting > Edit Port Setting

Item	Description
Port	Select specified port or all ports to configure LLDP state.
Mode	Select the transmission state of LLDP port interface. ● Disable: Disable the transmission of LLDP PDUs. ● RX Only: Receive LLDP PDUs only. ● TX Only: Transmit LLDP PDUs only. ● TX And RX: Transmit and receive LLDP PDUs both.
Optional TLV	Select the LLDP optional TLVs to be carried (multiple selection is allowed). ● 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).

IV-8-1-3 Packet View

To display LLDP Overloading, click **Discovery > LLDP > Packet View**.

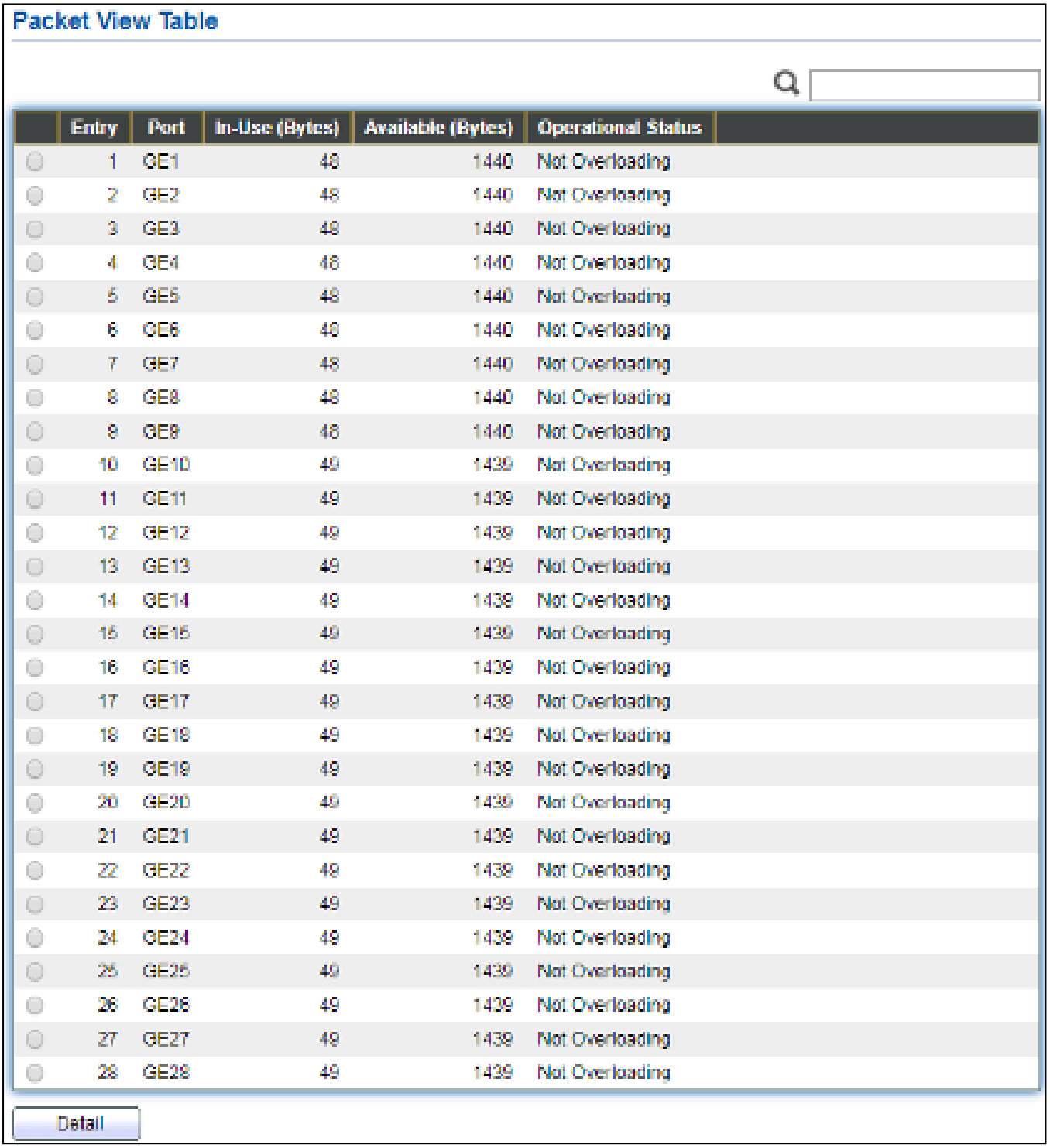
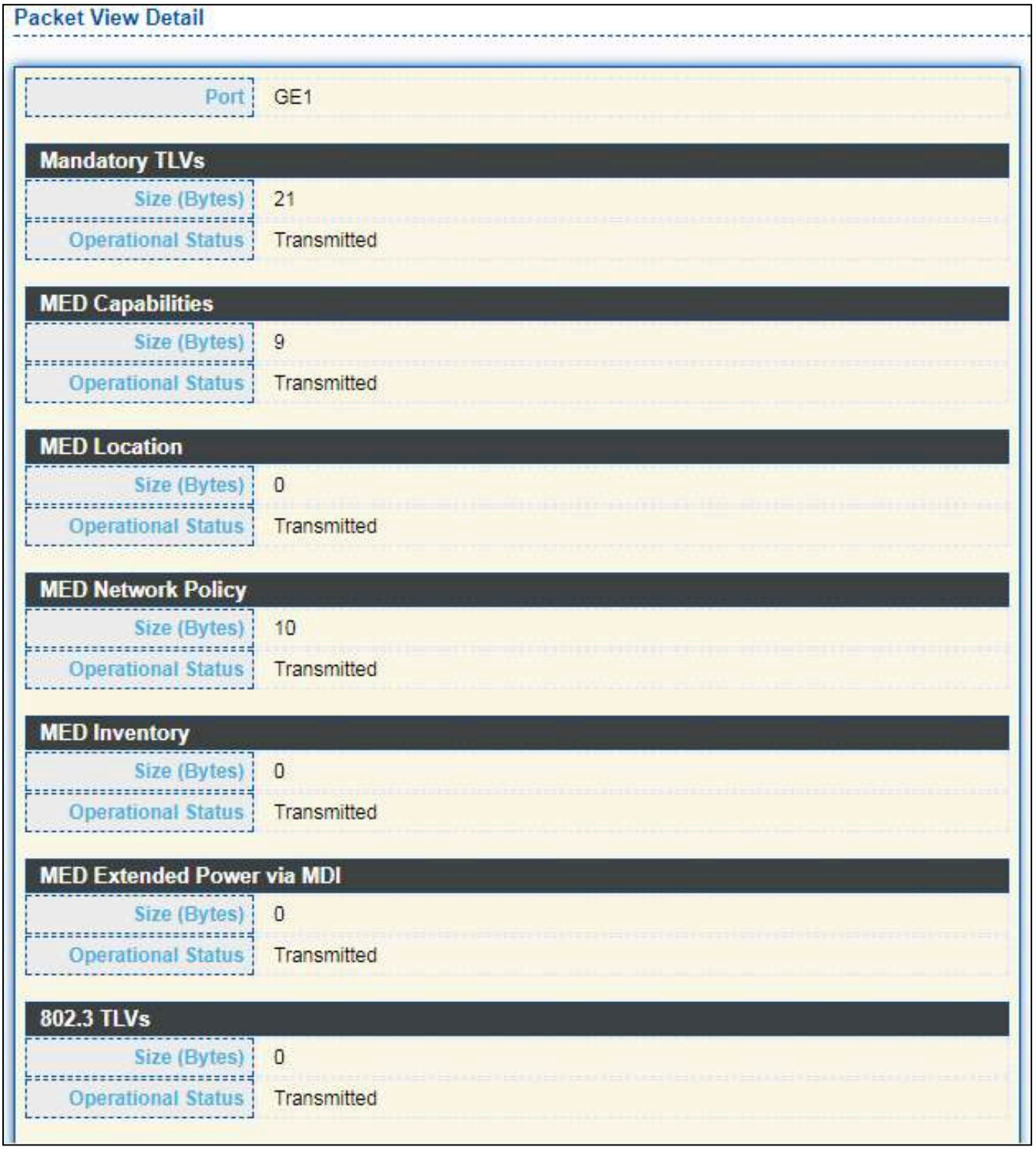


Figure 71 - Discovery > LLDP > Packet View

Item	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 "**Detail**" button to view Packet View Detail menu.



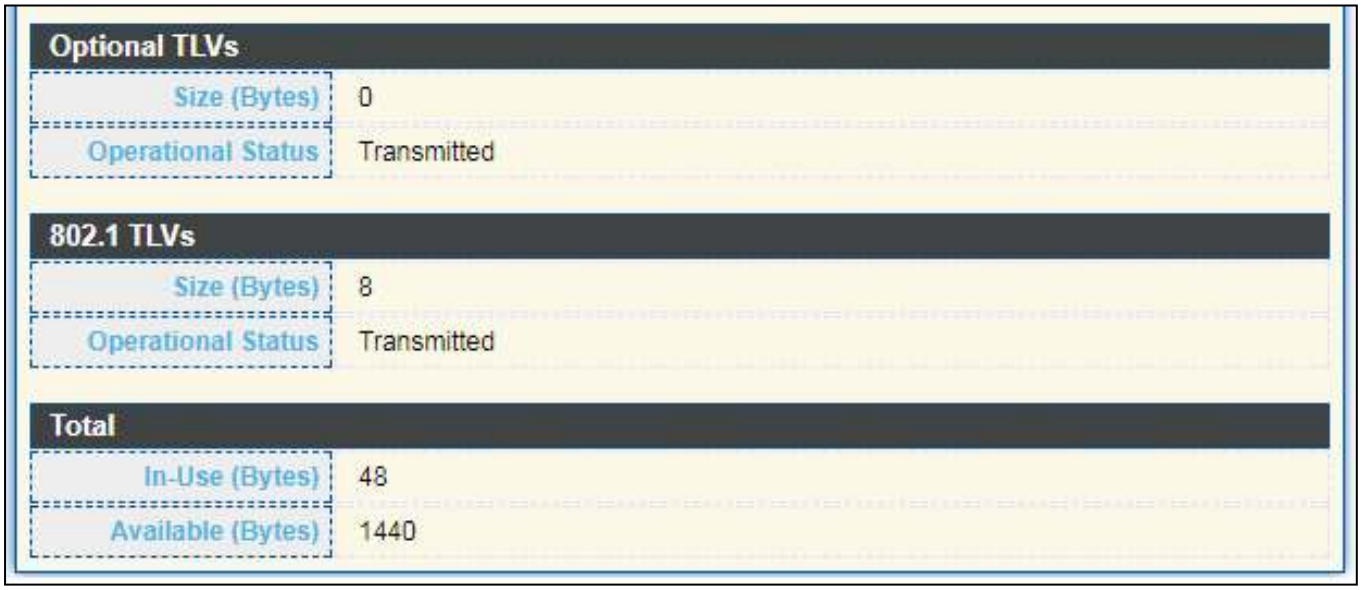


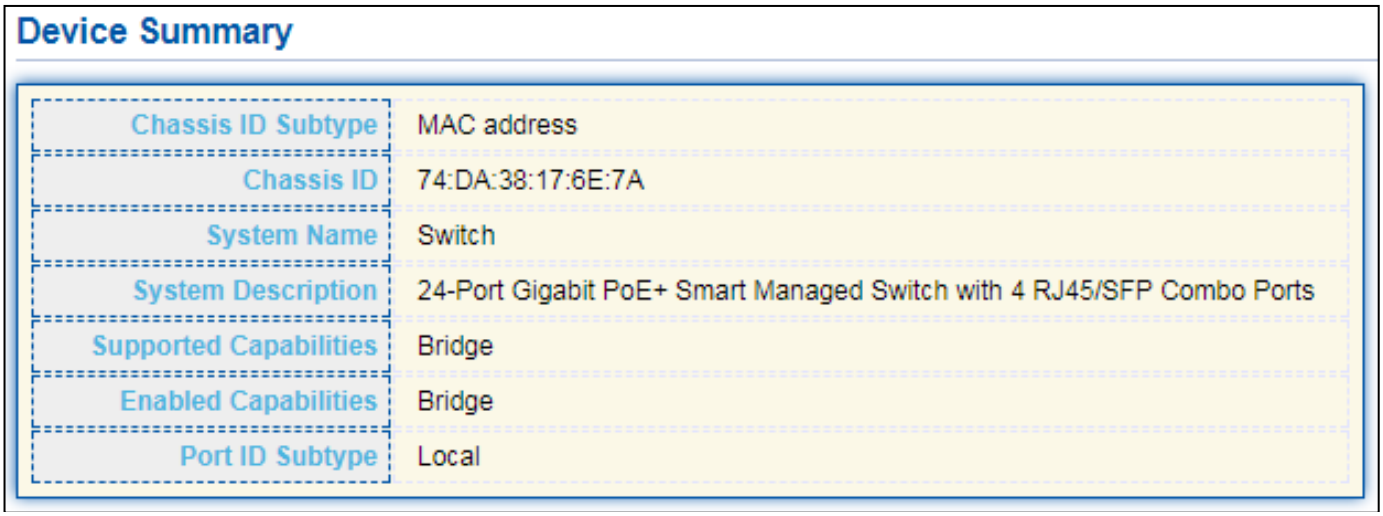
Figure 72 - Discovery > LLDP > Packet View > Packet View Detail

Item	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.

IV-8-1-4 Local Information

Use the LLDP Local Information to view LLDP local device information.

To display LLDP Local Device, click **Discovery > LLDP > Local Information**.



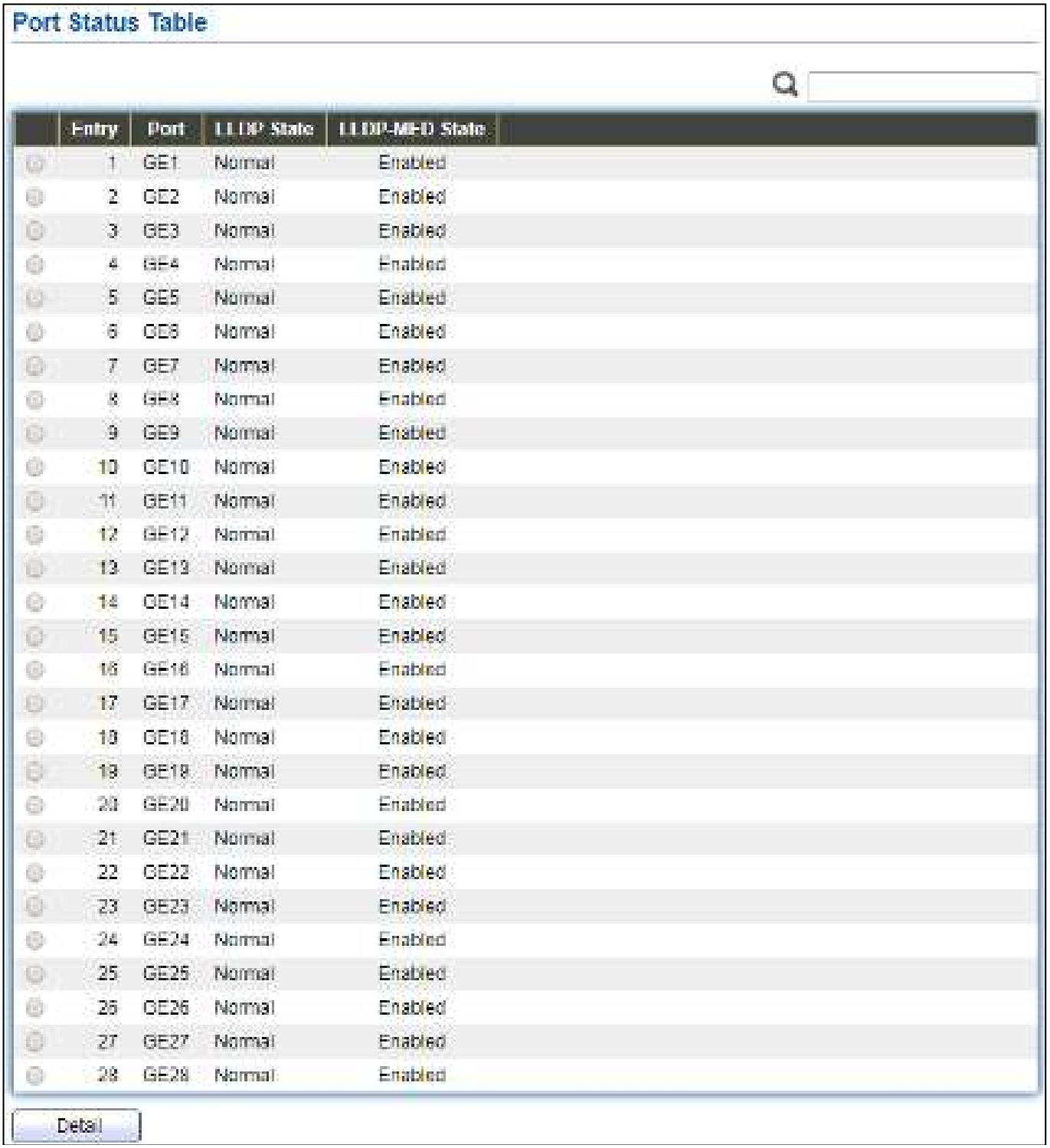


Figure 73 - Discovery > LLDP > Local Information

Item	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.
Capabilities	Primary functions of the device, such as Bridge, WLAN AP, or Router.

Supported	
Capabilities Enabled	Primary enabled functions of the device.
Port ID Subtype	Type of the port identifier that is shown.
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.

Figure 74 - Discovery > LLDP > Local Information > Detail

IV-8-1-5 Neighbor

Use the LLDP Neighbor page to view LLDP neighbors information.

To display LLDP Remote Device, click **Discovery > LLDP > Neighbor**.

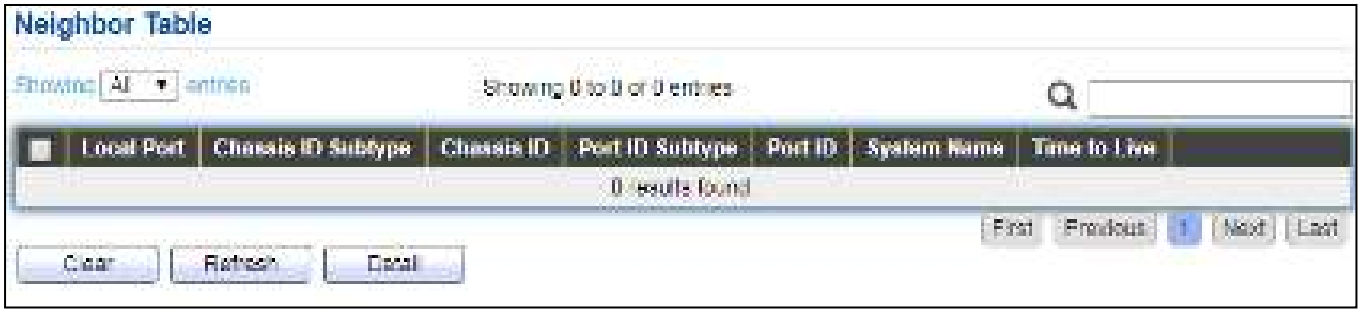


Figure 75 - Discovery > LLDP > Neighbor

Item	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).
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

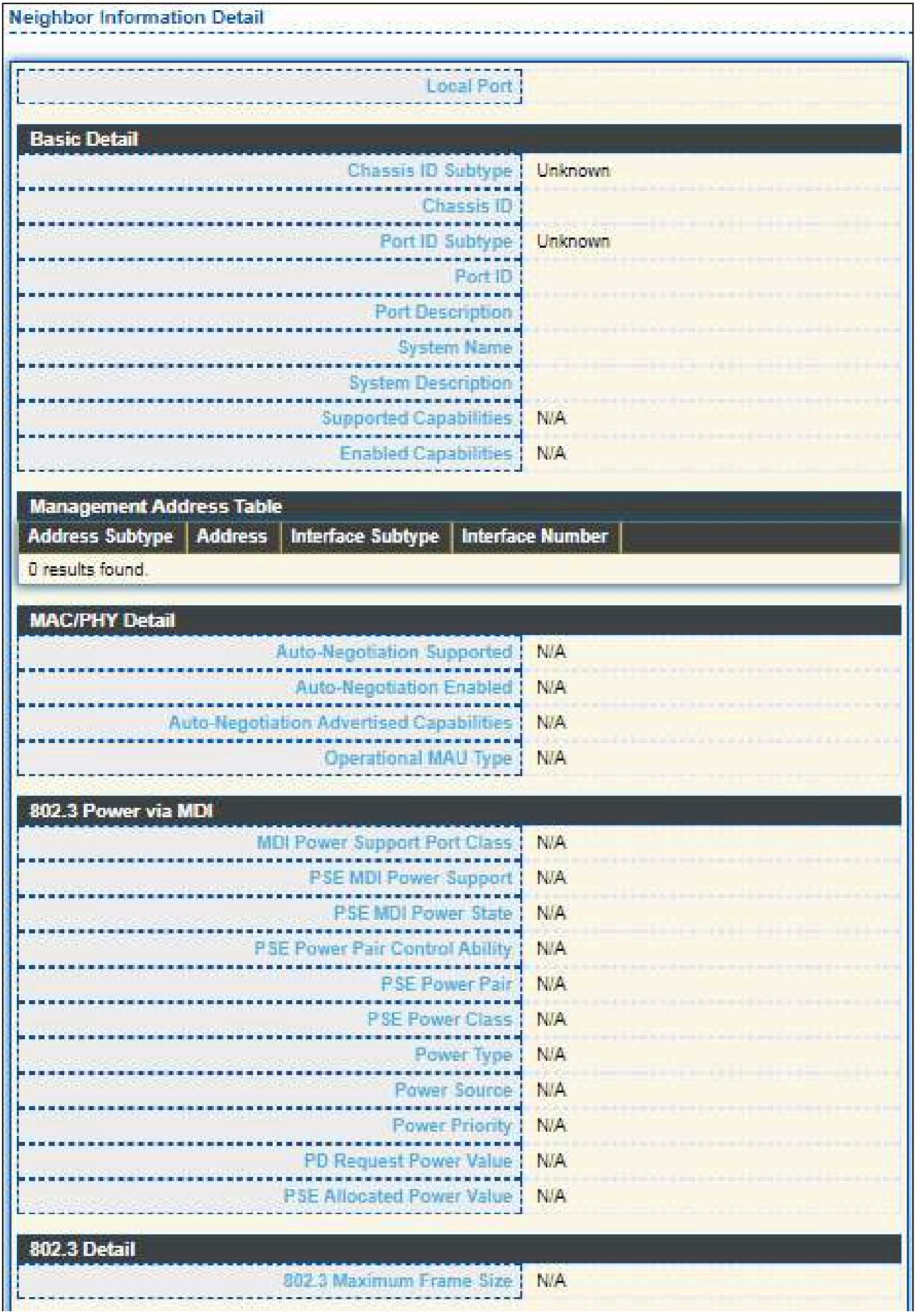
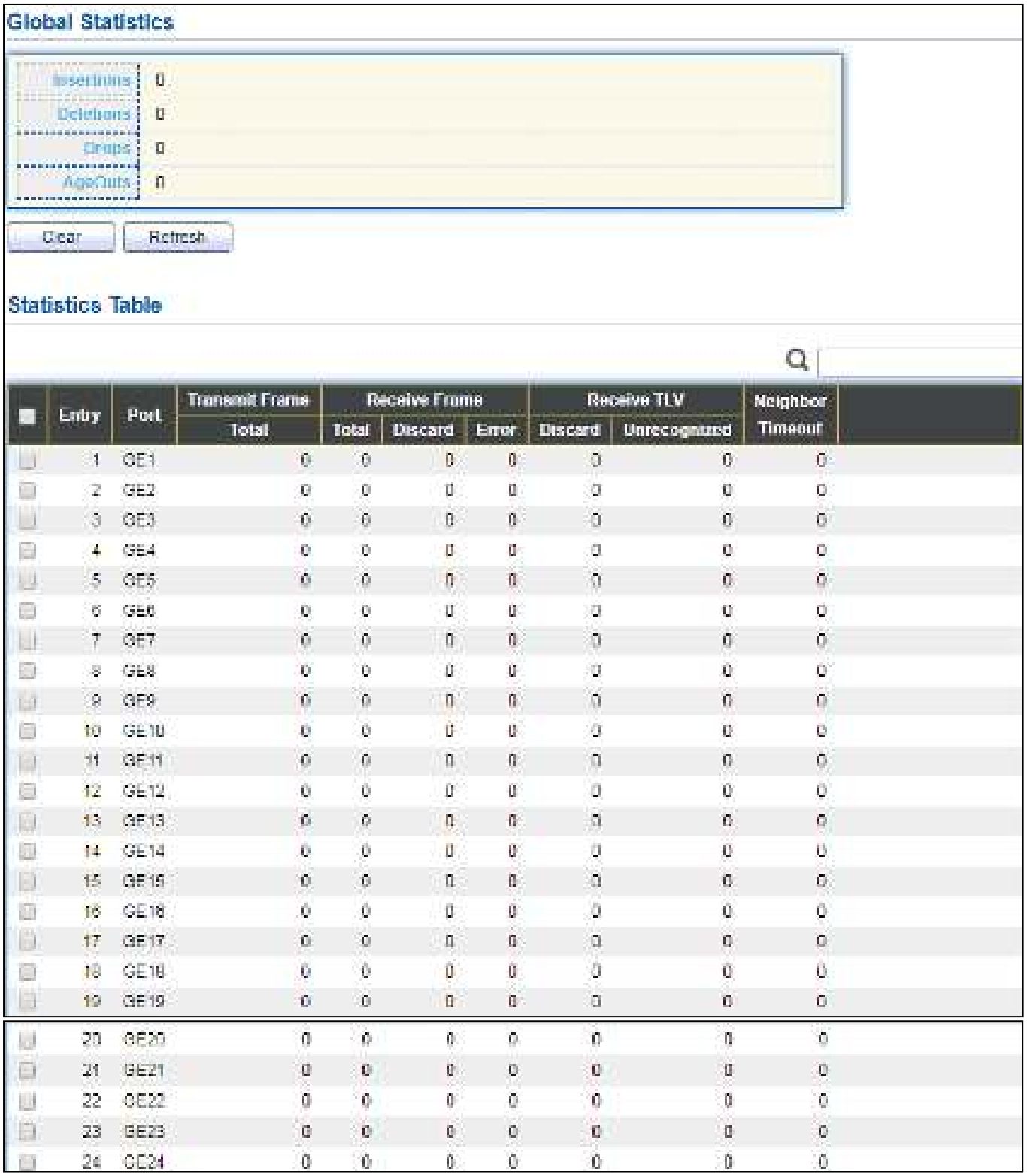


Figure 76 LLDP Neighbor Detail Page

IV-8-1-6 Statistics

The Link Layer Discovery Protocol (LLDP) Statistics page displays summary and per-port information for LLDP frames transmitted and received on the switch.
To display LLDP Statistics status, click **Discovery > LLDP > Statistics**.



Entry	Port	Transmit Frame	Receive Frame			Receive TLV		Neighbor
		Total	Total	Discard	Error	Discard	Unrecognized	Timeout
1	GE1	0	0	0	0	0	0	0
2	GE2	0	0	0	0	0	0	0
3	GE3	0	0	0	0	0	0	0
4	GE4	0	0	0	0	0	0	0
5	GE5	0	0	0	0	0	0	0
6	GE6	0	0	0	0	0	0	0
7	GE7	0	0	0	0	0	0	0
8	GE8	0	0	0	0	0	0	0
9	GE9	0	0	0	0	0	0	0
10	GE10	0	0	0	0	0	0	0
11	GE11	0	0	0	0	0	0	0
12	GE12	0	0	0	0	0	0	0
13	GE13	0	0	0	0	0	0	0
14	GE14	0	0	0	0	0	0	0
15	GE15	0	0	0	0	0	0	0
16	GE16	0	0	0	0	0	0	0
17	GE17	0	0	0	0	0	0	0
18	GE18	0	0	0	0	0	0	0
19	GE19	0	0	0	0	0	0	0
20	GE20	0	0	0	0	0	0	0
21	GE21	0	0	0	0	0	0	0
22	GE22	0	0	0	0	0	0	0
23	GE23	0	0	0	0	0	0	0
24	GE24	0	0	0	0	0	0	0

Figure 77 - Discovery > LLDP > Statistics

Item	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.
Statistics Table	
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.
Receive Frame Discard	Number of LLDP frames discarded for any reason by the LLDP agent on the corresponding port.
Receive Frame Error	Number of invalid LLDP frames received by the LLDP agent on the corresponding port, while the LLDP agent is enabled.
Receive TLV Discard	Number of TLVs of LLDP frames discarded for any reason by the LLDP agent on the corresponding port.
Receive TLV Unrecognized	Number of TLVs of LLDP frames that are unrecognied while the LLDP agent is enabled.
Neighbor Timeout	Number of age out LLDP frames.

IV-9 Multicast

Use this section to configure Multicast.

IV-9-1 General

Use the General pages to configure settings of IGMP and MLD common function.

IV-9-1-1 Property

To display multicast general property Setting web page, click **Multicast> General> Property**.

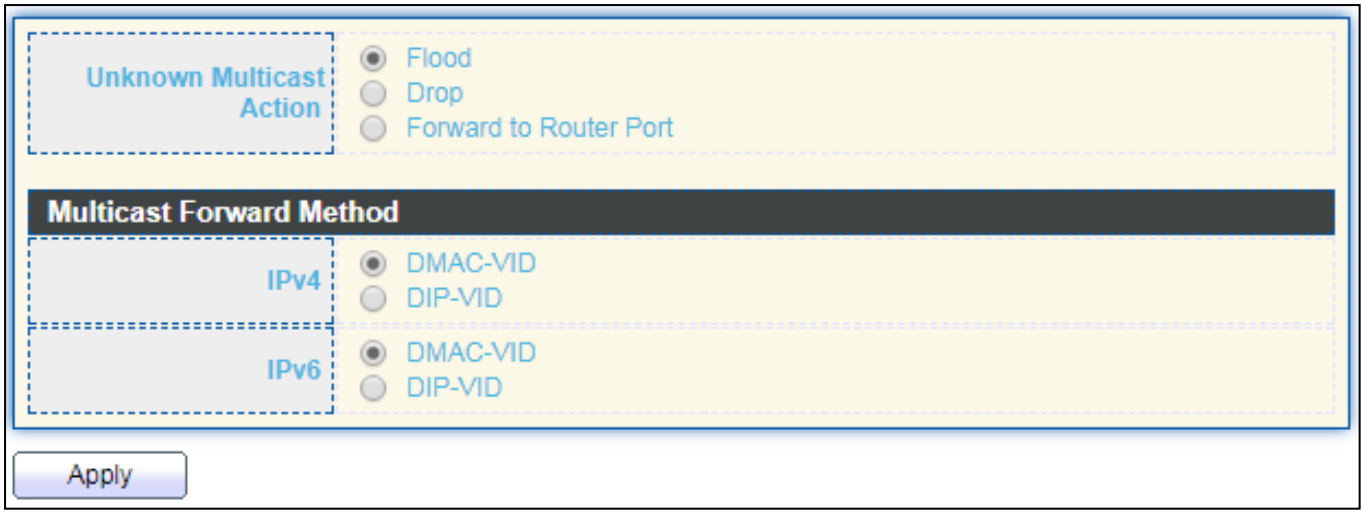


Figure 78 - Multicast > General > Property

Item	Description
Unknown Multicast Action	Set the unknown multicast action ● Flood: flood the unknown multicast data. ● Drop: drop the unknown multicast data. ● Router port: forward the unknown multicast data to router port.
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).

IV-9-1-2 Group Address

This page allow user to browse all multicast groups that dynamic learned or statically added.

To display Multicast General Group web page, click **Multicast> General > Group Address**.

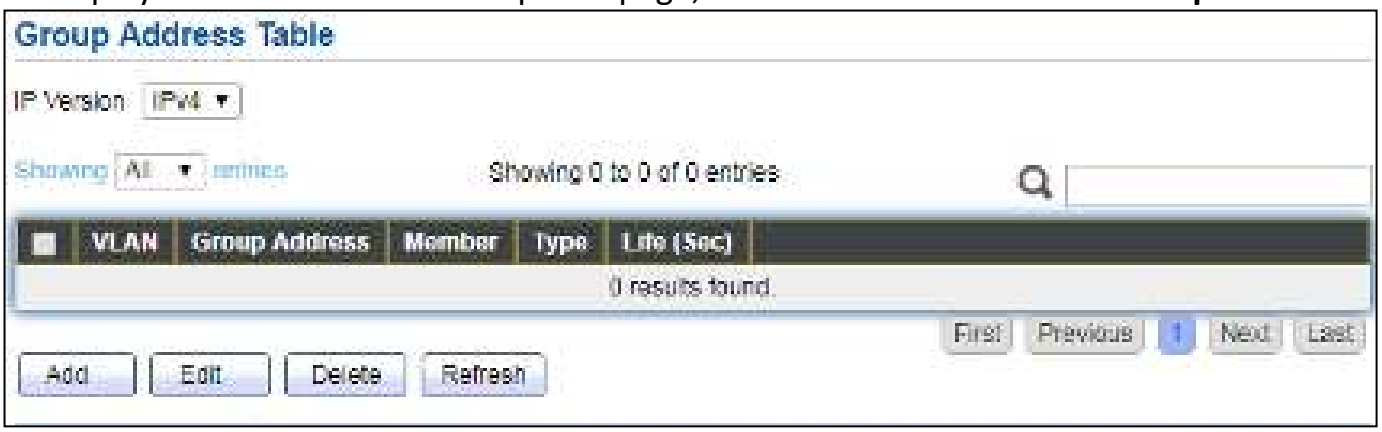


Figure 79 - Multicast > General > Group Address

Item	Description
IP Version	IP Version ● IPv4: ipv4 multicast group ● IPv6: ipv6 multicast group
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.

Click “**Add**” or “**Edit**” button to view Add or Edit Group Address menu.

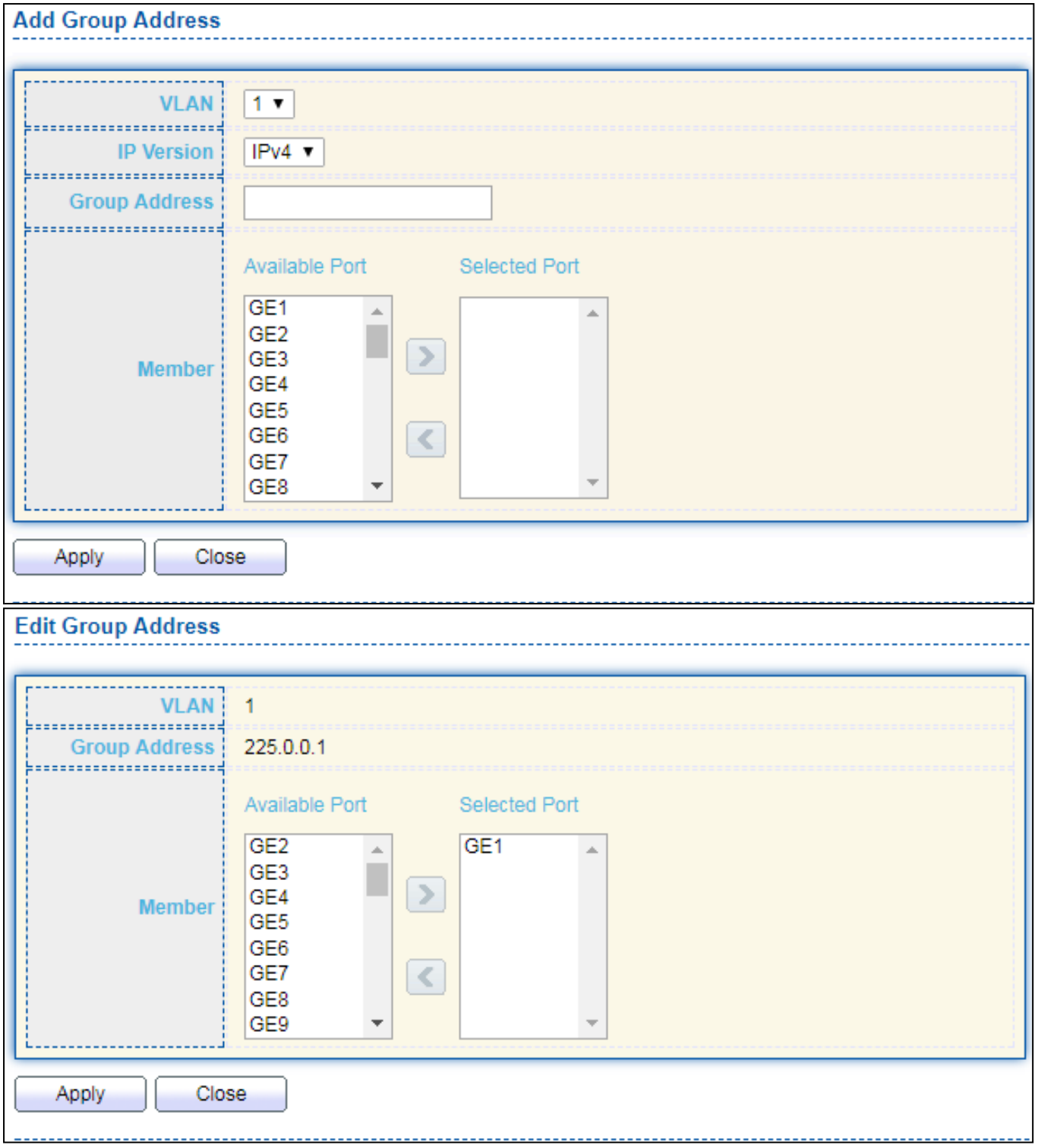


Figure 80 - Multicast > General > Group Address > Add/Edit Group Address

Item	Description
VLAN	The VLAN ID of group.
IP Version	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

IV-9-1-3 Router Port

This page allow user to browse all router port information. The static and forbidden router port can set by user.

To display multicast router port table web page, click **Multicast > General > Router Port**.

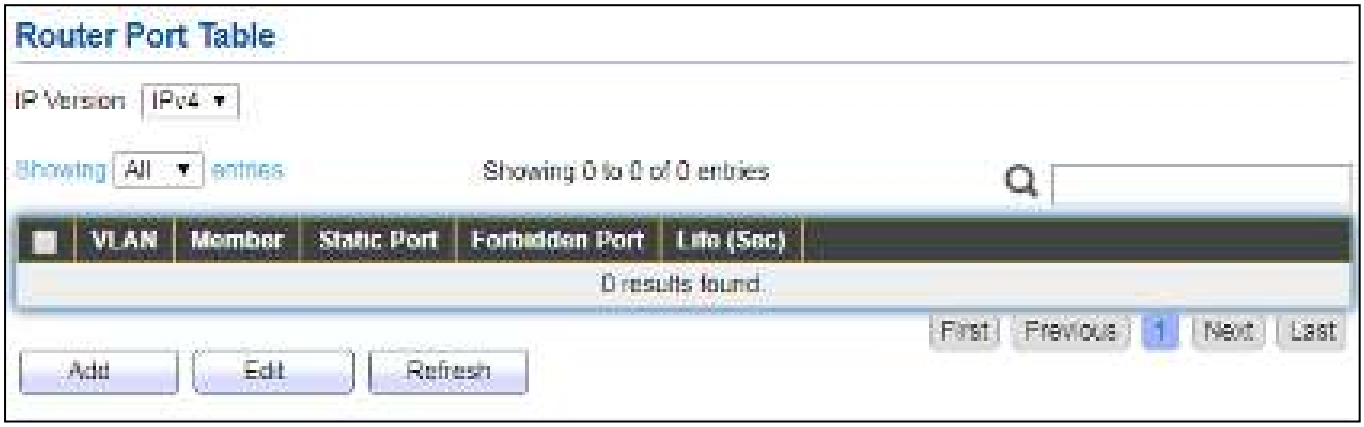


Figure 81 - Multicast > General > Router Port

Item	Description
IP Version	IP Version ● IPv4: ipv4 multicast router ● IPv6: ipv6 multicast router
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.

Click "**Add**" or "**Edit**" button to view Add/Edit Router Port menu.

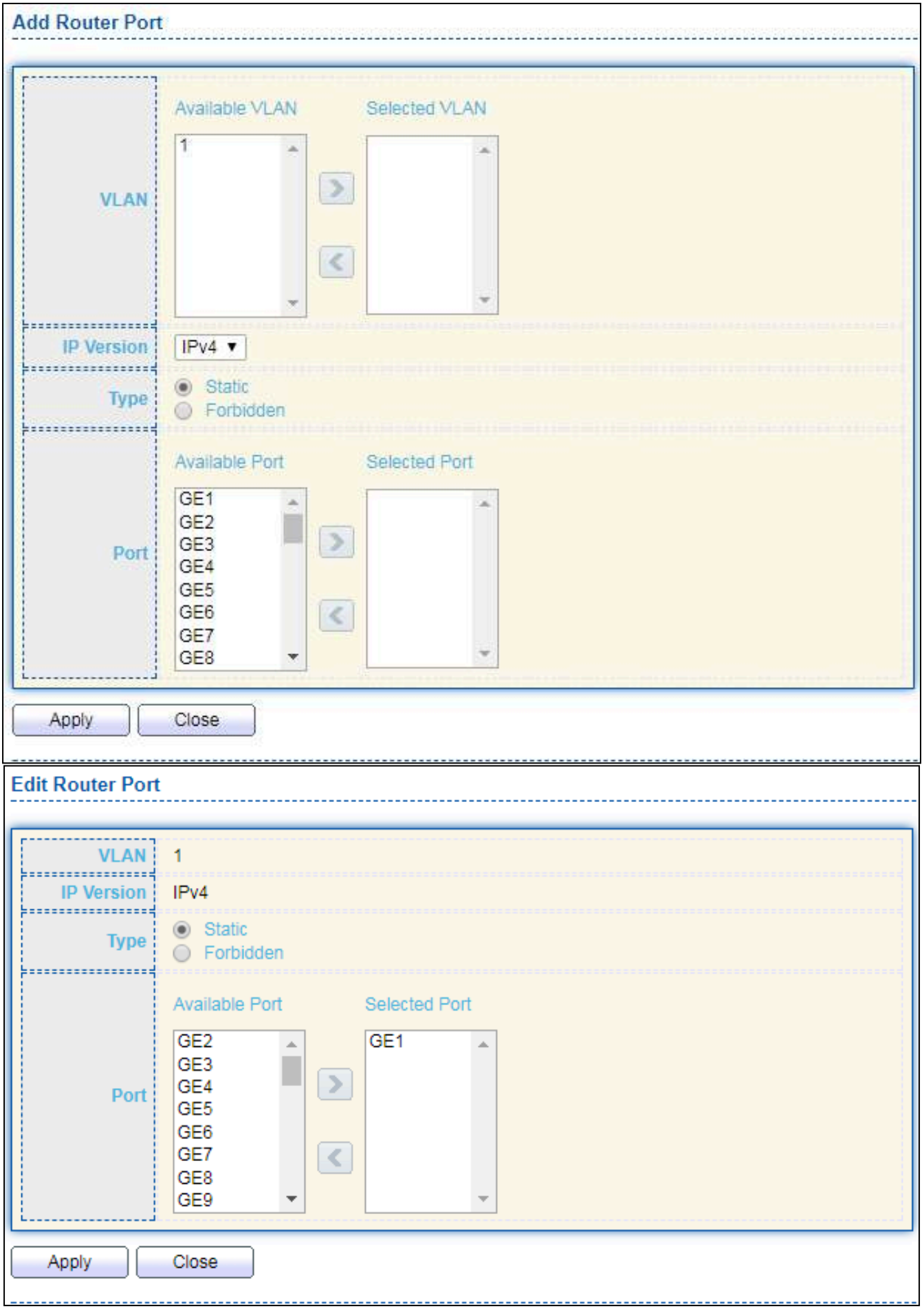


Figure 82 - Multicast > General > Router Port > Add/Edit Router Port

Item	Description
VLAN	The VLAN ID for router entry ● Available VLAN: Optional VLAN member ● Selected VLAN: Selected VLAN member.
IP Version	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

IV-9-2 IGMP Snooping

Use the IGMP Snooping pages to configure settings of IGMP snooping function.

IV-9-2-1 Property

This page allow user to configure global settings of IGMP snooping and configure specific VLAN settings of IGMP Snooping.

To display IGMP Snooping global setting and VLAN Setting web page, click **Multicast > IGMP Snooping > Property**.

Figure 83 - Multicast > IGMP Snooping > Property

Item	Description
State	Set the enabling status of IGMP Snooping functionality Enable: If Checked Enable IGMP Snooping, else is Disabled IGMP Snooping.
Version	Set the igmp snooping version ● IGMPv2: Only support process igmp v2 packet. ● IGMPv3: Support v3 basic and v2.
Report Suppression	Set the enabling status of IGMP v2 report suppression Enable: If Checked Enable IGMP Snooping v2 report suppression, else Disable the report suppression function.
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.

Click "**Edit**" button to Edit VLAN Setting menu.

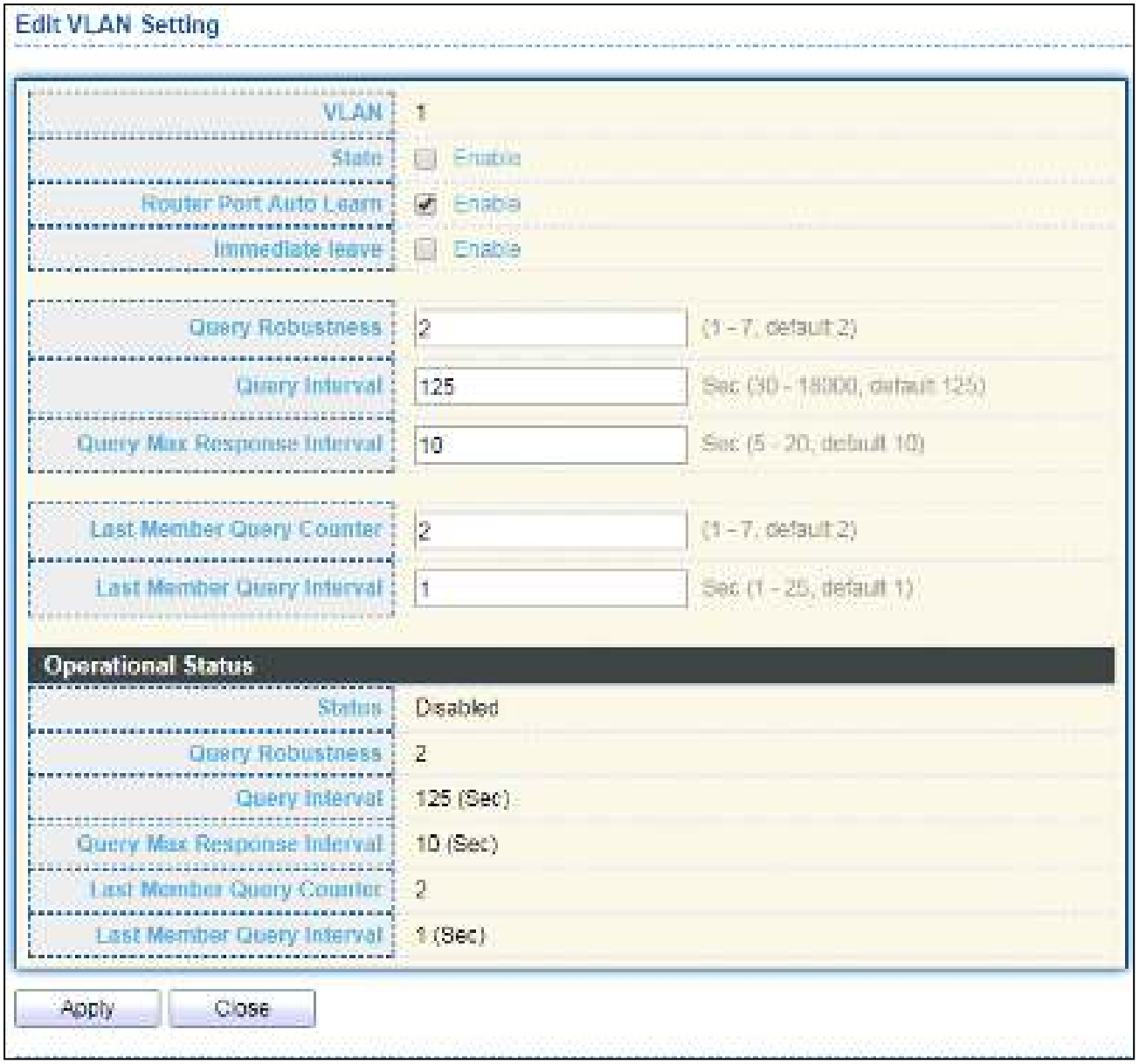


Figure 84 - Multicast > IGMP Snooping > Property >Edit VLAN Setting

Item	Description
VLAN	The selected VLAN List.
State	Set the enabling status of IGMP Snooping VLAN functionality 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	
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.

IV-9-2-2 Querier

This page allow user to configure querier settings on specific VLAN of IGMP Snooping.

To display IGMP Snooping Querier Setting web page, click **Multicast > IGMP Snooping > Querier**.

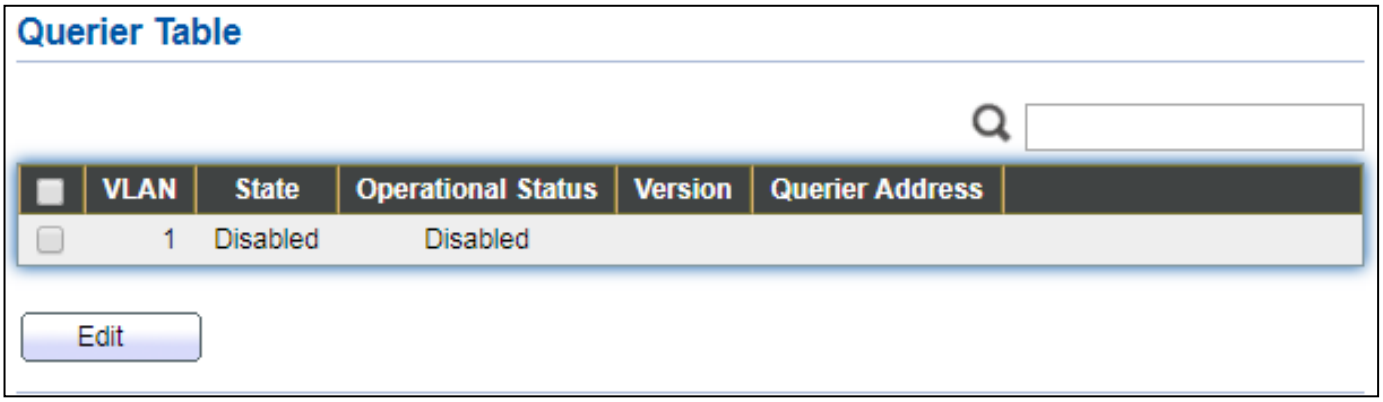


Figure 85 - Multicast > IGMP Snooping > Querier

Item	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.

Click "**Edit**" button to view Edit Querier menu.

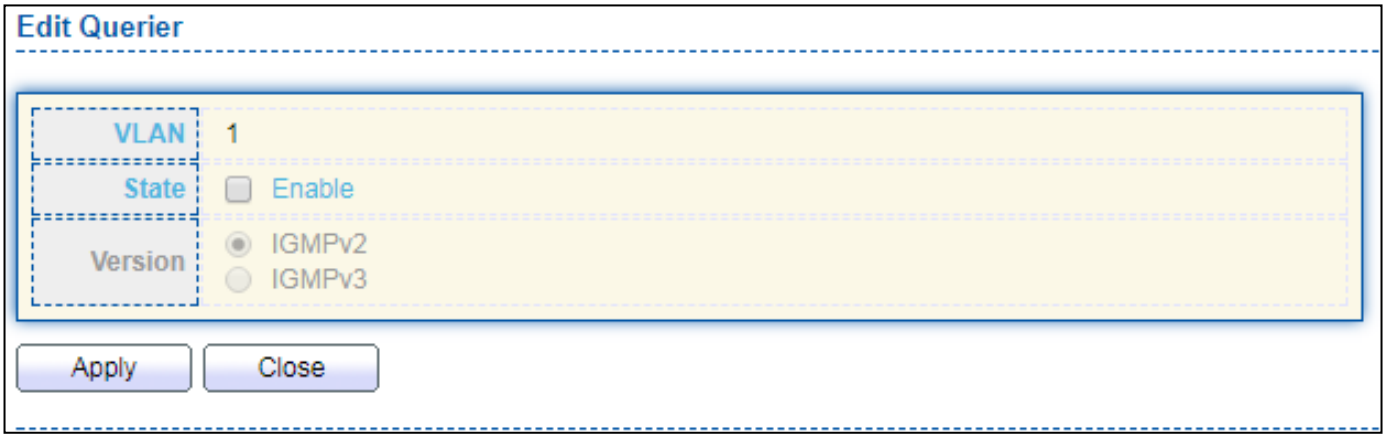


Figure 86 - Multicast > IGMP Snooping > Querier > Edit Querier

Item	Description
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)

IV-9-2-3 Statistics

This page allow user to clear igmp snooping statics.

To display IGMP Snooping Statistics, click **Multicast > IGMP Snooping > Statistics**.

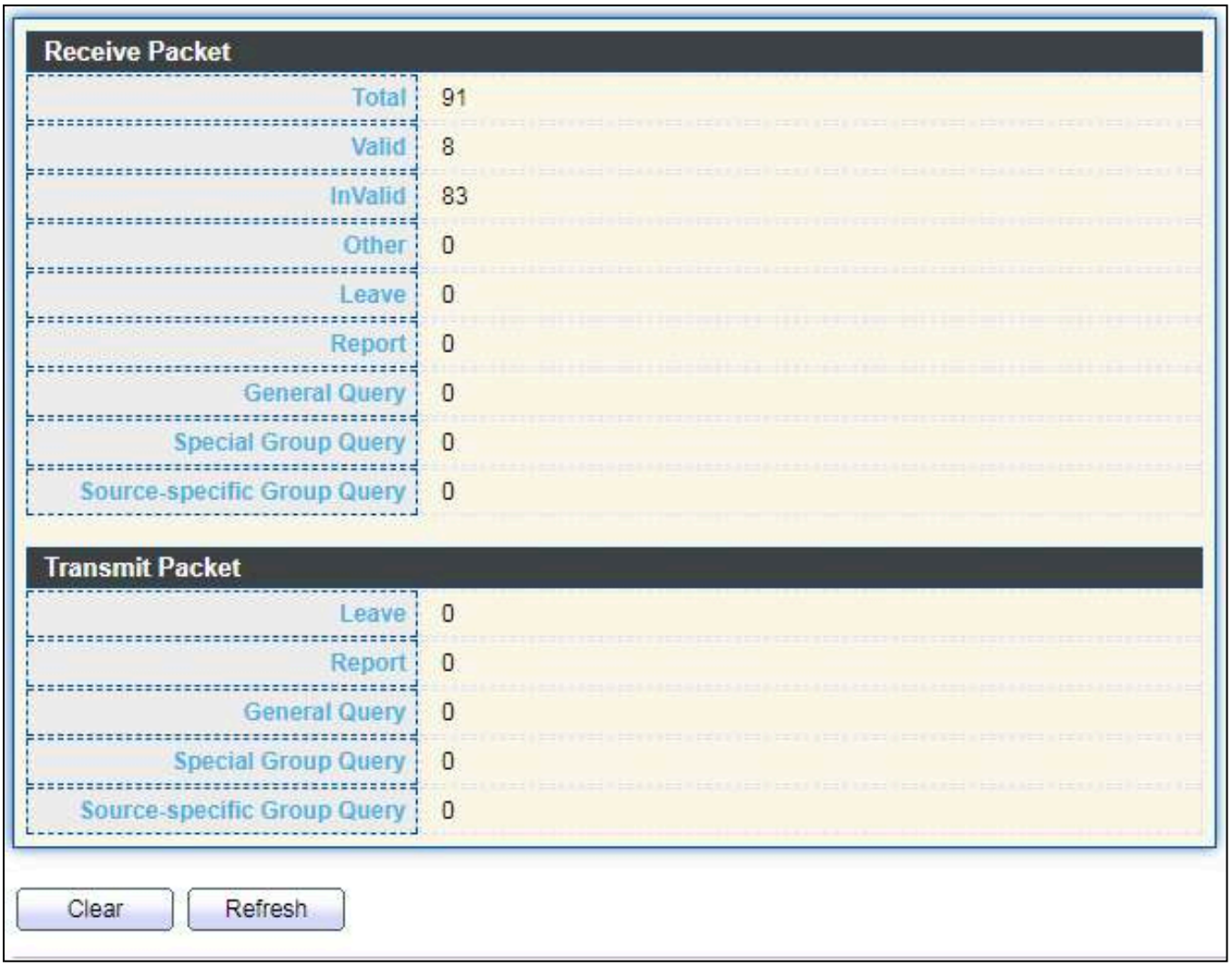


Figure 87 - Multicast > IGMP Snooping > Statistics

Item	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	IGMP Special Source and Group General Query packet.

Group Query	
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.

IV-9-3 MVR

Use the MVR pages to configure settings of MVR function.

IV-9-3-1 Property

To display multicast MVR property Setting web page, click **Multicast > MVR > Property**.

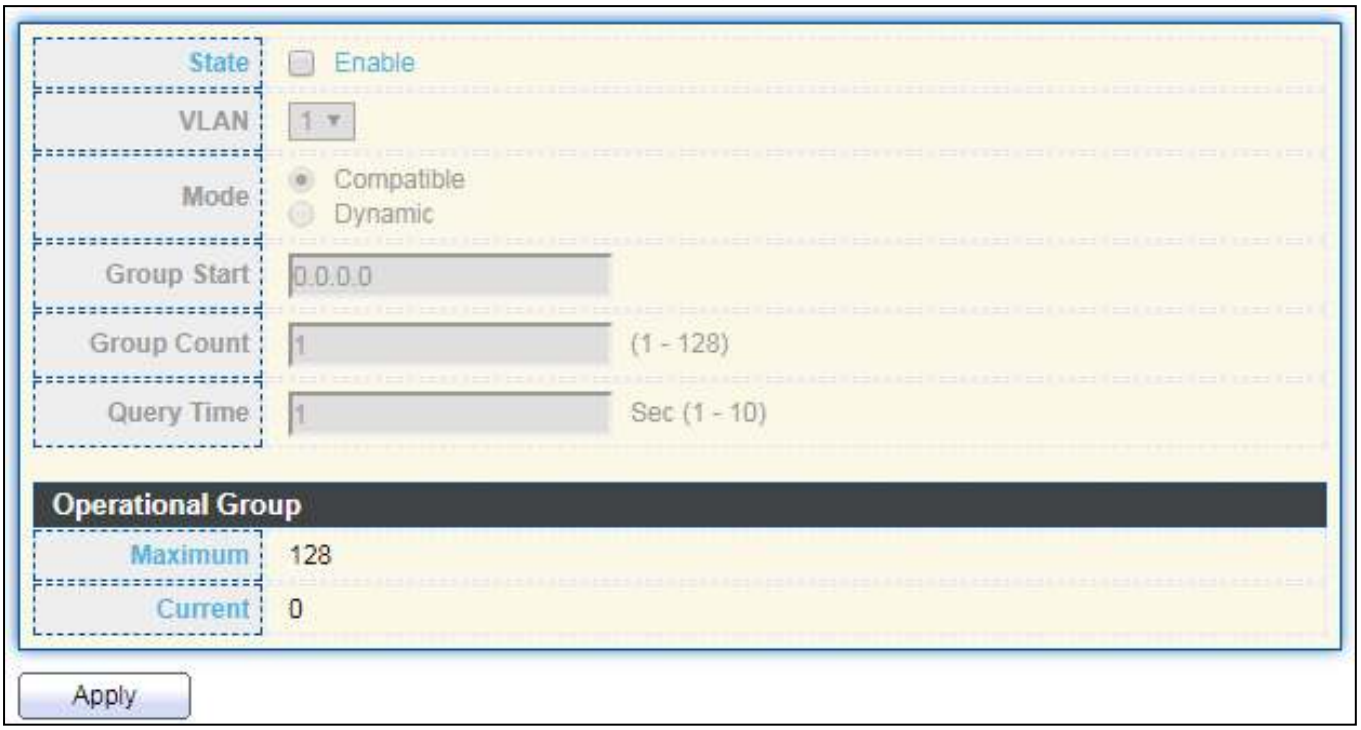


Figure 88 - Multicast > MVR > Property

Item	Description
State	Enable: if checked enable the MVR state, else disable the MVR state.
VLAN	The MVR VLAN ID.
Mode	Set the MVR mode ● Compatible: compatible mode. ● Dynamic: learn group member on source port.
Group Start	MVR group range start.
Group Count	MVR group continue count.
Query Time	MVR query time when receive MVR leave MVR group packet.
Maximum	The max number of MVR group database.
Current	The learned MVR group current time

IV-9-3-2 Port Setting

This page allow user to configure port role and port immediate leave.

To display MVR port role and immediate leave state setting web page, click **Multicast > MVR > Port Setting**.

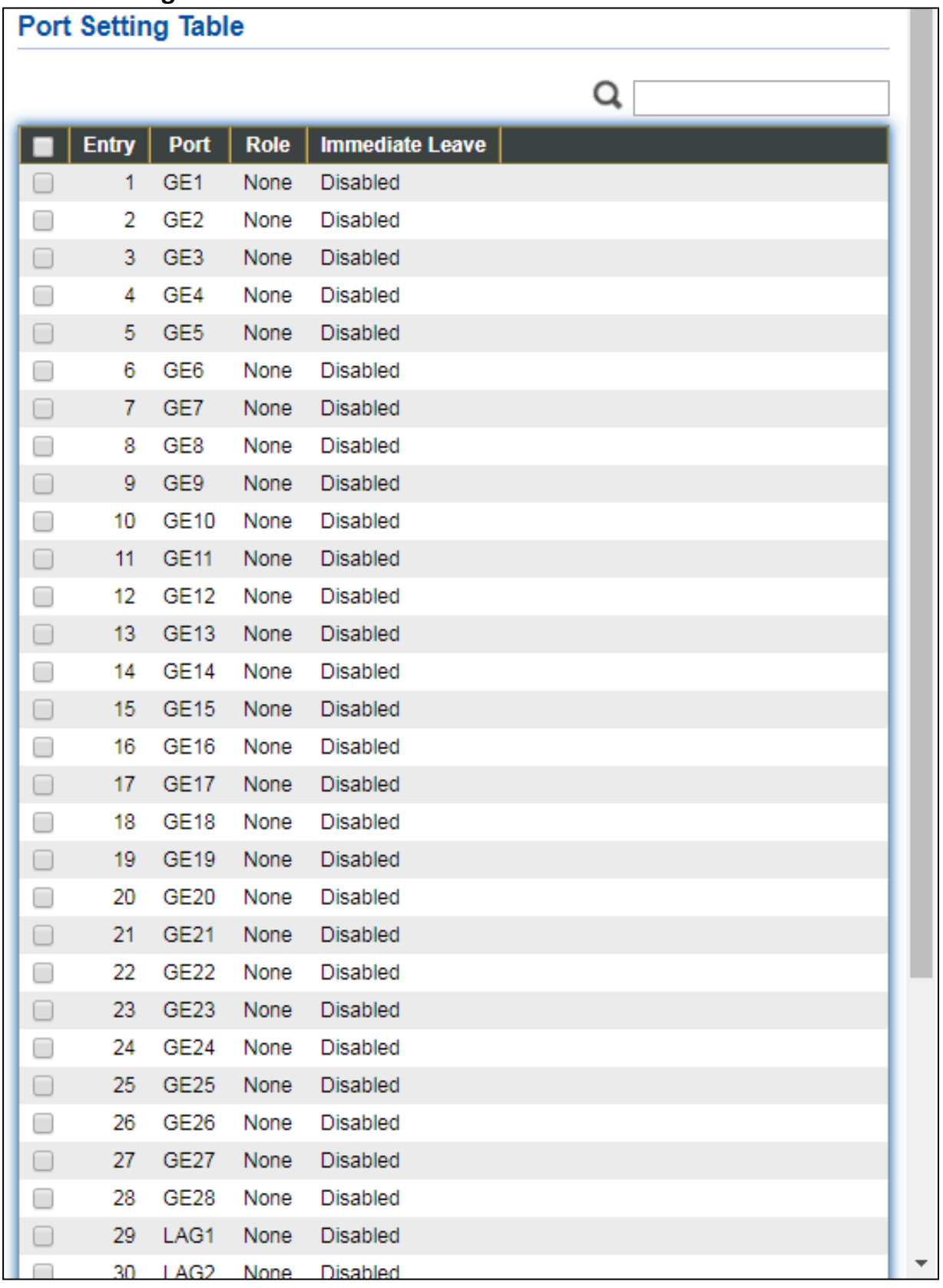


Figure 89 - Multicast > MVR > Port Setting

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

Click "**Edit**" button to view Edit Port Setting menu.

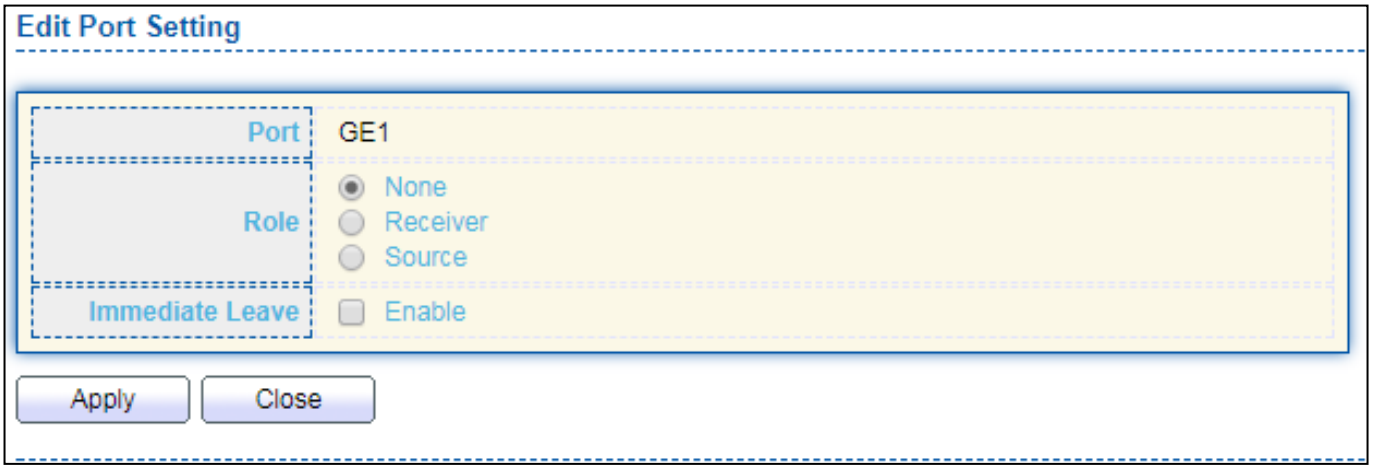


Figure 90 - Multicast > MVR > Port Setting > Edit Port Setting

Item	Description
Port	Display the selected port list.
Role	MVR port role ● None: port role is none. ● Receiver: port role is receiver. ● Source: port role is source.
Immediate Leave	MVR Port immediate leave Enable: if checked is enable immediate leave, else disable immediate leave.

IV-9-3-3 Group Address

This page allow user to browse all multicast MVR groups that dynamic learned or statically added.

To display Multicast MVR Group web page, click **Multicast > MVR > Group Address**.

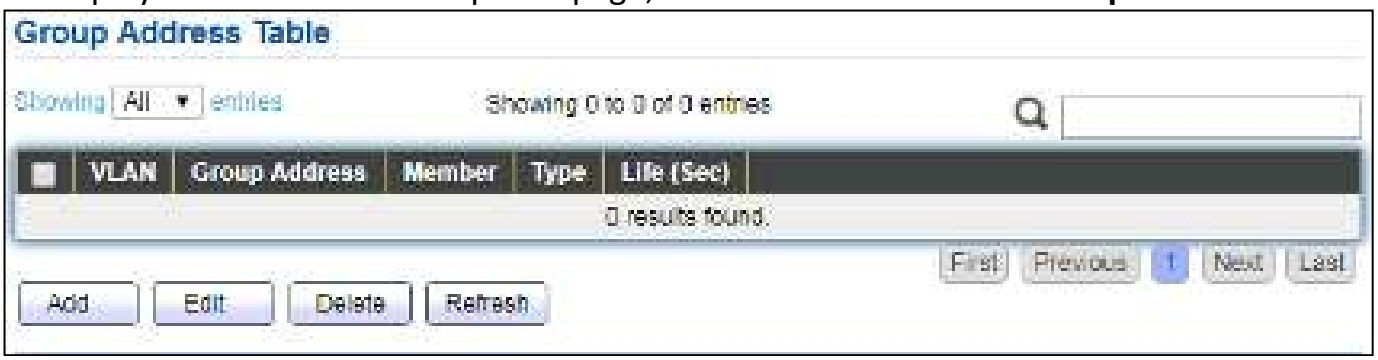


Figure 91 - Multicast > MVR > Group Address

Item	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.

Click "**Add**" button to view Add/Edit Group Address Table menu.

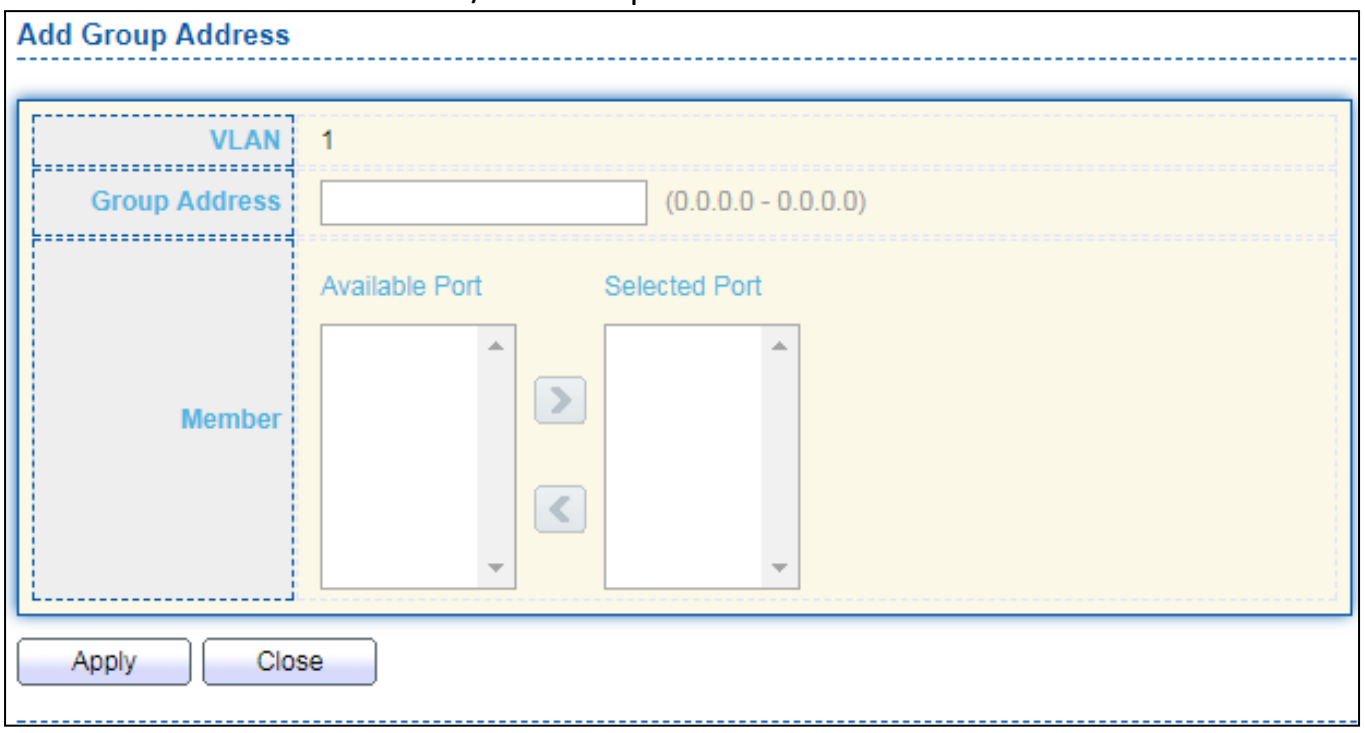


Figure 92 - Multicast > MVR > Group Address > Add Group Address

Item	Description
VLAN	The VLAN ID of MVR group.
Group Address	The MVR group IP address.
Member	The member ports of 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

IV-10 Security

Use the Security pages to configure settings for the switch security features.

IV-10-1 RADIUS

This page allow user to add, edit or delete RADIUS server settings and modify default parameter of RADIUS server.

To display RADIUS web page, click **Security > RADIUS**.

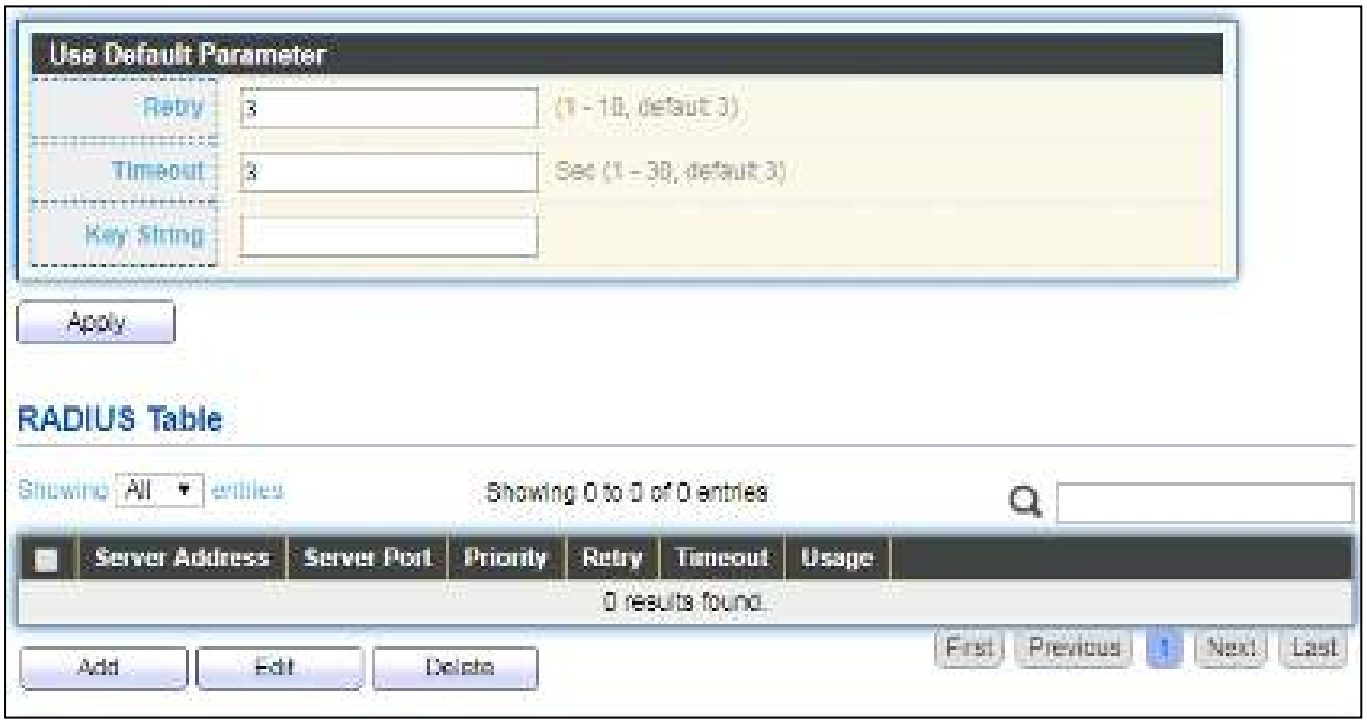
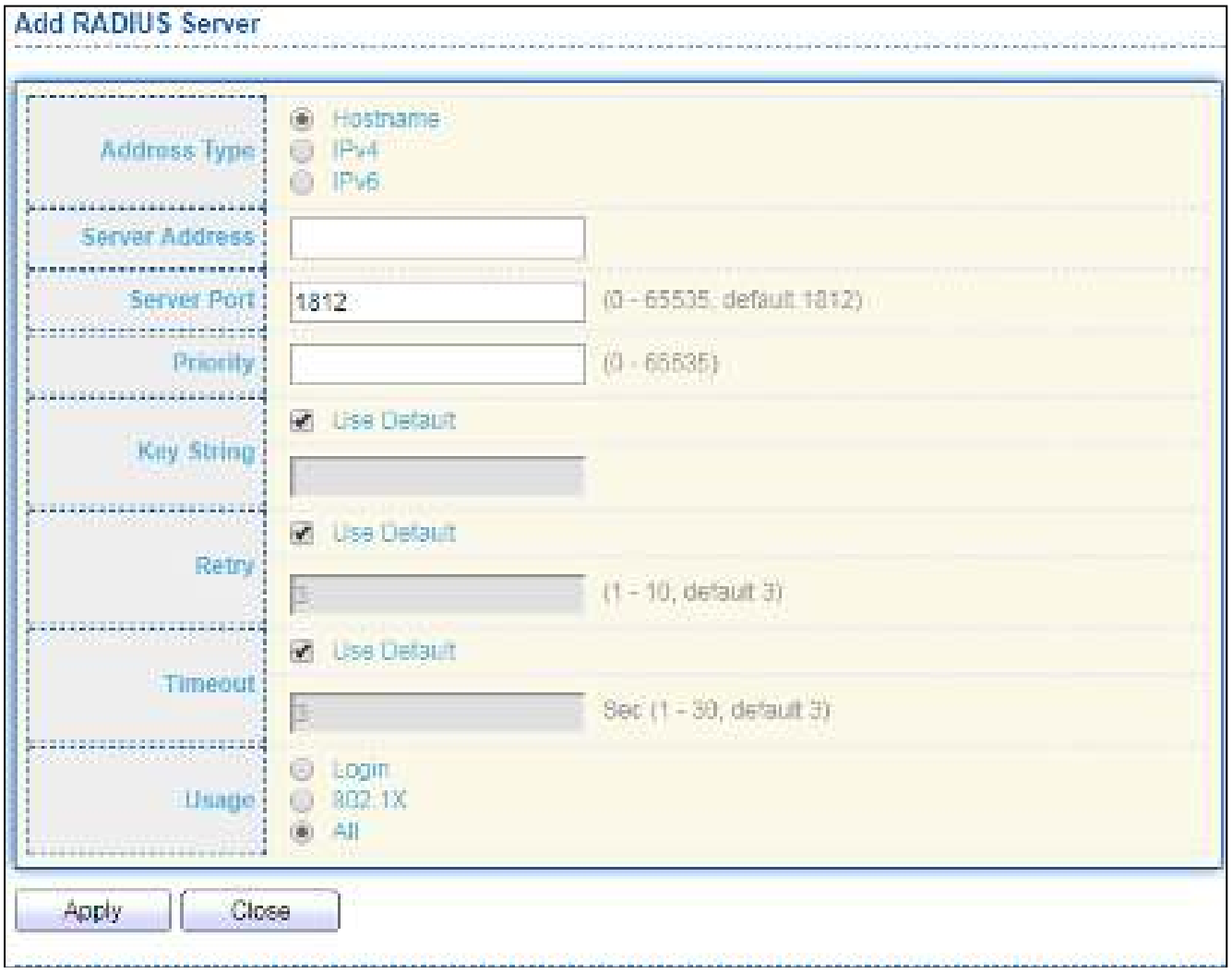


Figure 93 - Security > RADIUS

Item	Description
Retry	Set default retry number.
Timeout	Set default timeout value.
Key String	Set default RADIUS key string
RADIUS Table	
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 authentifation. 802.1x: For 802.1x authentication. All: For all types.

Click "**Add**" or "**Edit**" button to view Add/Edit RADIUS Server menu.



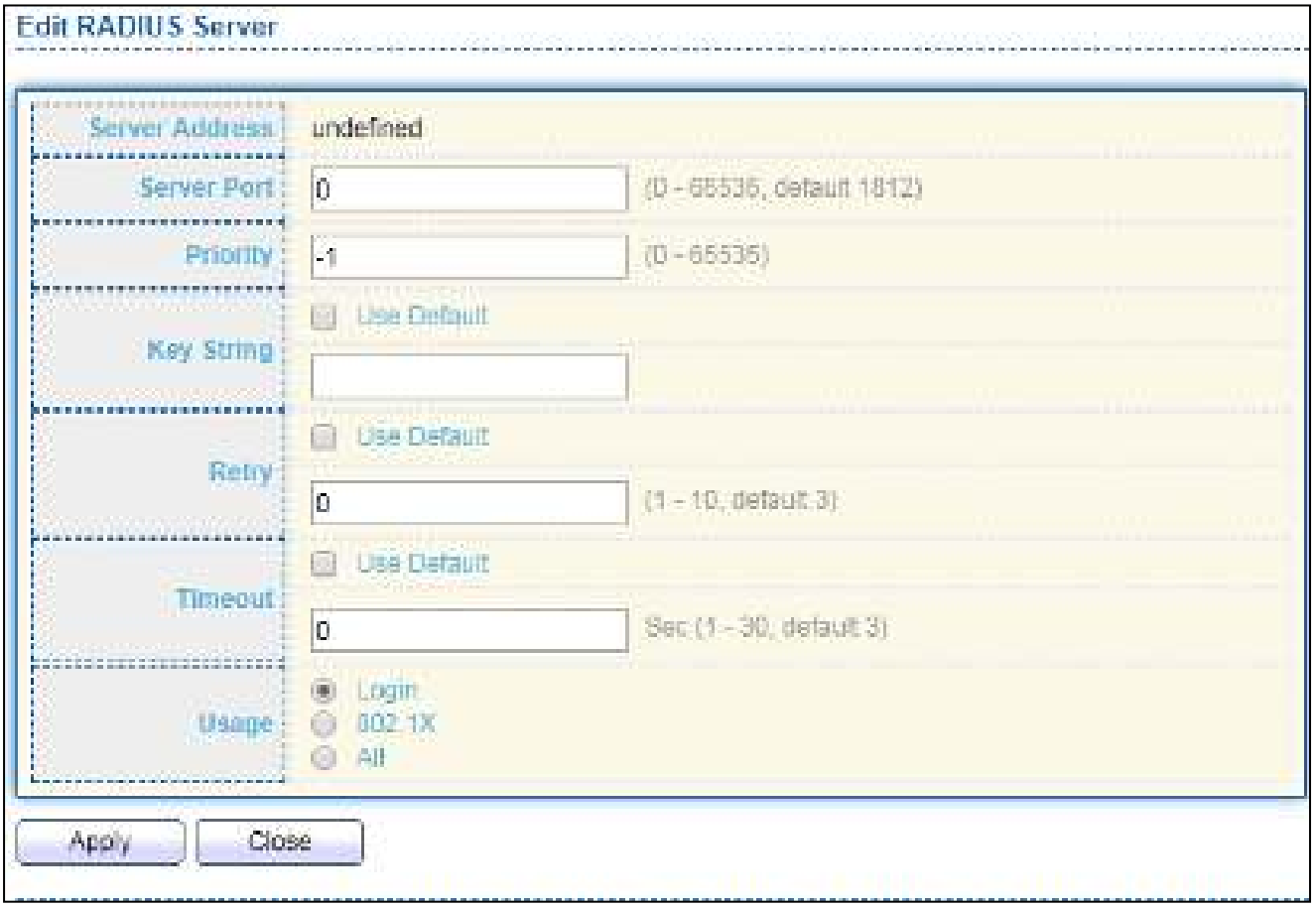


Figure 94 - Security > RADIUS > Add/Edit RADIUS Server

Item	Description
Address Type	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 RADIUS server port.
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.
Retry	Set RADIUS server retry value. If it is fail to connect to server, it will keep trying until timeout with retry times.
Timeout	Set RADIUS server timeout value. If it is fail to connect to server, it will keep trying until timeout.
Usage	Set RADIUS server usage type ● Login: For login authentifation. ● 802.1x: For 802.1x authentication. ● All: For all types.

IV-10-2 Management Access

Use the Management Access pages to configure settings of management access.

IV-10-2-1 Management VLAN

Note: Change Management VLAN may cause connection interrupted

IV-10-2-2 Management Service

This page allow user to change management services related configurations.

To display Management Service click **Security > Management Access > Management Service**.

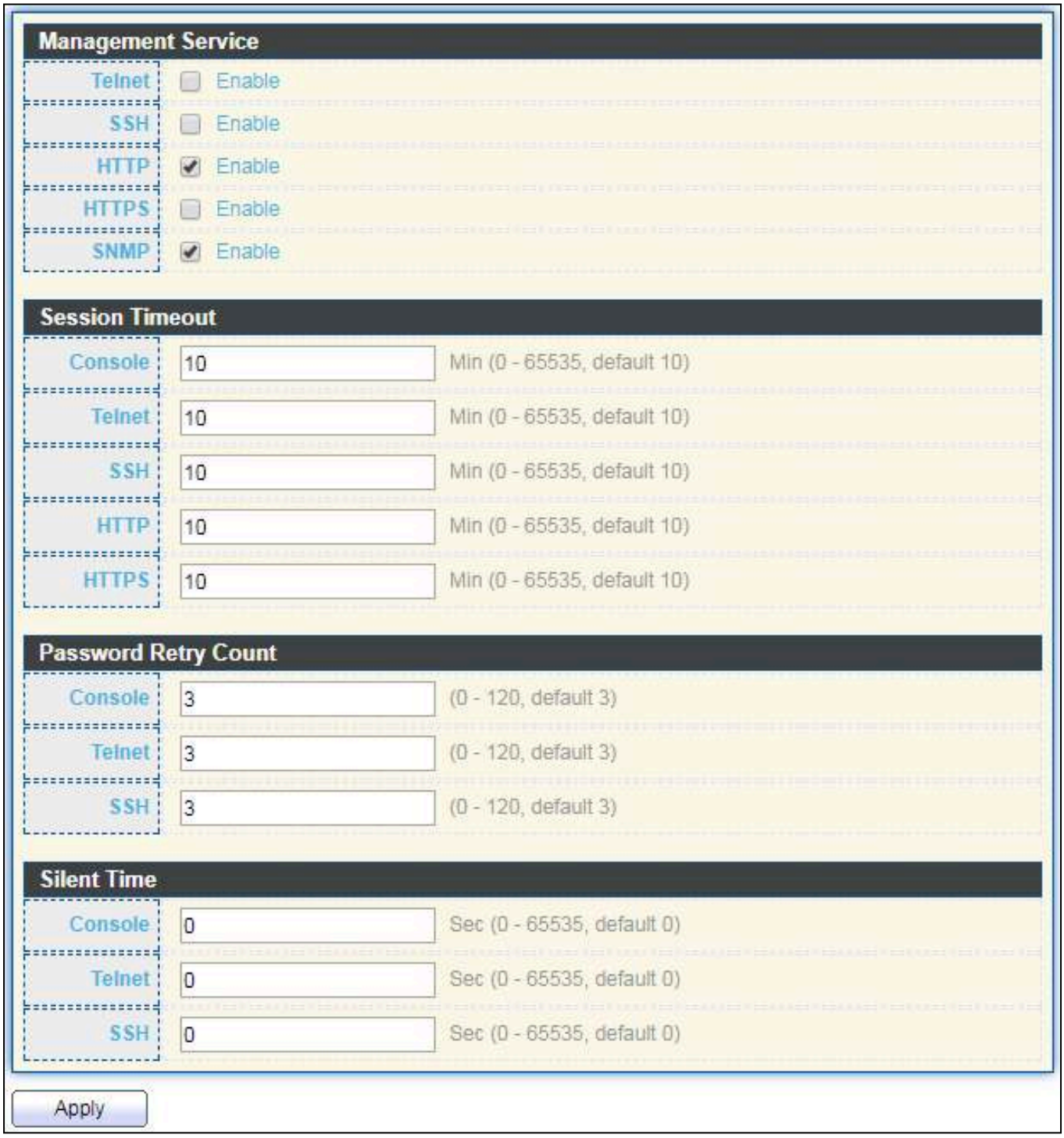


Figure 95 - Security > Management Access > Management Service

Item	Description
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.
Password Retry	Retry count is the number which CLI password input error

Count	tolerance count. After input error password exceeds this count, the CLI will freeze after silent time.
Silent Time	After input error password exceeds password retry count, the CLI will freeze after silent time.

IV-10-2-3 Management ACL

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

To display Management ACL page, click **Security > Management Access > Management ACL**.

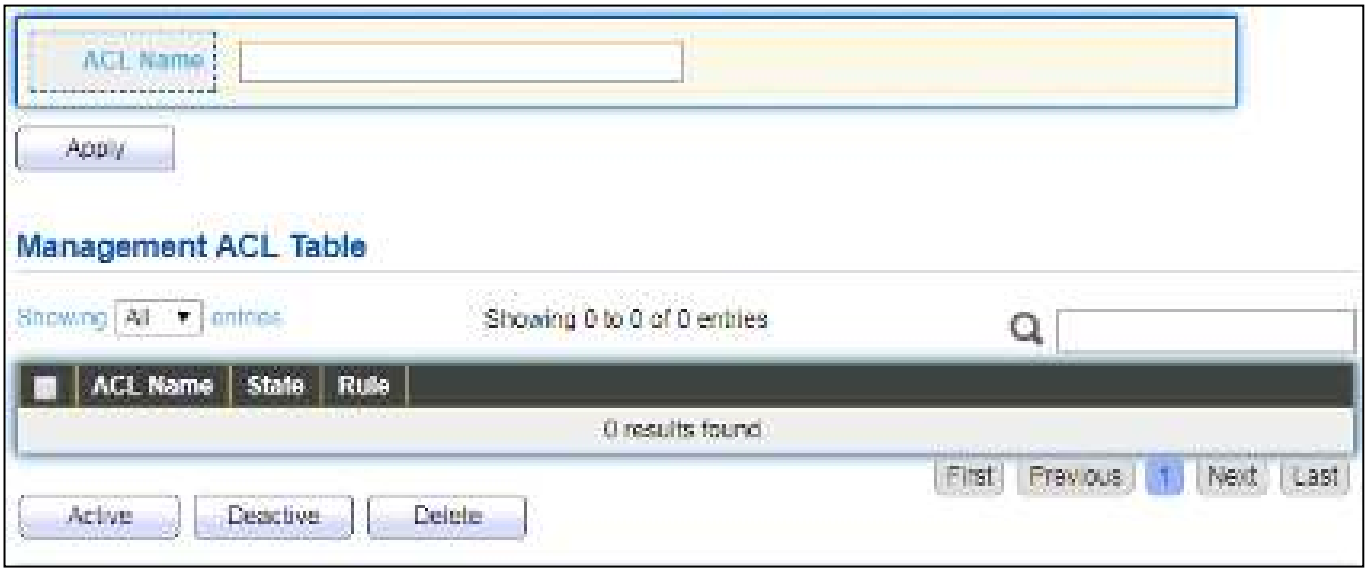


Figure 96 - Security > Management Access > Management ACL

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

IV-10-2-4 Management ACE

This page allow user to add, edit or delete ACE rule. An ACE rule cannot be edited or deleted if ACL under active. New ACE cannot be added if ACL under active

To display Management ACE page, click **Security > Management Access > Management ACE**.

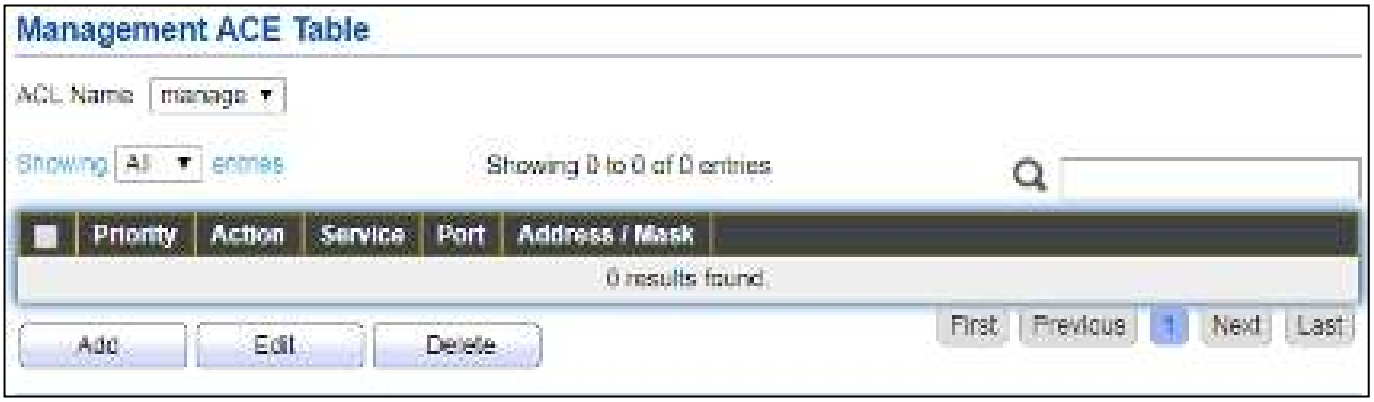
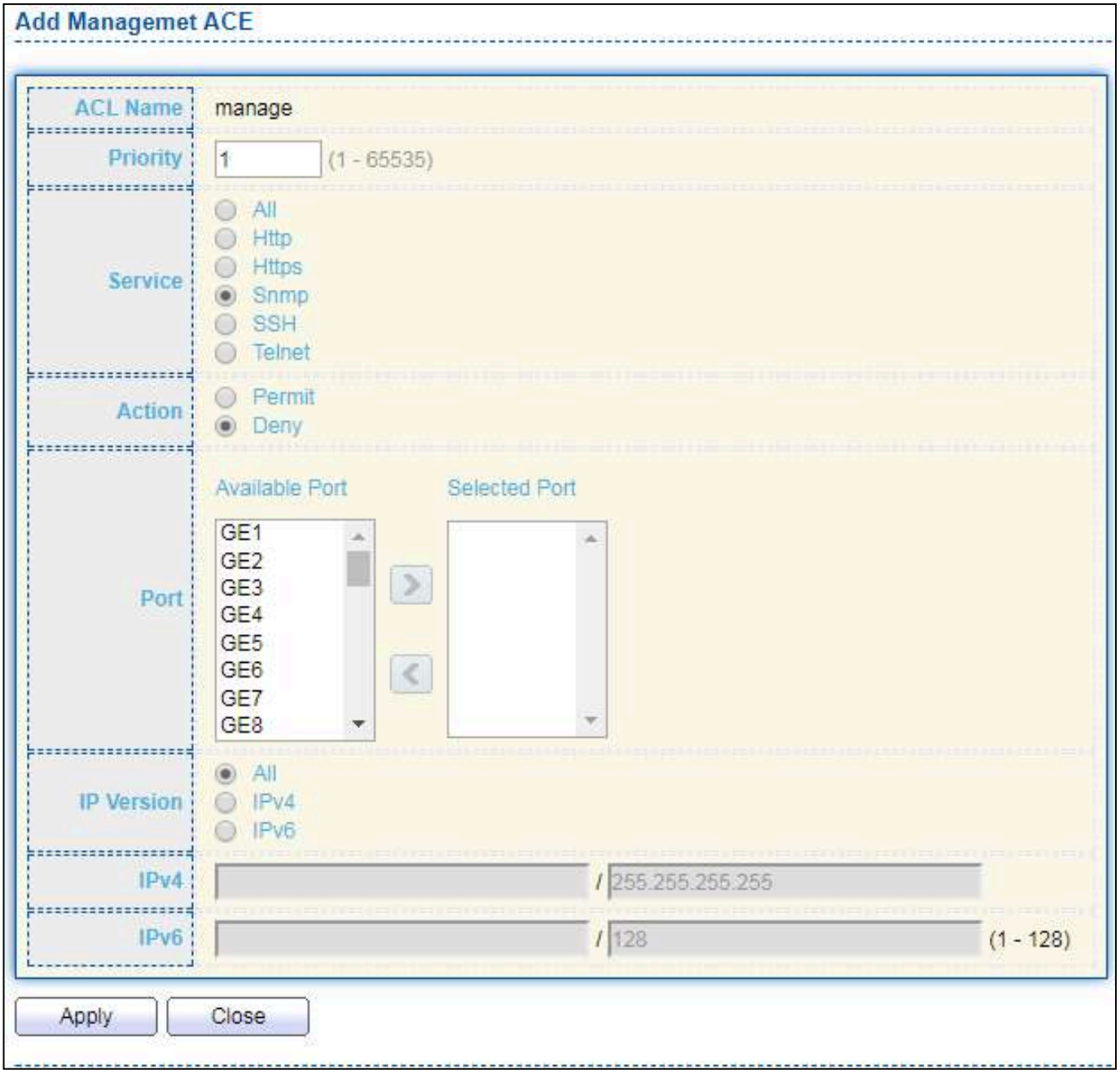


Figure 97 - Security > Management Access > Management ACE

Item	Description
ACL Name	Select the ACL name to which an ACE is being added.
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.

Click "**Add**" or "**Edit**" button to view Add/Edit Management ACE menu.



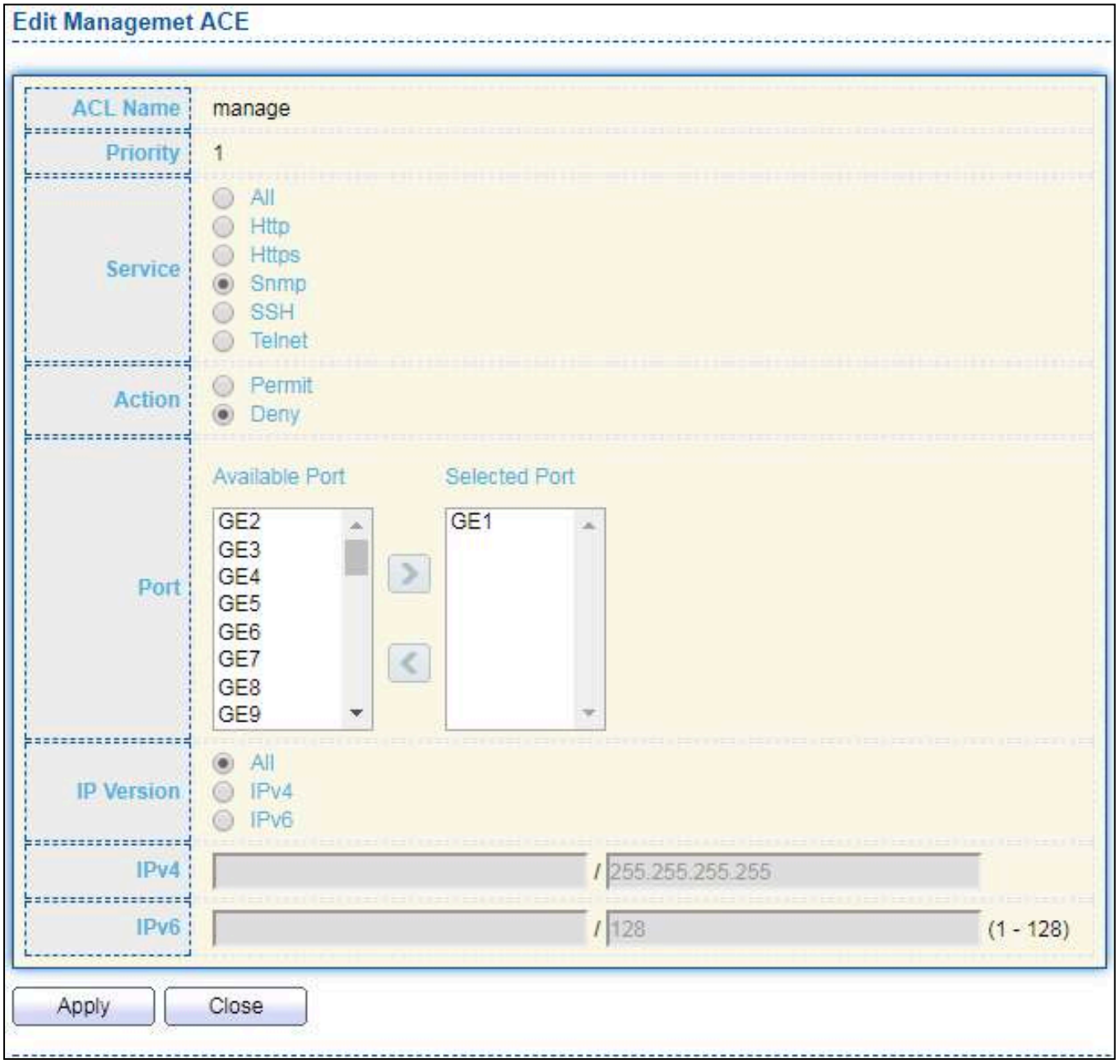


Figure 98 - Security > Management Access > Add/Edit Management ACE

Item	Description
ACL Name	Display the ACL name to which an ACE is being added.
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.

IV-10-3 Authentication Manager

IV-10-3-1 Property

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

To display authentication manager Property web page, click **Security > Authentication Manager > Property**.

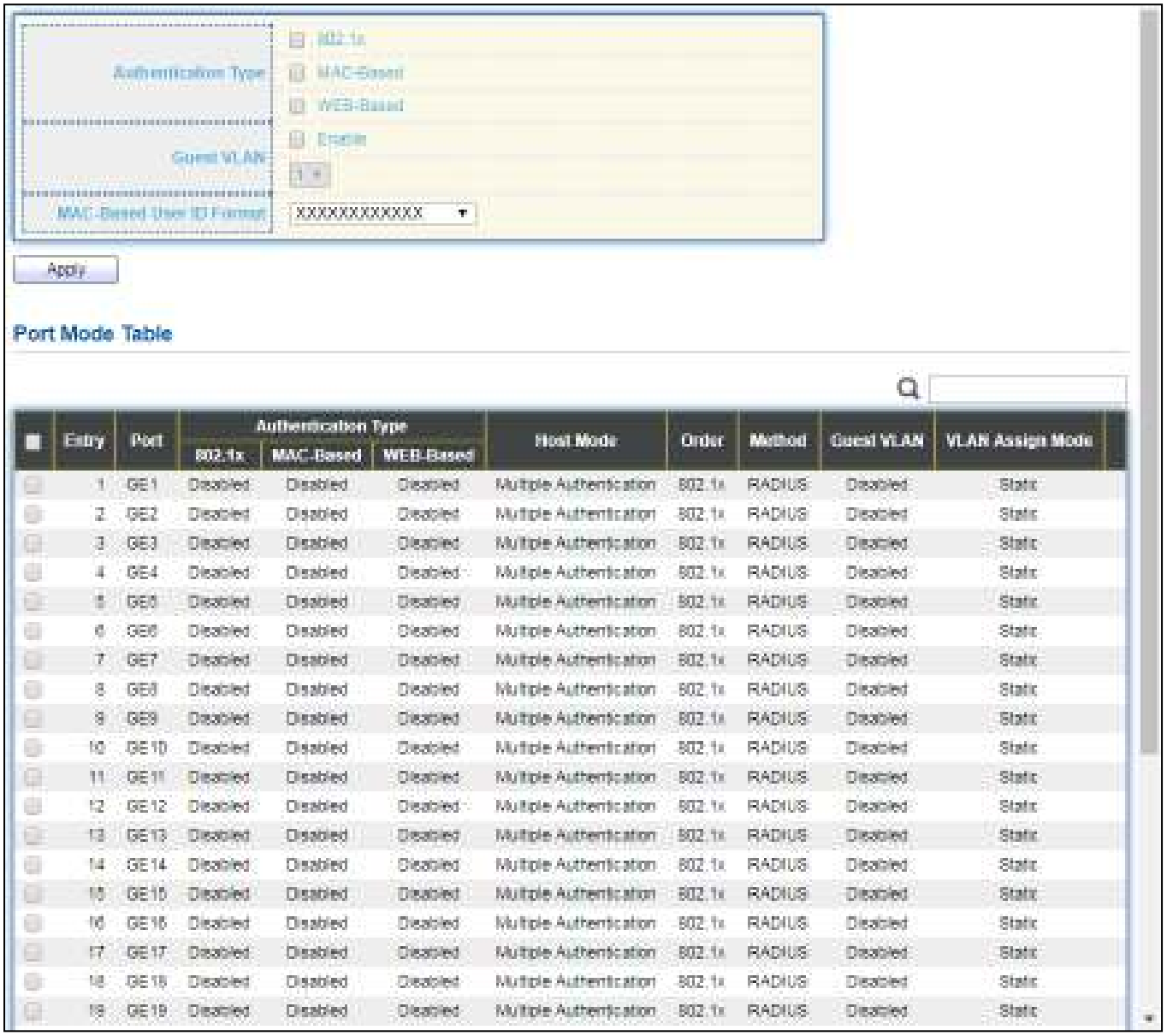


Figure 99 - Security > Authentication Manager > Property

Item	Description
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. ● XXXXXXXXXXXX ● 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-XXXXXX ● XXXXXX-XXXXXX
Port Mode Table	
Port	Port Name.
Authentication Type (802.1X)	802.1X 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.

Click “**Edit**” button to view the Edit Port Mode menu.

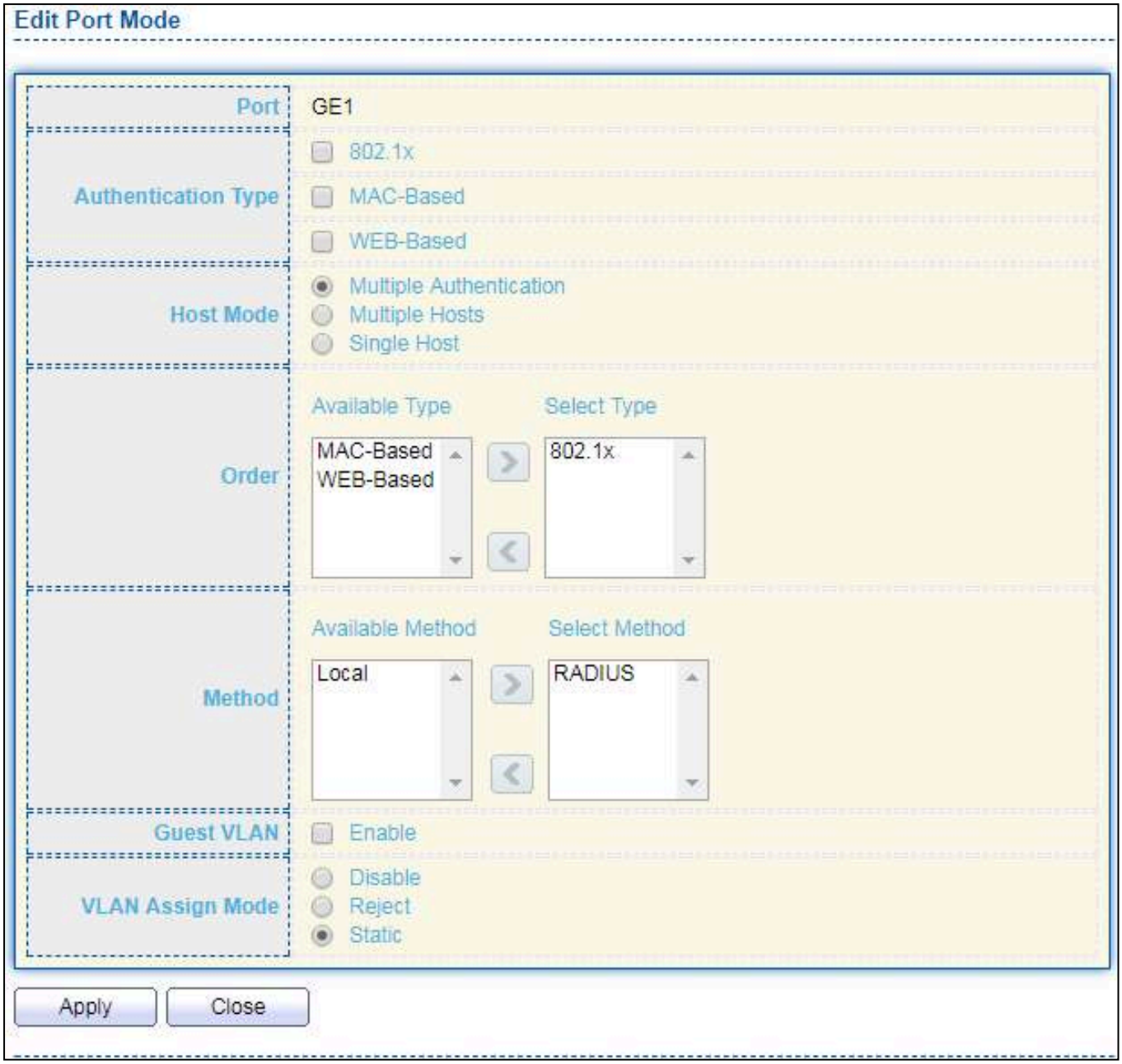


Figure 100 - Security > Authentication Manager > Property > Edit Port Mode

Item	Description
Port	Selected port list.
Authentication Type	Set checkbox to enable/disable authentication types.
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. ● Local Radius. ● Radius Local.
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. ● Static: If get VLAN authorized information, just use it. If there is no VLAN authorized information, keep original VLAN of host.

IV-10-3-2 Port Setting

This page allow user to configure authentication manger port settings

To display the authentication manager Port Setting web page, click **Security > Authentication Manager > Port Setting**.

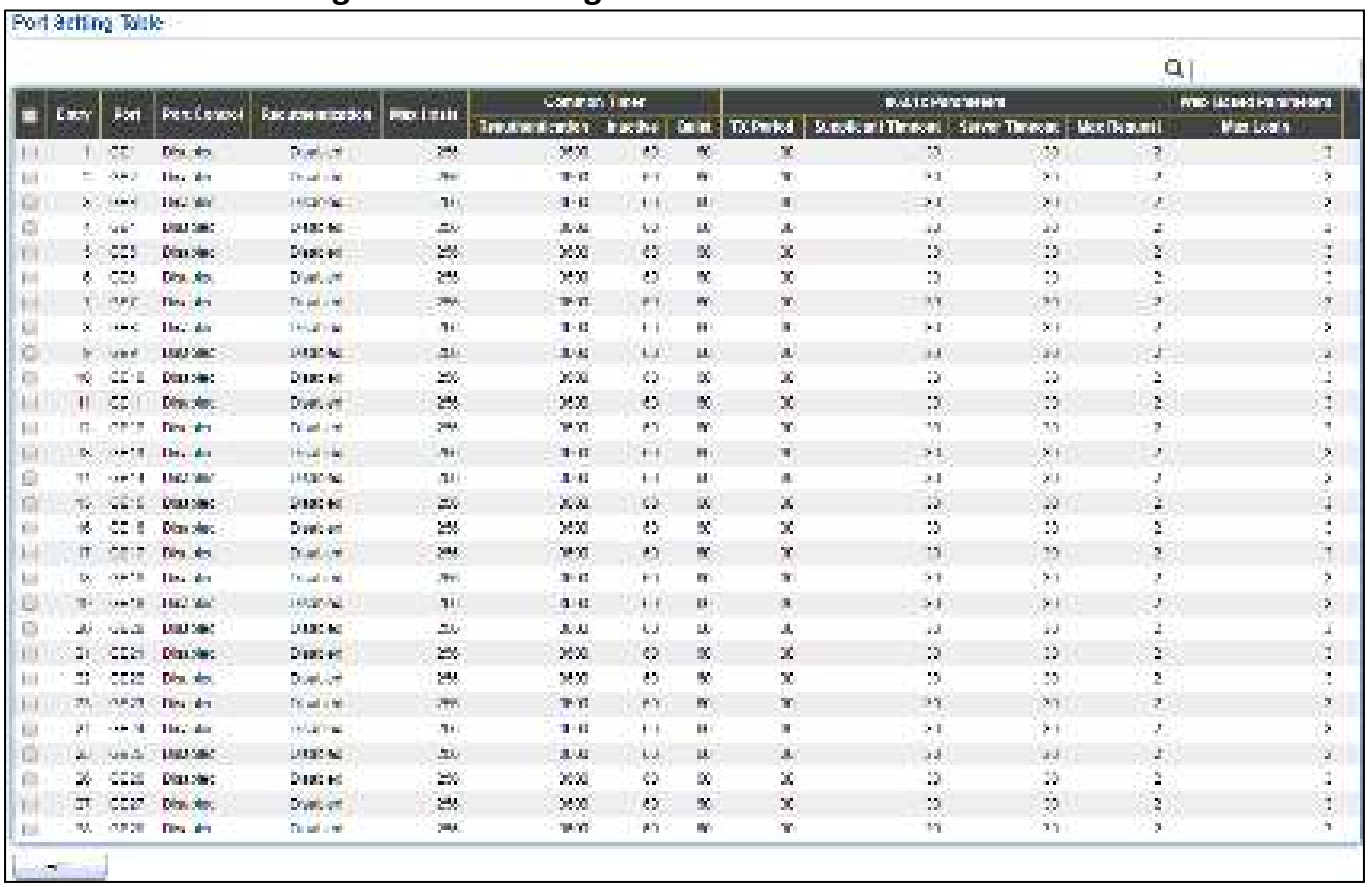


Figure 101 - Security > Authentication Manager > Port Setting

Item	Description
Port	Port
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.
Common Timer (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.
Common Timer (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.
802.1X Params (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.
802.1X Params (Server Timeout)	Number of seconds that lapses before EAP requests are resent to the supplicant.
802.1X Params (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.

Click "**Edit**" button to view Edit Port Setting menu.

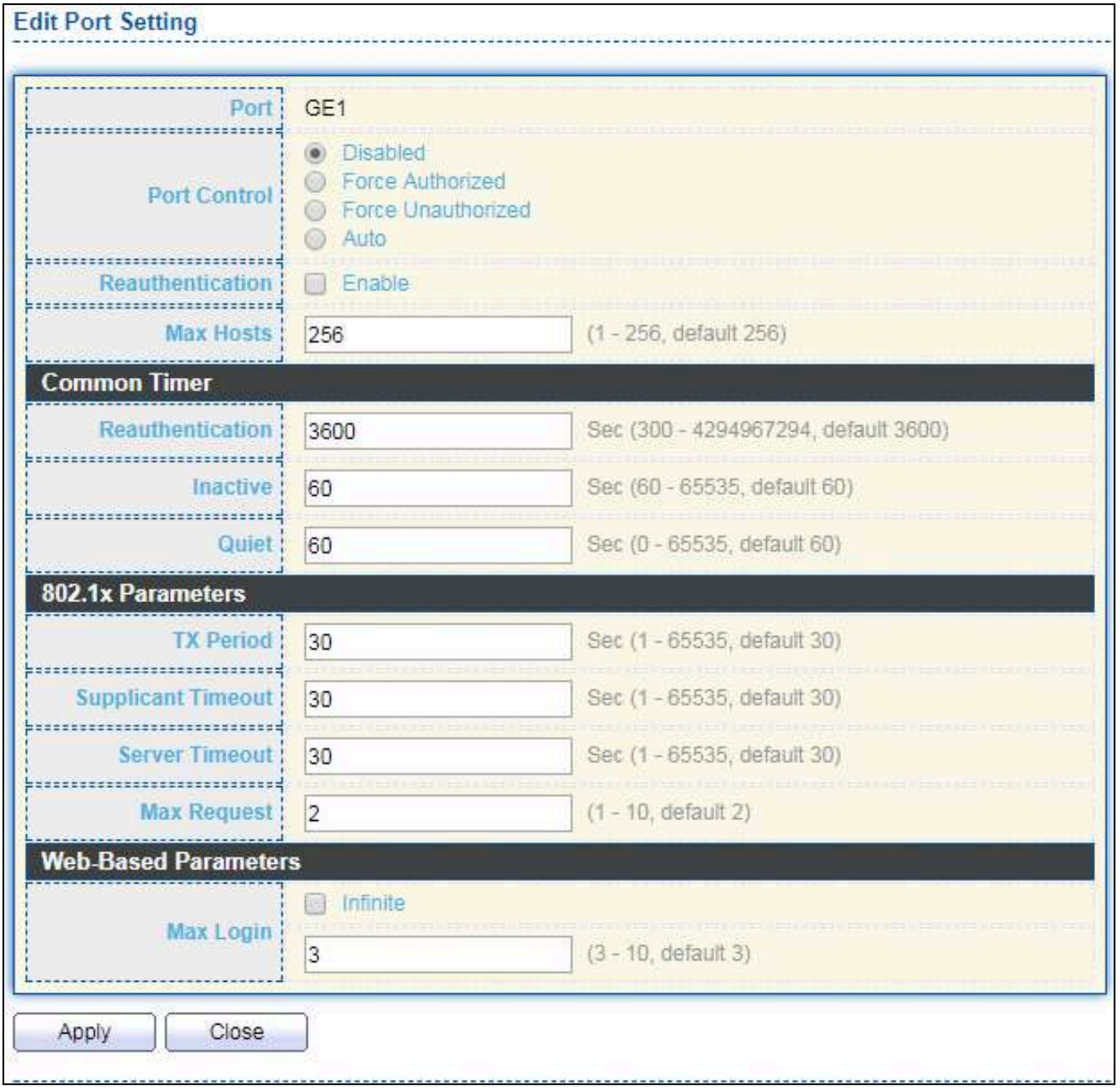


Figure 102 - Security > Authentication Manager > Port Setting > Edit Port Setting

Item	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	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.
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	Set checkbox to set max login number to be infinite or specify max login number.

IV-10-3-3 Sessions

This page show all detail information of authentication sessions and allow user to select specific session to delete by clicking “**Clear** ” button.

To display Sessions web page, click **Security > Authentication Manger > Sessions**.

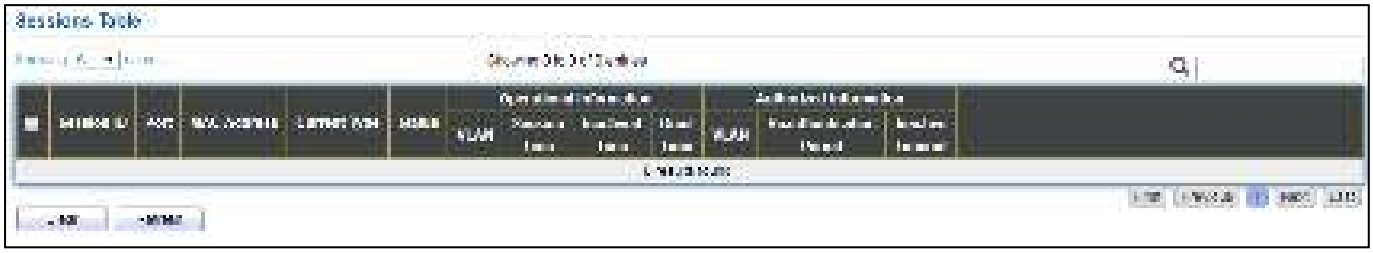


Figure 103 - Security > Authentication Manager > Sessions

Item	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 IP version (IPv4, IPv6) ● 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.
Operational (VLAN)	Shows host operational VLAN ID.
Operational (Session Time)	In “Authorized” state, it shows total time after authorized.
Operational (Inactived)	In “Authorized” state, it shows how long the host do not send any packet.
Operational (Quiet Time)	In “Locked” state, it shows total time after locked.
Authorized (VLAN)	Shows VLAN ID given from authorized procedure.
Authorized (Reauthentication Period)	Shows reauthentication period given from authorized procedure.
Authorized (Inactive Timeouts)	Shows inactive timeout given from authorized procedure.

IV-10-4 Port Security

This page allow user to configure port security settings for each interface. When port security is enabled on interface, action will be perform once learned MAC address over limitation.

To display Port Security web page, click **Security > Port Security**.

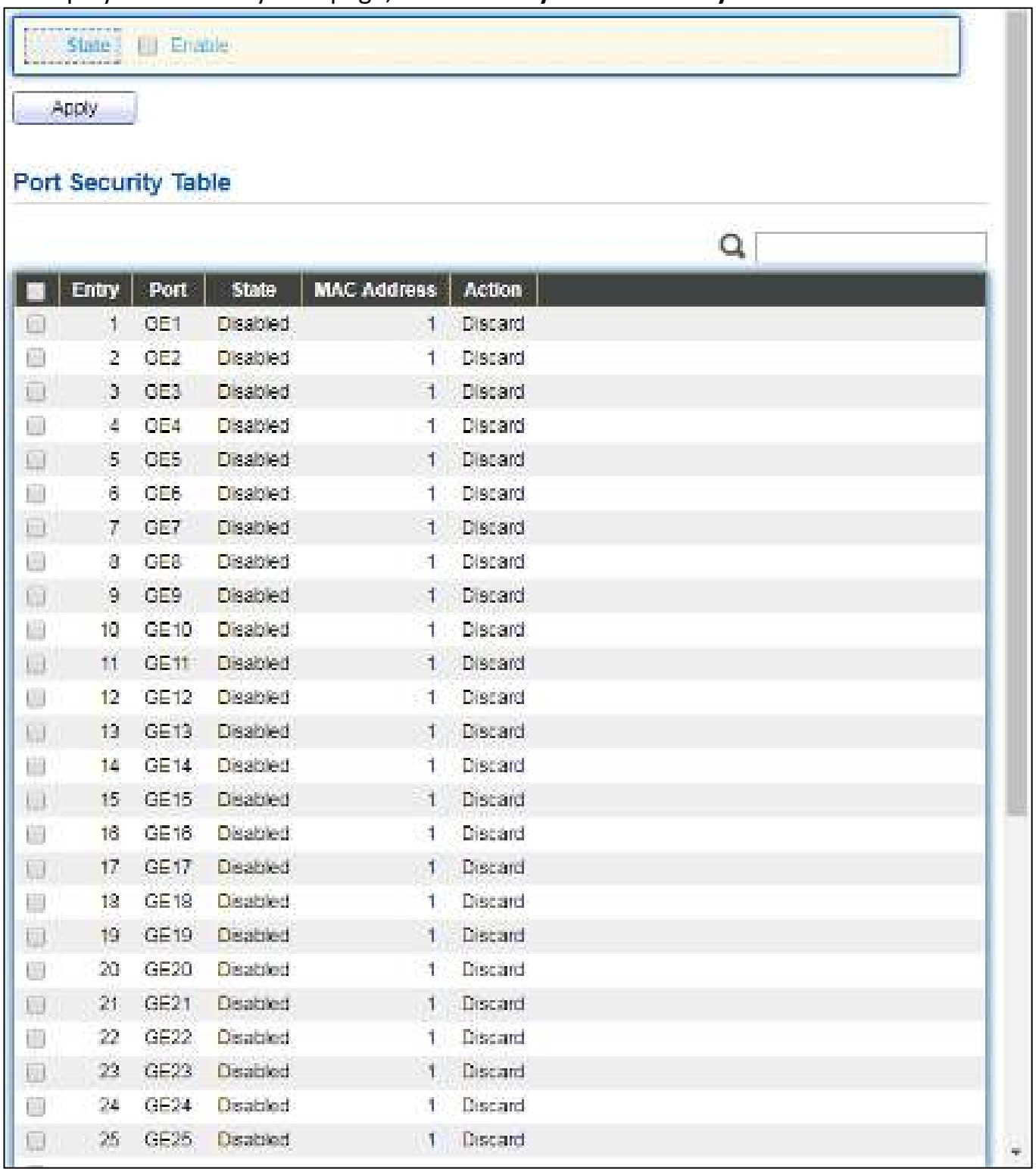


Figure 104 - Security > Port Security

Item	Description
State	Enable/Disable the port security function.
Port	Select one or multiple ports to configure.
State	Select the status of port security ● Disable: Disable port security function. ● Enable: Enable port security function.
MAC Address	Specify the number of how many mac addresses can be learned.
Action	Select the action if learned mac addresses ● Forward: Forward this packet whose SMAC is new to system and exceed the learning-limit number. ● Discard: Discard this packet whose SMAC is new to system and exceed the learning-limit number. ● Shutdown: Shutdown this port when receives a packet whose SMAC is new to system and exceed the learning limit number.

Click "**Edit**" button to view Edit Port Security menu.

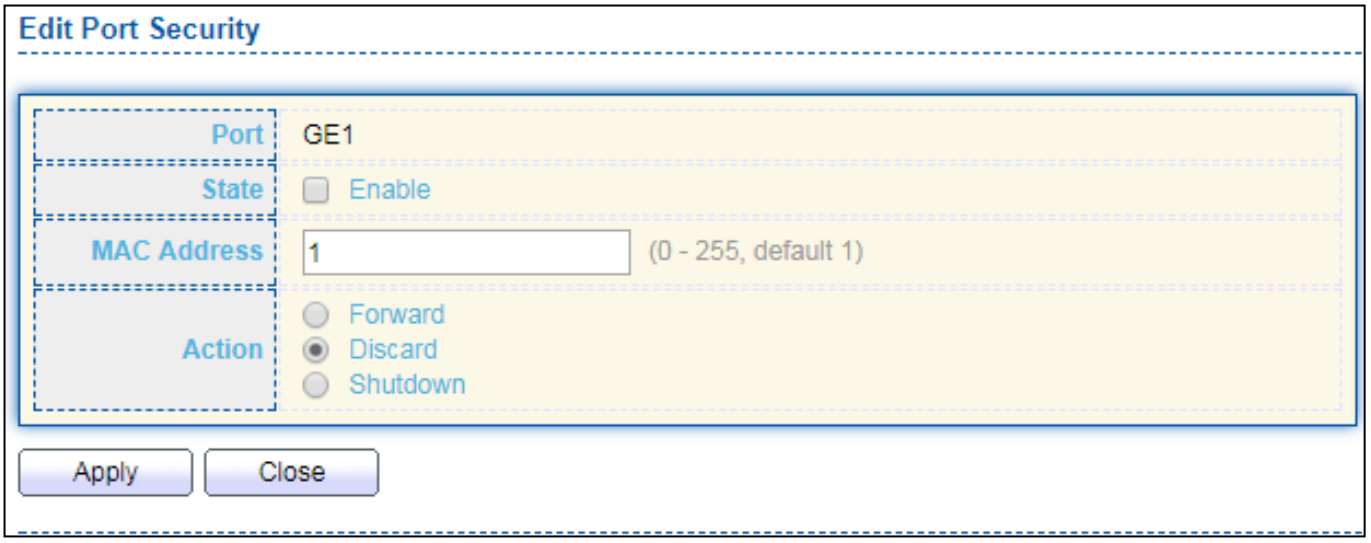
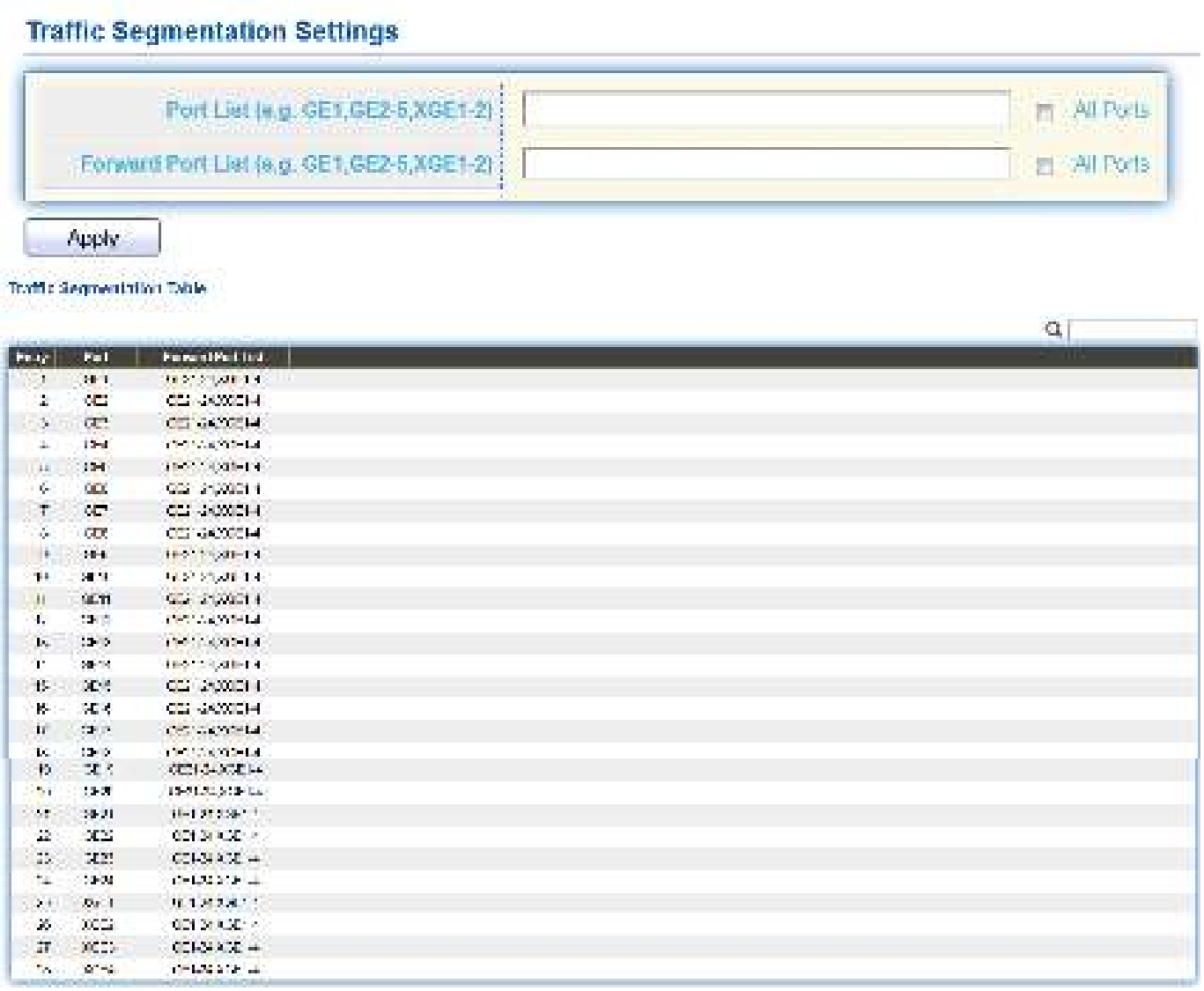


Figure 105 - Security > Port Security > Edd Port Security

Item	Description
Port	Select one or multiple ports to configure.
State	Select the status of port security Disable: Disable port security function. Enable: Enable port security function.
MAC Address	Specify the number of how many mac addresses can be learned.
Action	Select the action if learned mac addresses ● Forward: Forward this packet whose SMAC is new to system and exceed the learning-limit number. ● Discard: Discard this packet whose SMAC is new to system and exceed the learning-limit number. ● Shutdown: Shutdown this port when receives a packet whose SMAC is new to system and exceed the learning limit number.

IV-10-5 Traffic Segmentation

Traffic Segmentation prohibits ports to communicate with each other directly, on other manufacturers' switches



IV-10-6 Storm Control

To display Storm Control global setting web page, click **Security > Storm Control**.

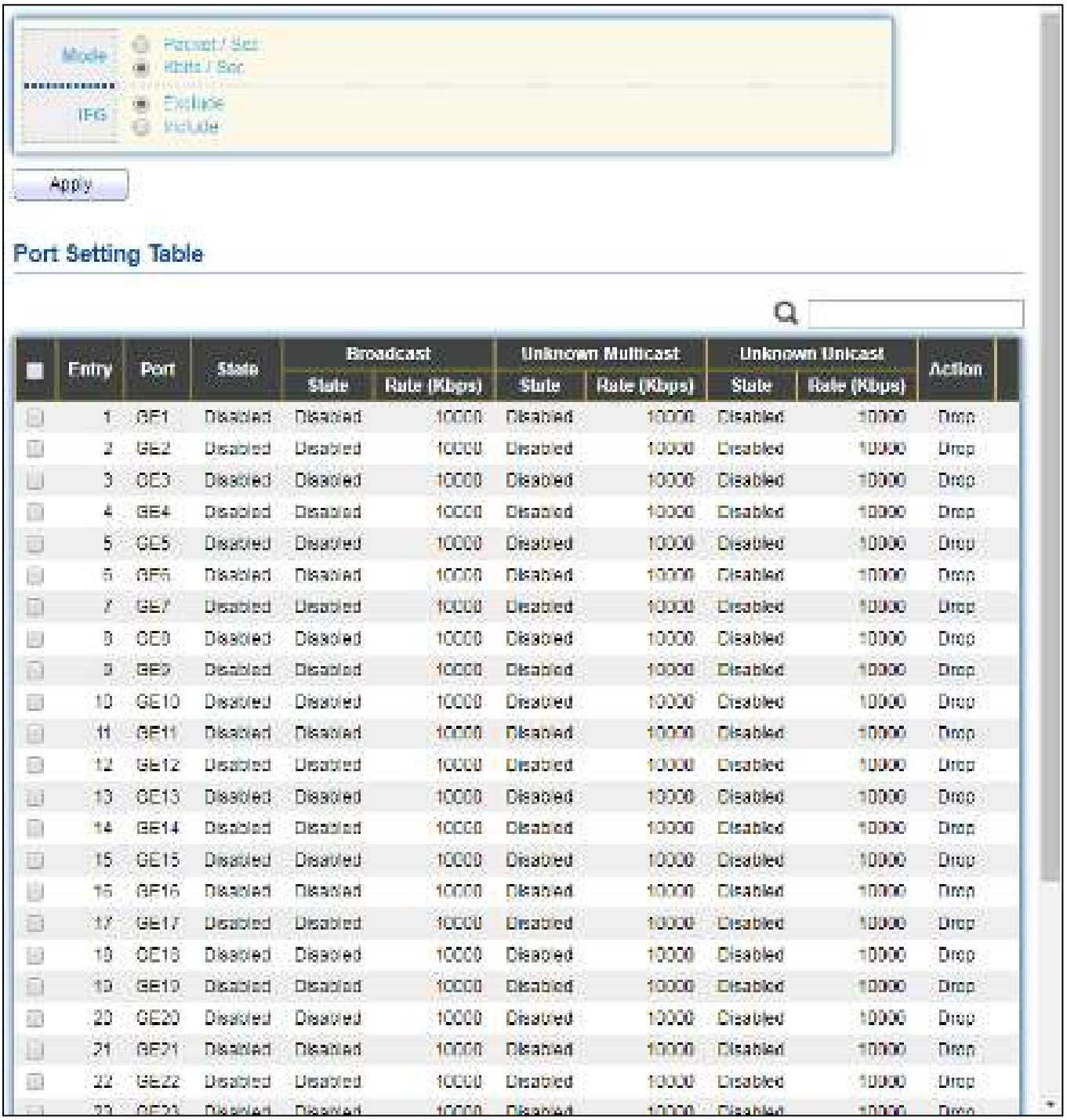


Figure 108 - Security > Storm Control

Item	Description
Mode(Unit)	Select the unit of storm control ● Packet / Sec: storm control rate calculates by packet-based ● Kbits / Sec: storm control rate calculates by octet-based.
IFG	Select the rate calculates w/o preamble & IFG (20 bytes) ● Excluded: exclude preamble & IFG (20 bytes) when count ingress storm control rate.

	● Included: include preamble & IFG (20 bytes) when count ingress storm control rate.

Click "**Edit**" button to view Edit Port Setting menu.

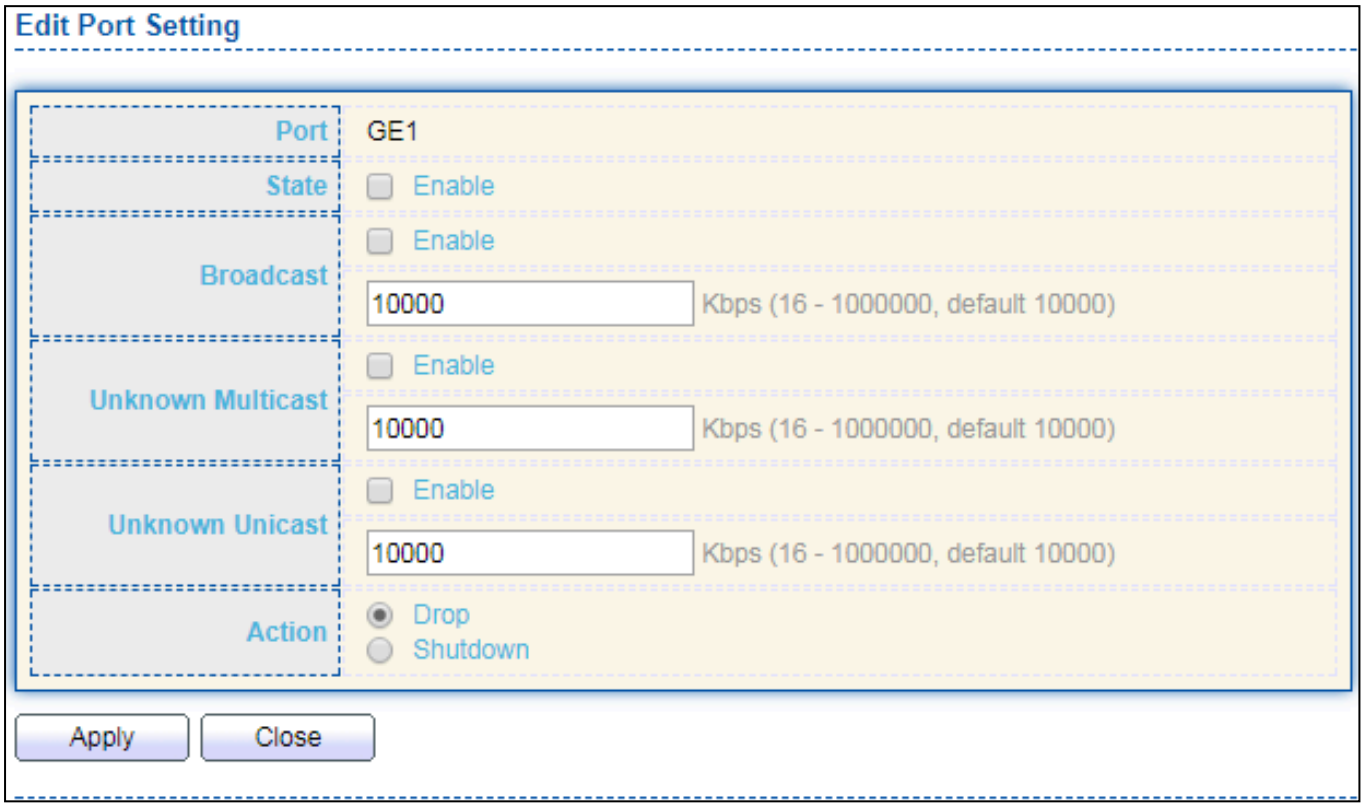


Figure 109 - Security > Storm Control > Edit Port Setting

Item	Description
Port	Select the setting ports.
State	Select the state of setting Enable: Enable the storm control function.
Broadcast	Enable: Enable the storm control function of Broadcast packet. Value of storm control rate, Unit: pps (packet per-second, range 1- 262143) or Kbps (Kbits per-second, range16 - 1000000) depends on global mode setting.
Unknown Multicast	Enable: Enable the storm control function of Unknown multicast packet. Value of storm control rate, Unit: pps (packet per-second, range 1- 262143) or Kbps (Kbits per-second, range16 - 1000000) depends on global mode setting.
Unknown Unicast	Enable: Enable the storm control function of Unknown unicast packet. Value of storm control rate, Unit: pps (packet per-second, range 1 - 262143) or Kbps (Kbits per-second, range16 - 1000000) depends on global mode setting.
Action	Select the state of setting ● Drop: Packets exceed storm control rate will be dropped. ● Shutdown: Port will be shutdown when packets exceed storm

	control rate.

IV-10-7 DoS

A Denial of Service (DoS) attack is a hacker attempt to make a device unavailable to its users. DoS attacks saturate the device with external communication requests, so that it cannot respond to legitimate traffic. These attacks usually lead to a device CPU overload.

The DoS protection feature is a set of predefined rules that protect the network from malicious attacks. The DoS Security Suite Settings enables activating the security suite.

IV-10-7-1 Property

To display Dos Global Setting web page, click **Security > Dos > Property**.

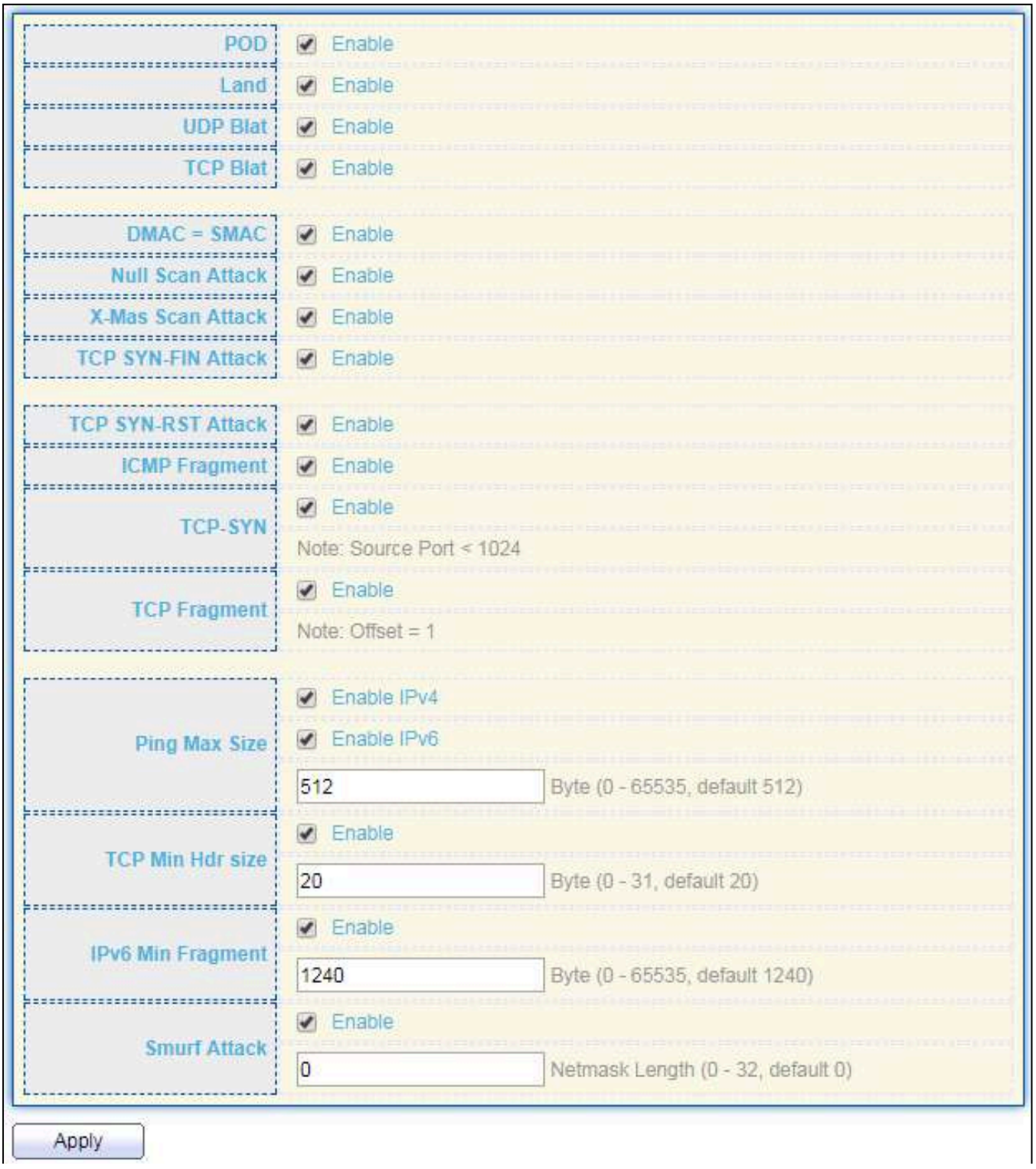


Figure 110 - Security > DoS > Property

Item	Description
POD	Avoids ping of death attack.
Land	Drops the packets if the source IP address is equal to the destination IP address.
UDP Blat	Drops the packets if the UDP source port equals to the UDP

	destination port.
TCP Blat	Drops the packages if the TCP source port is equal to the TCP destination port.
DMAC = SMAC	Drops the packets if the destination MAC address is equal to the source MAC address.
Null Scan Attach	Drops the packets with NULL scan.
X-Mas Scan Attack	Drops the packets if the sequence number is zero, and the FIN, URG and PSH bits are set.
TCP SYN-FIN Attack	Drops the packets with SYN and FIN bits set.
TCP SYN-RST Attack	Drops the packets with SYN and RST bits set
ICMP Fragment	Drops the fragmented ICMP packets.
TCP SYN (SPORT<1024)	Drops SYN packets with sport less than 1024.
TCP Fragment (Offset = 1)	Drops the TCP fragment packets with offset equals to one.
Ping Max Size	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.
IPv6 Min Fragment	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.
Smurf Attack	Avoids smurf attack. The length range of the netmask is from 0 to 323 bytes, and default length is 0 bytes.

IV-10-7-2 Port Setting

To configure and display the state of DoS protection for interfaces, click **Security > DoS > Port Setting**.

Figure 111 - Security > DoS > Port Setting

Item	Description
Port	Interface or port number.
State	Enable/Disable the DoS protection on the interface.

IV-10-8 DHCP Snooping

Use the DHCP Snooping pages to configure settings of DHCP Snooping.

IV-10-8-1 Property

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

To display property page, click **Security > DHCP Snooping > Property**.

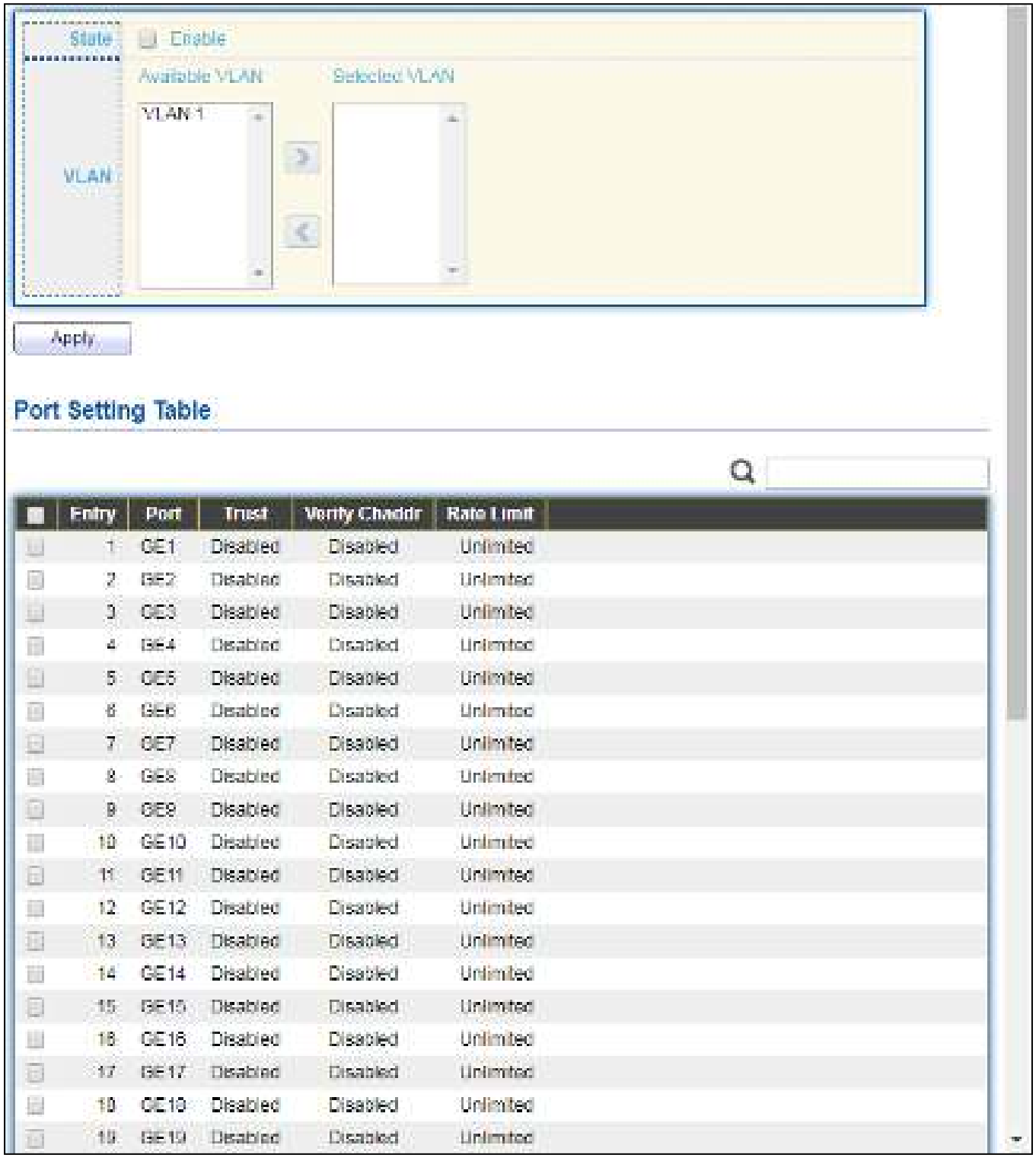


Figure 112 - Security > DHCP Snooping > Property

Item	Description
State	Set checkbox to enable/disable DHCP Snooping function.
VLAN	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.
Port Setting Table	
Port	Display port ID.
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.

Click "**Edit**" button to view Edit Port Setting menu.

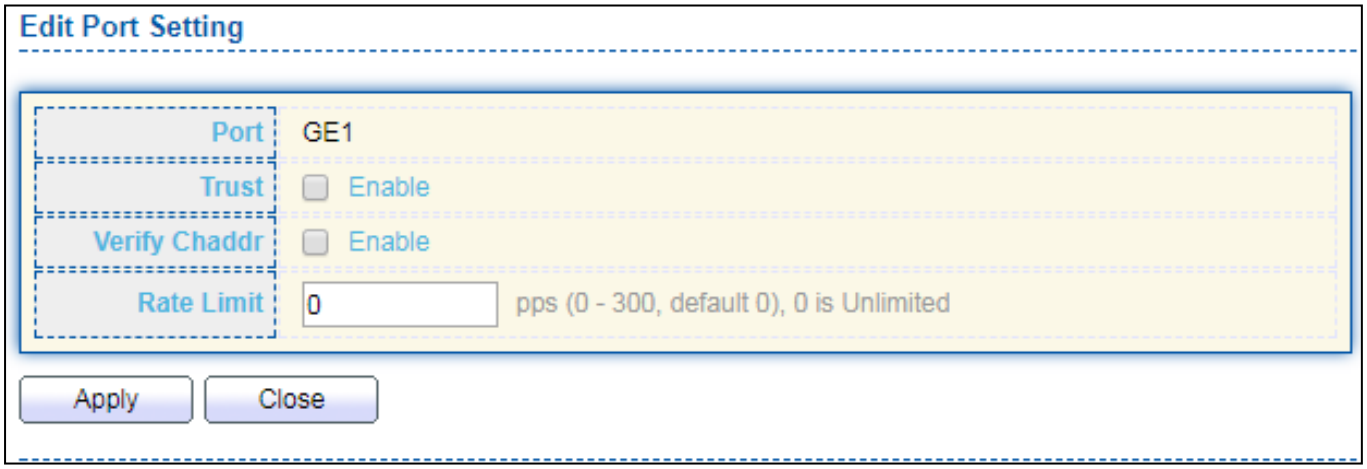


Figure 113 - Security > DHCP Snooping > Property > Edit Port Setting

Item	Description
Port	Display selected port to be edited
Trust	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	Input rate limitation of DHCP packets. The unit is pps. 0 means unlimited. Default is unlimited.

IV-10-8-2 Statistics

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

To view the Statistics menu, navigate to **Security > DHCP Snooping > Statistics**.

Figure 114 - Security > DHCP Snooping > Statistics

Item	Description
Port	Display port ID.
Forwarded	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.

IV-10-8-3 Option82 Property

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

To display Option82 Property page, click **Security > DHCP Snooping > Option82 Property**.

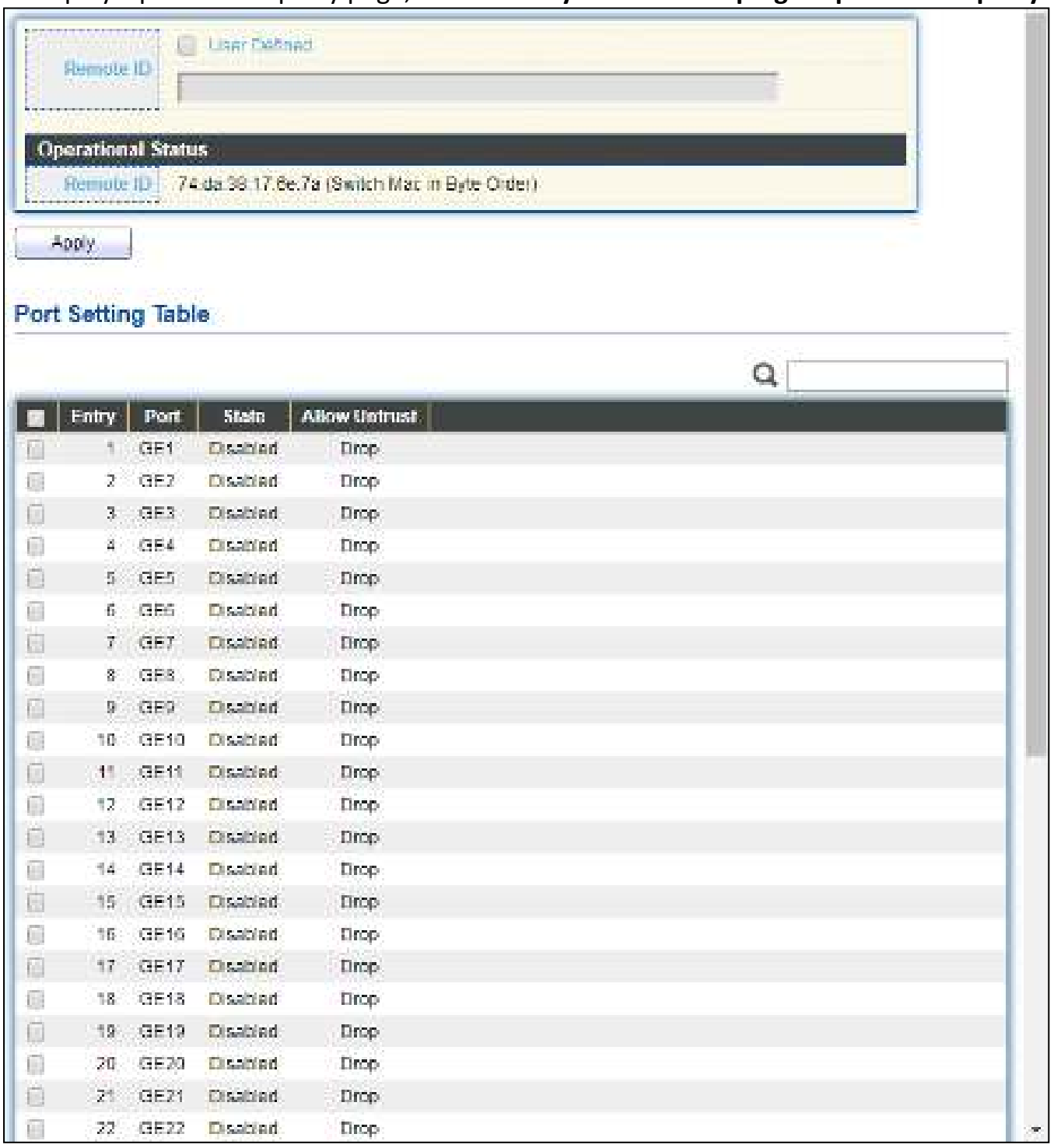


Figure 115 - Security > DHCP Snooping > Option82 Property

Item	Description
User Defined	Set checkbox to enable user-defined remote-ID. By default, remote ID is switch mac in byte order.

Remote ID	Input user-defined remote ID. Only available when enable user-define remote ID.
Port Setting Table	
Port	Display port ID.
State	Display option82 enable/disable status of interface.
Allow untrusted	Display allow untrusted action of interface.

Click "**Edit**" button to view Edit Port Setting menu.

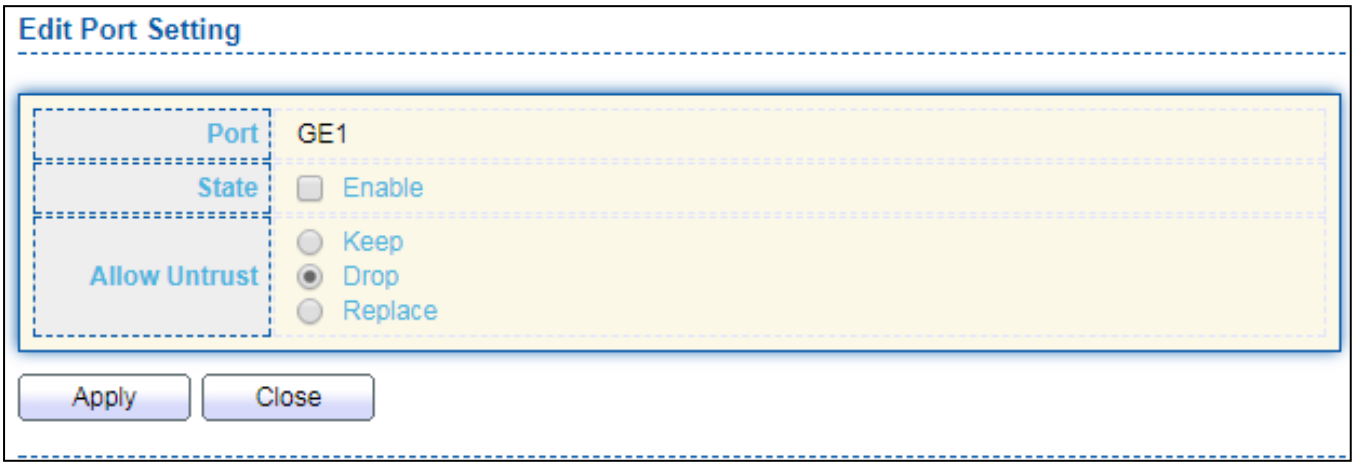


Figure 116 DHCP Snooping > Option82 Property > Edit Port Setting

Item	Description
Port	Display selected port to be edited
State	Set checkbox to enable/disable option82 function 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. ● Replace: Replace option82 content by switch setting ● Drop: Drop packets with option82

IV-10-8-4 Option82 Circuit ID

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

To display Option82 Circuit ID page, click **Security > DHCP Snooping > Option82 Circuit ID**.

Figure 117 - Security > DHCP Snooping > Option82 Circuit ID

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

Click “**Add**” button or "**Edit**" button to view the Add/Edit Option82 Circuit ID menu.

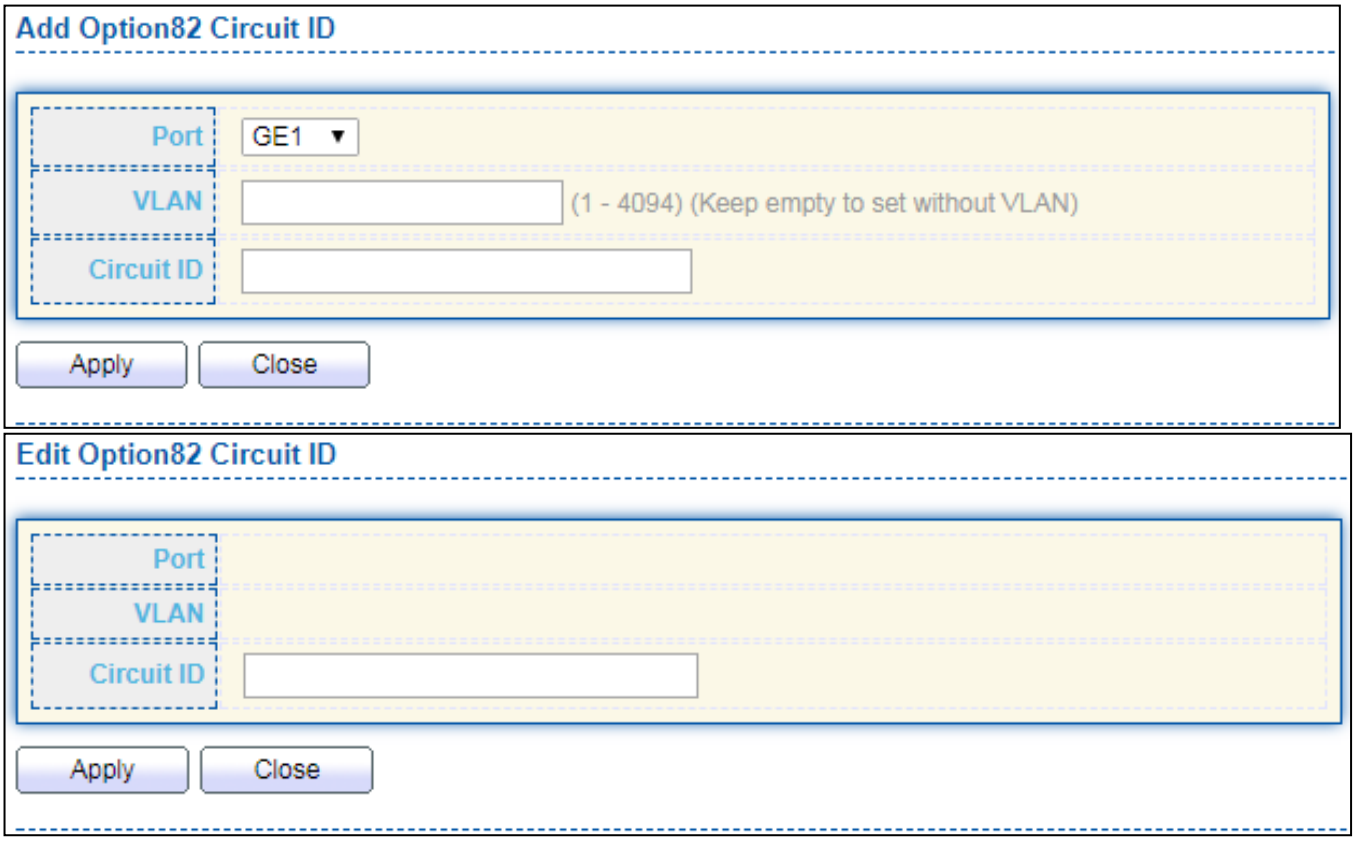


Figure 118 - Security > DHCP Snooping > Option82 Circuit ID > Add/Edit Option82 Circuit ID

Item	Description
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.
Circuit ID	Input String as circuit ID. Packets match port and VLAN will be inserted circuit ID.

IV-10-9 IP Source Guard

Use the IP Source Guard pages to configure settings of IP Source Guard.

IV-10-9-1 Port Setting

Use the IP Source Guard pages to configure settings of IP Source Guard.

To display Port Setting page, click **Security > IP Source Guard > Port Setting**.

Port Setting Table

Entry	Port	State	Verify Source	Current Entry	Max Entry
1	GE1	Disabled	IP	0	Unlimited
2	GE2	Disabled	IP	0	Unlimited
3	GE3	Disabled	IP	0	Unlimited
4	GE4	Disabled	IP	0	Unlimited
5	GE5	Disabled	IP	0	Unlimited
6	GE6	Disabled	IP	0	Unlimited
7	GE7	Disabled	IP	0	Unlimited
8	GE8	Disabled	IP	0	Unlimited
9	GE9	Disabled	IP	0	Unlimited
10	GE10	Disabled	IP	0	Unlimited
11	GE11	Disabled	IP	0	Unlimited
12	GE12	Disabled	IP	0	Unlimited
13	GE13	Disabled	IP	0	Unlimited
14	GE14	Disabled	IP	0	Unlimited
15	GE15	Disabled	IP	0	Unlimited
16	GE16	Disabled	IP	0	Unlimited
17	GE17	Disabled	IP	0	Unlimited
18	GE18	Disabled	IP	0	Unlimited
19	GE19	Disabled	IP	0	Unlimited
20	GE20	Disabled	IP	0	Unlimited
21	GE21	Disabled	IP	0	Unlimited
22	GE22	Disabled	IP	0	Unlimited
23	GE23	Disabled	IP	0	Unlimited
24	GE24	Disabled	IP	0	Unlimited
25	GE25	Disabled	IP	0	Unlimited
26	GE26	Disabled	IP	0	Unlimited
27	GE27	Disabled	IP	0	Unlimited
28	GE28	Disabled	IP	0	Unlimited
29	LAG1	Disabled	IP	0	Unlimited
30	LAG2	Disabled	IP	0	Unlimited
31	LAG3	Disabled	IP	0	Unlimited

Figure 119 - Security > IP Source Guard > Port Setting

Item	Description
Port	Display port ID.
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.

Click "**Edit**" button to view the Edit Port Setting menu.

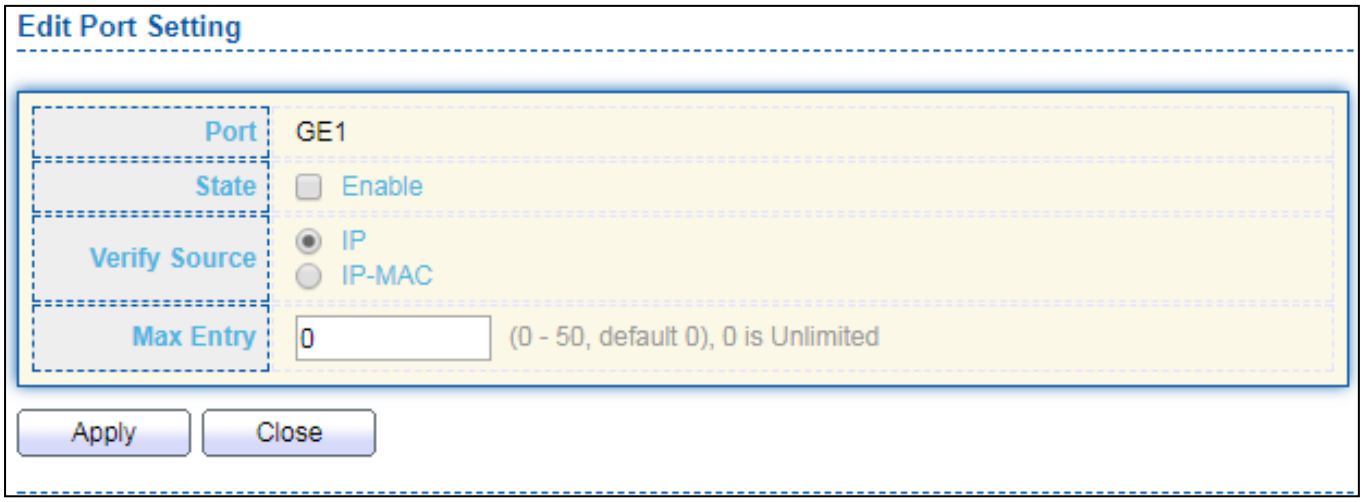


Figure 120 - Security > IP Source Guard > Port Setting > Edit Port Setting

Item	Description
Port	Display selected port to be edited.
Status	Set checkbox to enable or disable IP Source Guard function. Default is disabled.
Verify Source	Select the mode of IP Source Guard verification ● IP: Only verify source IP address of packet. ● IP-MAC: Verify source IP and source MAC address of packet.
Max Entry	Input the maximum number of entries that a port can be bounded. Default is un-limited on all ports. No entry will be bound if limitation reached.

IV-10-9-2 IMPV Binding

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.

To display IPMV Binding page, click **Security > IP Source Guard > IMPV Binding**.

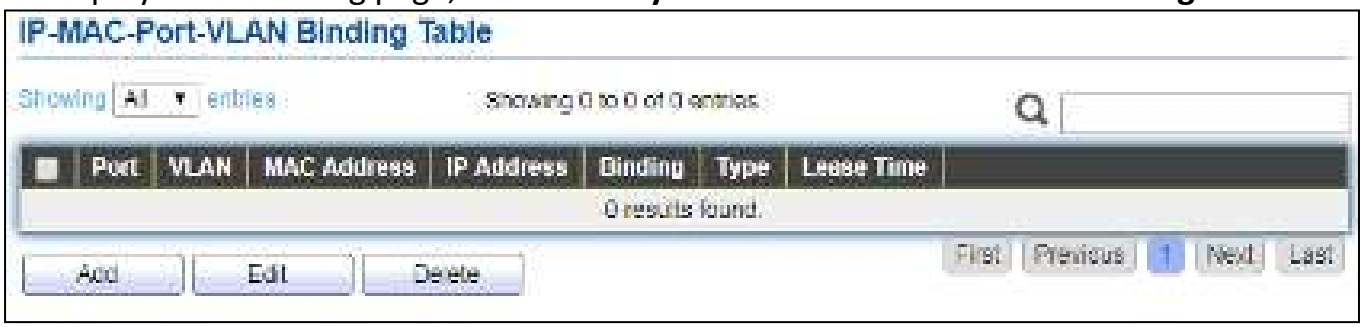


Figure 121 - Security > IP Source Guard > IMPV Binding

Item	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.
Type	Type of existing binding entry ● Static: Entry added by user. ● 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.

Click "**Add**" or "**Edit**" button to view the Add/Edit IP-MAC-Port-VLAN Binding menu.

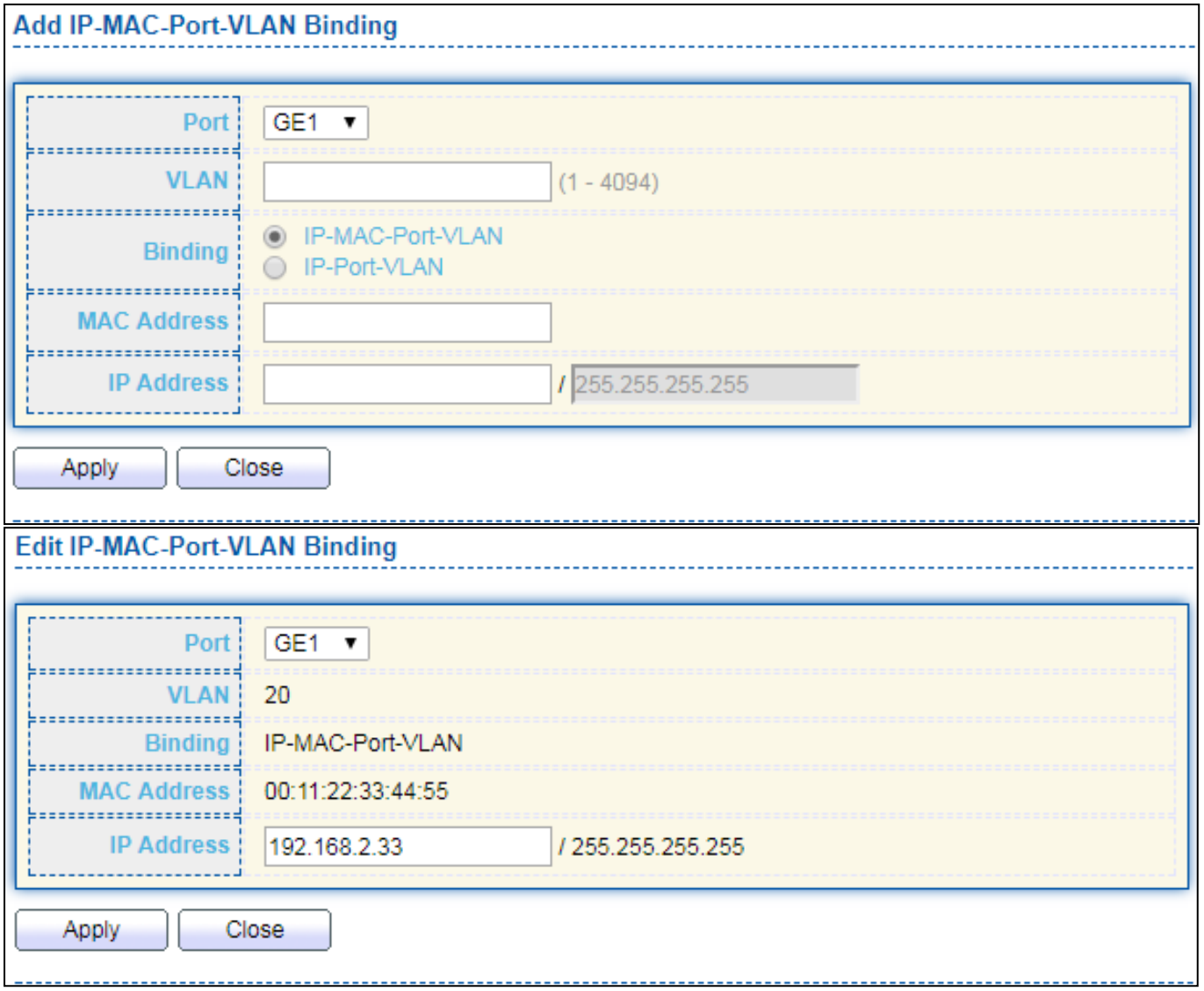


Figure 122 - Security > IP Source Guard > Add/Edit IP-MAC-Port-VLAN Binding

Item	Description
Port	Select port from list of a binding entry.
VLAN	Specify a VLAN ID of a binding entry.
Binding	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.

IV-10-9-3 Save Database

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

To display Save Database page, click **Security > DHCP Snooping > Save Database**.

Figure 123 - Security > IP Source Guard > Save Database

Item	Description
Type	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	Input filename for backup file. Only available when selecting type “flash” and “TFTP”.
Address Type	Select the type of 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 available when 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.

IV-11 ACL

Use the ACL pages to configure settings for the switch ACL features..

IV-11-1 MAC ACL

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

To display MAC ACL page, click **ACL > MAC ACL**.

Figure 124 - ACL > MAC ACL

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

IV-11-2 MAC 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.

To display MAC ACE page, click **ACL > MAC ACE**.

Figure 125 - ACL > MAC ACE

Item	Description
ACL Name	Select the ACL name to which an ACE is being added.
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.

Click “**Edit**” button to view the Edit ACE menu.

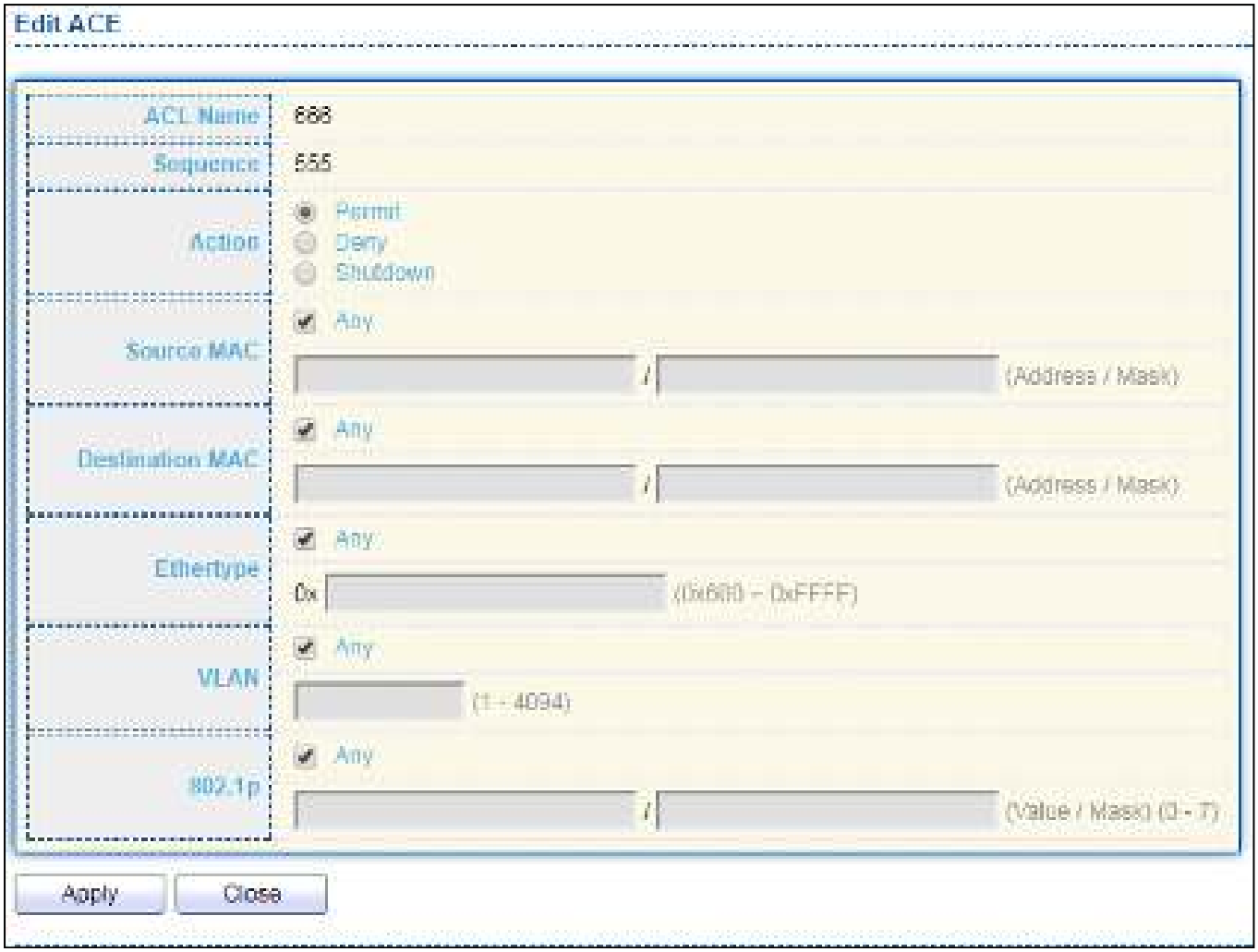


Figure 126 - ACL > Edit ACE

Item	Description
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	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	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.
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	Select the type for VLAN ID. ● Any: All VLAN ID is acceptable. ● 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: 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.

IV-11-3 IPv4 ACL

This page allow user to add or delete IPv4 ACL rule. A rule cannot be deleted if under binding.

To display IPv4 ACL page, click **ACL > IPv4 ACL**.

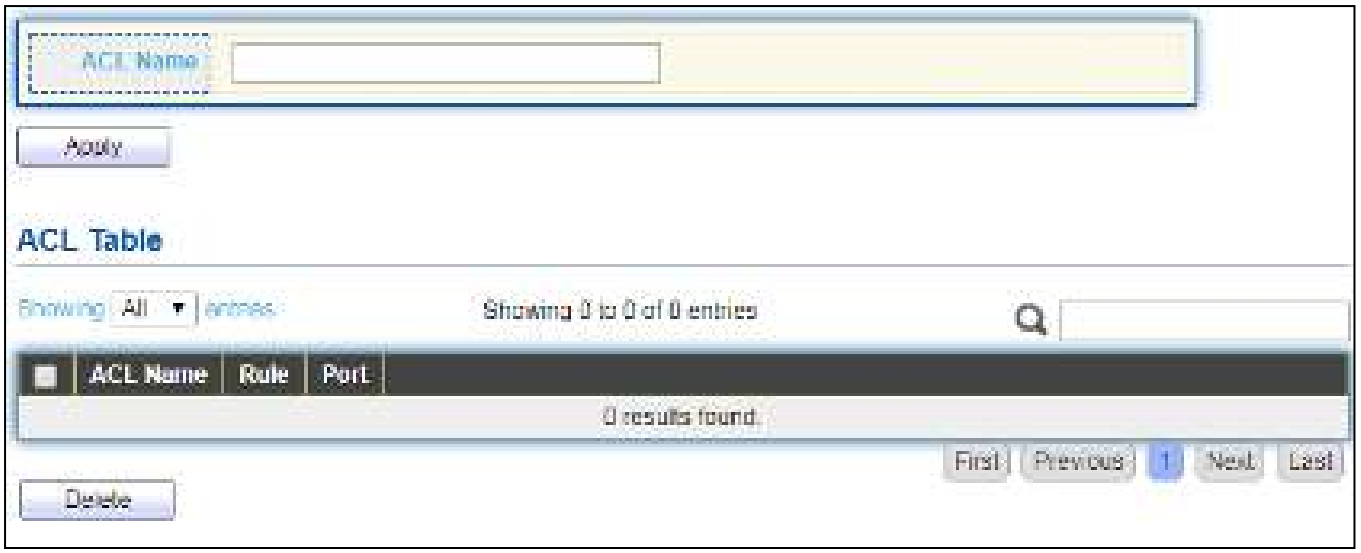


Figure 127 - ACL > IPv4 ACL

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

IV-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.

To display IPv4 ACE page, click **ACL > IPv4 ACE**.

Figure 128 - ACL > IPv4 ACE

Item	Description
ACL Name	Select the ACL name to which an ACE is being added.
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.
Destination IP	Display the destination IP address and mask of ACE.
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.

Click "**Add**" or "**Edit**" button to view the Add/Edit ACE menu.

Figure 129 - ACL > Add/Edit ACE

Item	Description
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 sequence). Only available on Add dialog.
Action	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	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.
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 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.
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.
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.
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.

IV-11-5 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.

To display ACL Binding page, click **ACL > ACL Binding**.

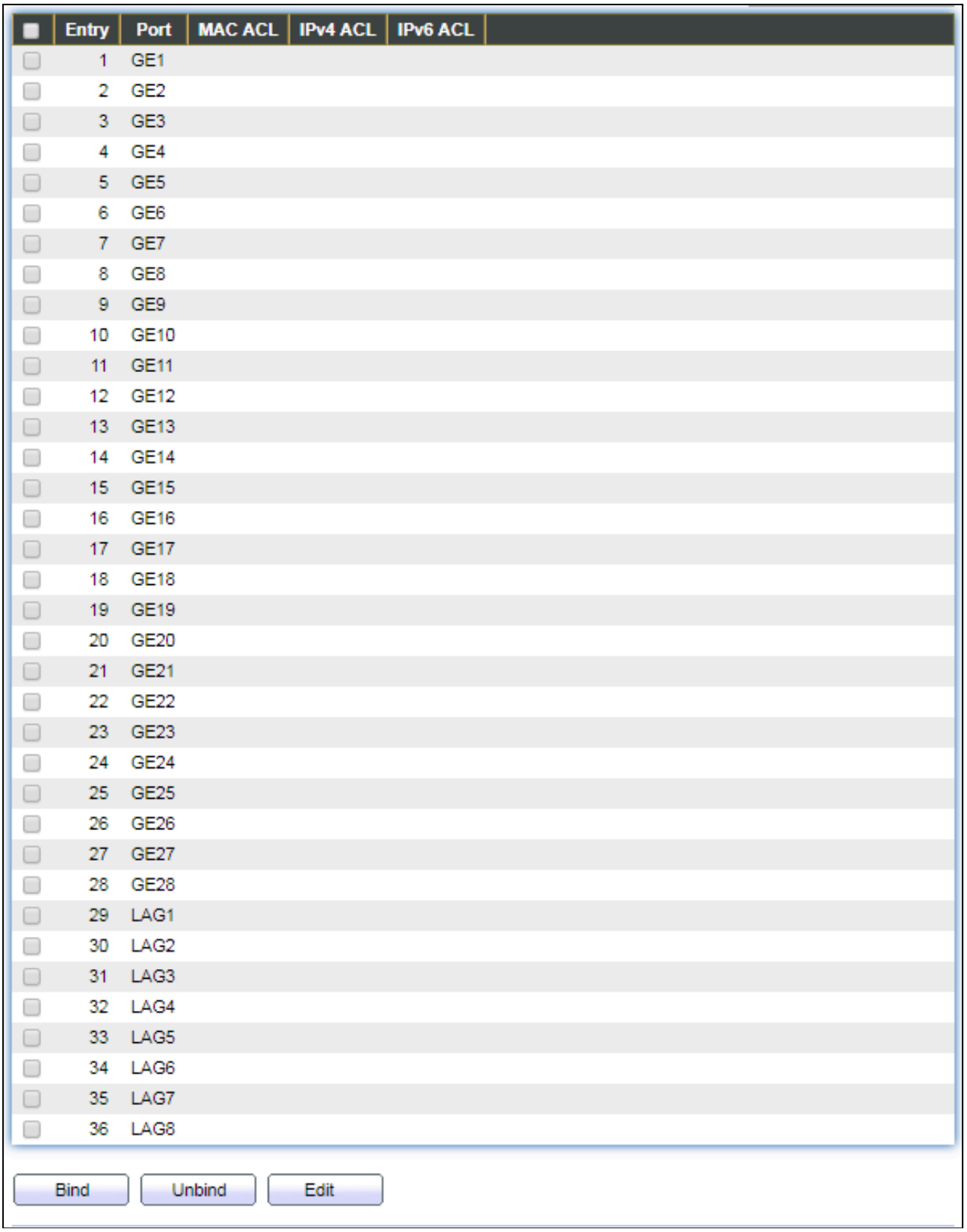


Figure 130 - ACL > ACL Binding

Item	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.

Click “**Edit**” button to view the Edit ACL Binding menu.

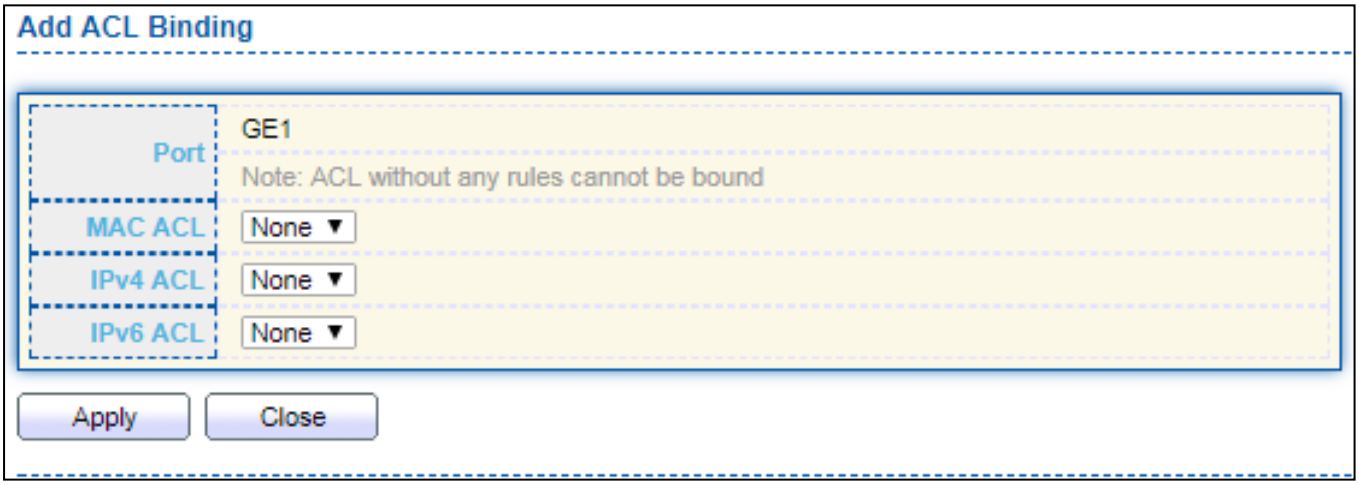


Figure 131 - ACL > Edit ACL Binding

Item	Description
Port	Display port entry ID.
MAC ACL	Select mac ACL name from list to bind.
IPv4 ACL	Select IPv4 ACL name from list to bind.
IPv6 ACL	Select IPv6 ACL name from list to bind.

IV-12 QoS

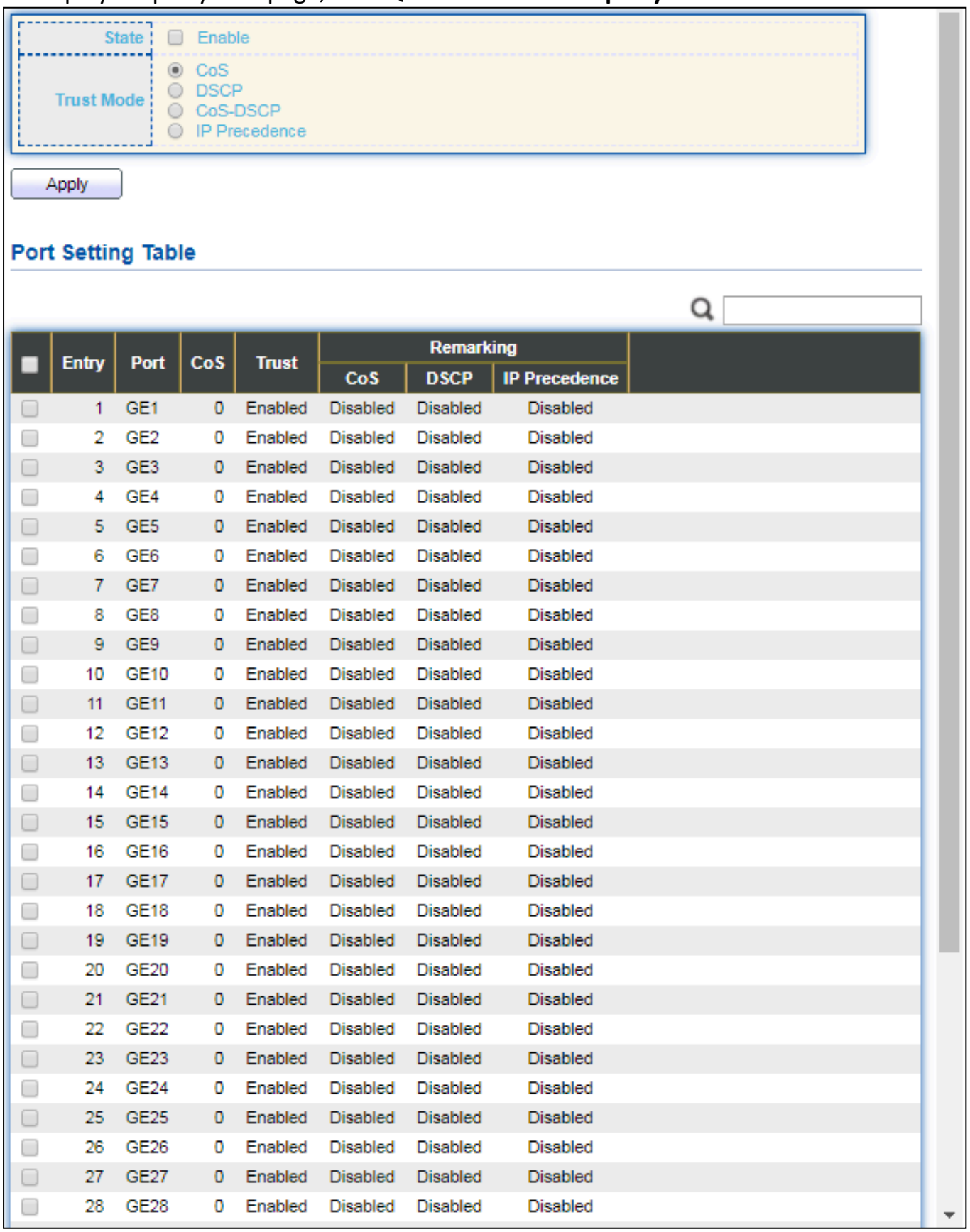
Use the QoS pages to configure settings for the switch QoS interface.

IV-12-1 General

Use the QoS general pages to configure settings for general purpose.

IV-12-1-1 Property

To display Property web page, click **QoS > General > Property**.



Entry	Port	CoS	Trust	Remarking		
				CoS	DSCP	IP Precedence
1	GE1	0	Enabled	Disabled	Disabled	Disabled
2	GE2	0	Enabled	Disabled	Disabled	Disabled
3	GE3	0	Enabled	Disabled	Disabled	Disabled
4	GE4	0	Enabled	Disabled	Disabled	Disabled
5	GE5	0	Enabled	Disabled	Disabled	Disabled
6	GE6	0	Enabled	Disabled	Disabled	Disabled
7	GE7	0	Enabled	Disabled	Disabled	Disabled
8	GE8	0	Enabled	Disabled	Disabled	Disabled
9	GE9	0	Enabled	Disabled	Disabled	Disabled
10	GE10	0	Enabled	Disabled	Disabled	Disabled
11	GE11	0	Enabled	Disabled	Disabled	Disabled
12	GE12	0	Enabled	Disabled	Disabled	Disabled
13	GE13	0	Enabled	Disabled	Disabled	Disabled
14	GE14	0	Enabled	Disabled	Disabled	Disabled
15	GE15	0	Enabled	Disabled	Disabled	Disabled
16	GE16	0	Enabled	Disabled	Disabled	Disabled
17	GE17	0	Enabled	Disabled	Disabled	Disabled
18	GE18	0	Enabled	Disabled	Disabled	Disabled
19	GE19	0	Enabled	Disabled	Disabled	Disabled
20	GE20	0	Enabled	Disabled	Disabled	Disabled
21	GE21	0	Enabled	Disabled	Disabled	Disabled
22	GE22	0	Enabled	Disabled	Disabled	Disabled
23	GE23	0	Enabled	Disabled	Disabled	Disabled
24	GE24	0	Enabled	Disabled	Disabled	Disabled
25	GE25	0	Enabled	Disabled	Disabled	Disabled
26	GE26	0	Enabled	Disabled	Disabled	Disabled
27	GE27	0	Enabled	Disabled	Disabled	Disabled
28	GE28	0	Enabled	Disabled	Disabled	Disabled

Figure 132 - QoS > General > Property

Item	Description
State	Set checkbox to enable/disable QoS.
Trust	Select QoS trust 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. ● CoS-DSCP: Uses the 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.
Port Setting Table	
Port	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)	Set checkbox to enable/disable port CoS remarking. ● Enabled: CoS remarking is enabled ● Disabled: CoS remarking is disabled
Remarking (IP Precedence)	Set checkbox to enable/disable port IP Precedence remarking. ● Enabled: DSCP remarking is enabled ● Disabled: DSCP remarking is disabled

Click "**Edit**" button to view the Edit Port Setting menu.

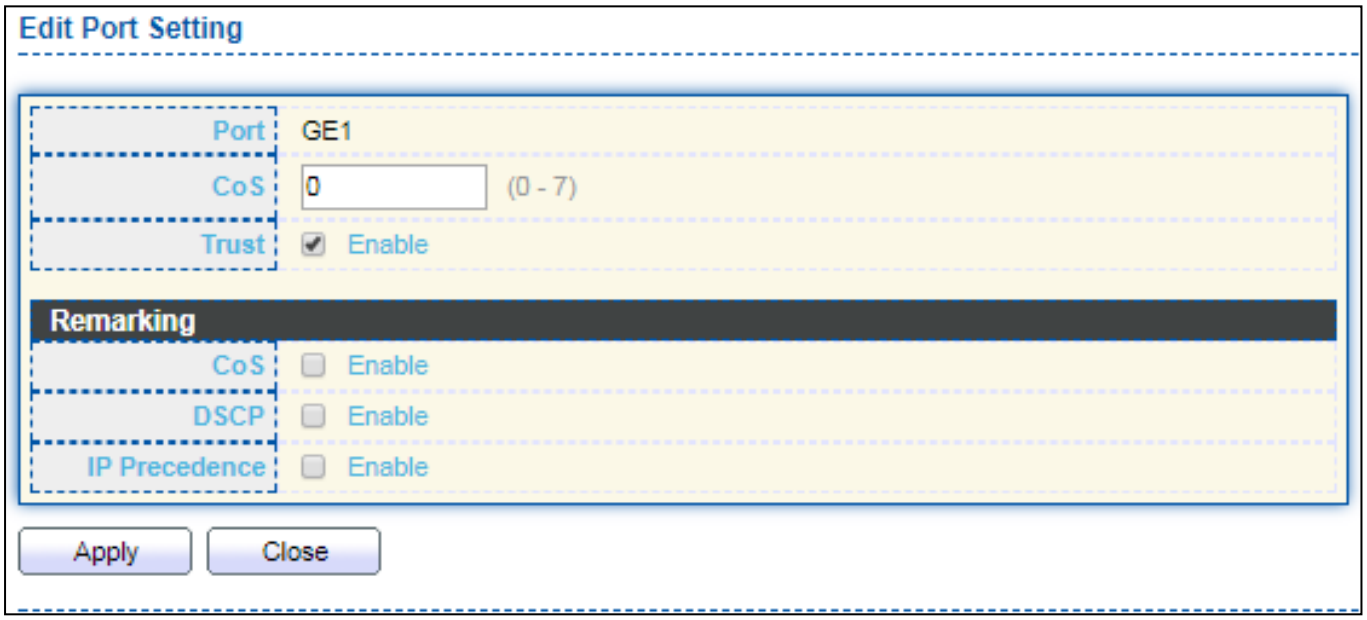


Figure 133 - Qos > General > Property

Item	Description
Port	Selected port list.
CoS	Set default CoS/802.1p priority value for the selected ports.
Trust	Set checkbox to enable/disable port trust state.
Remarking (CoS)	Set checkbox to enable/disable port CoS remarking.
Remarking (IP Precedence)	Set checkbox to enable/disable port IP Precedence remarking.

IV-12-1-2 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).

To display Queue Scheduling web page, click **QoS > General > Queue Scheduling**

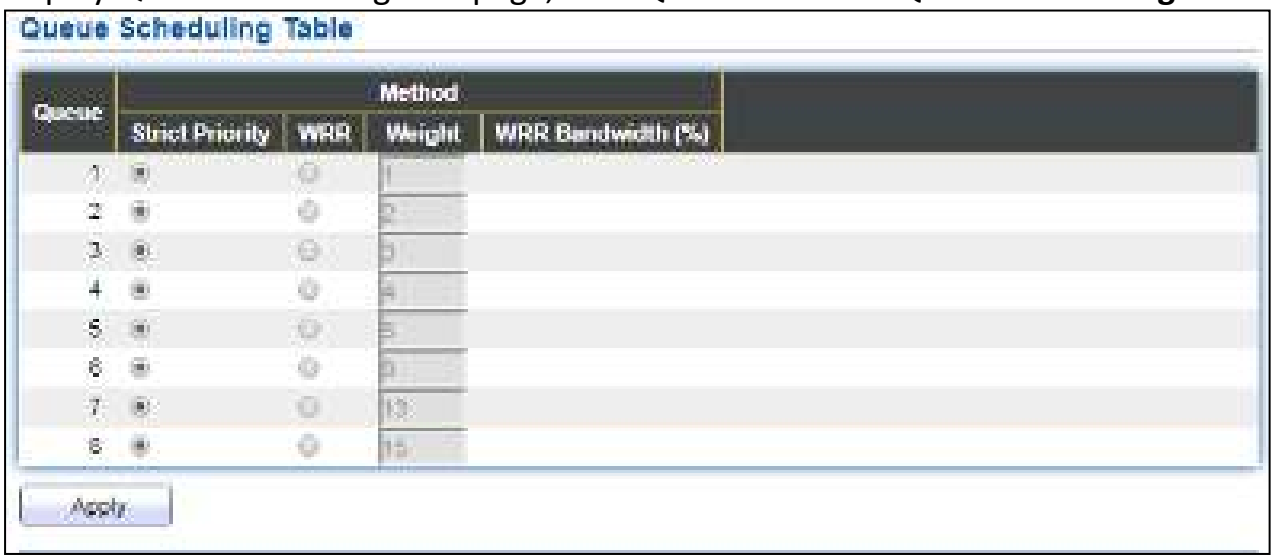


Figure 134 - QoS > General > Queue Scheduling

Item	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.

IV-12-1-3 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.

To display CoS Mapping web page, click **QoS > General > CoS Mapping**.

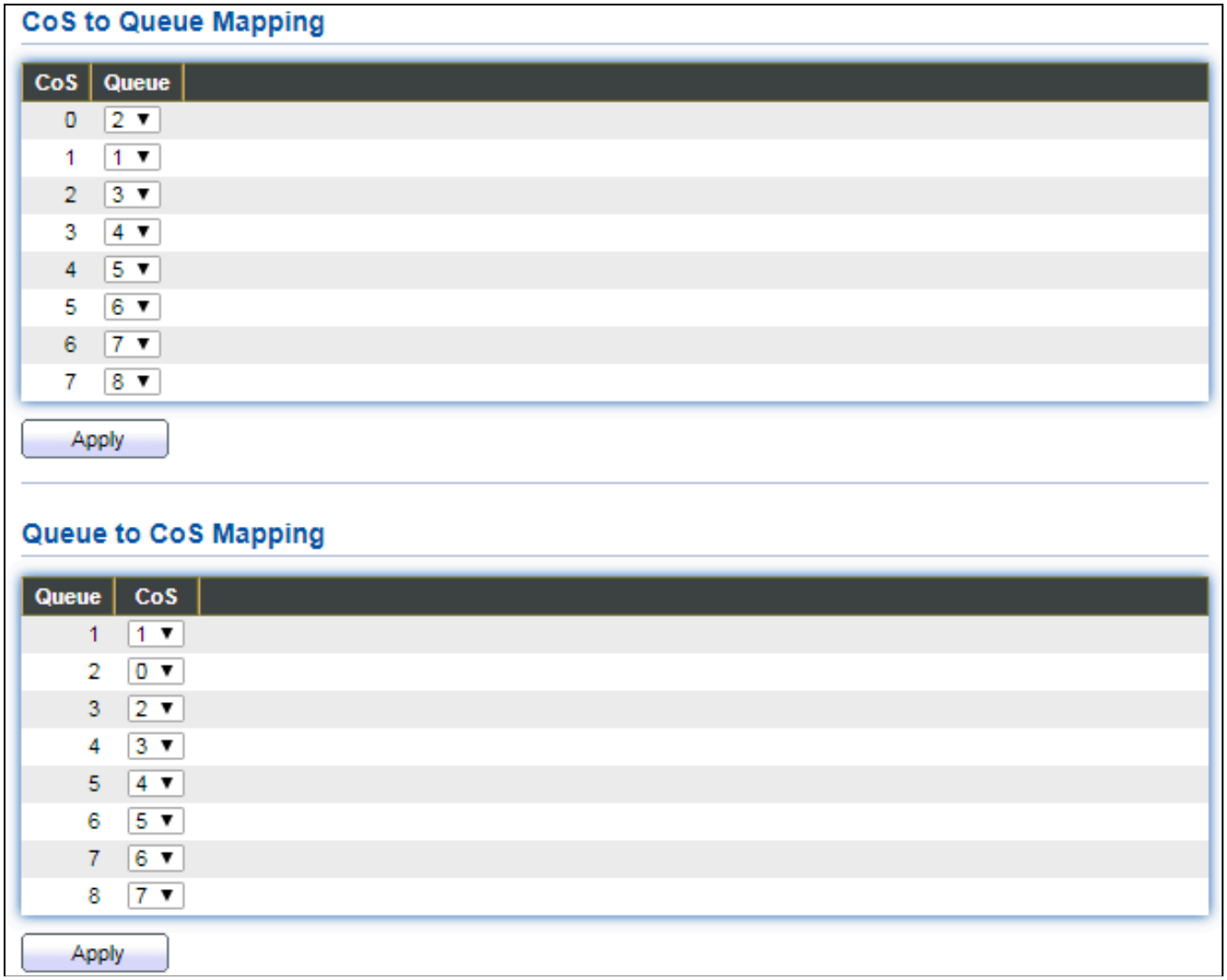


Figure 135 - QoS > General > Cos Mapping

Item	Description
CoS to Queue Mapping	
CoS	CoS value.
Queue	Select queue id for the CoS value.
Queue to CoS Mapping	
Queue	Queue ID
CoS	Select CoS value for the queue id.

IV-12-1-4 IP Precedence Mapping

This page allow user to configure IP Precedence to Queue mapping and Queue to IP Precedence mapping.

To display IP Precedence Mapping web page, click **QoS > General > IP Precedence Mapping**.

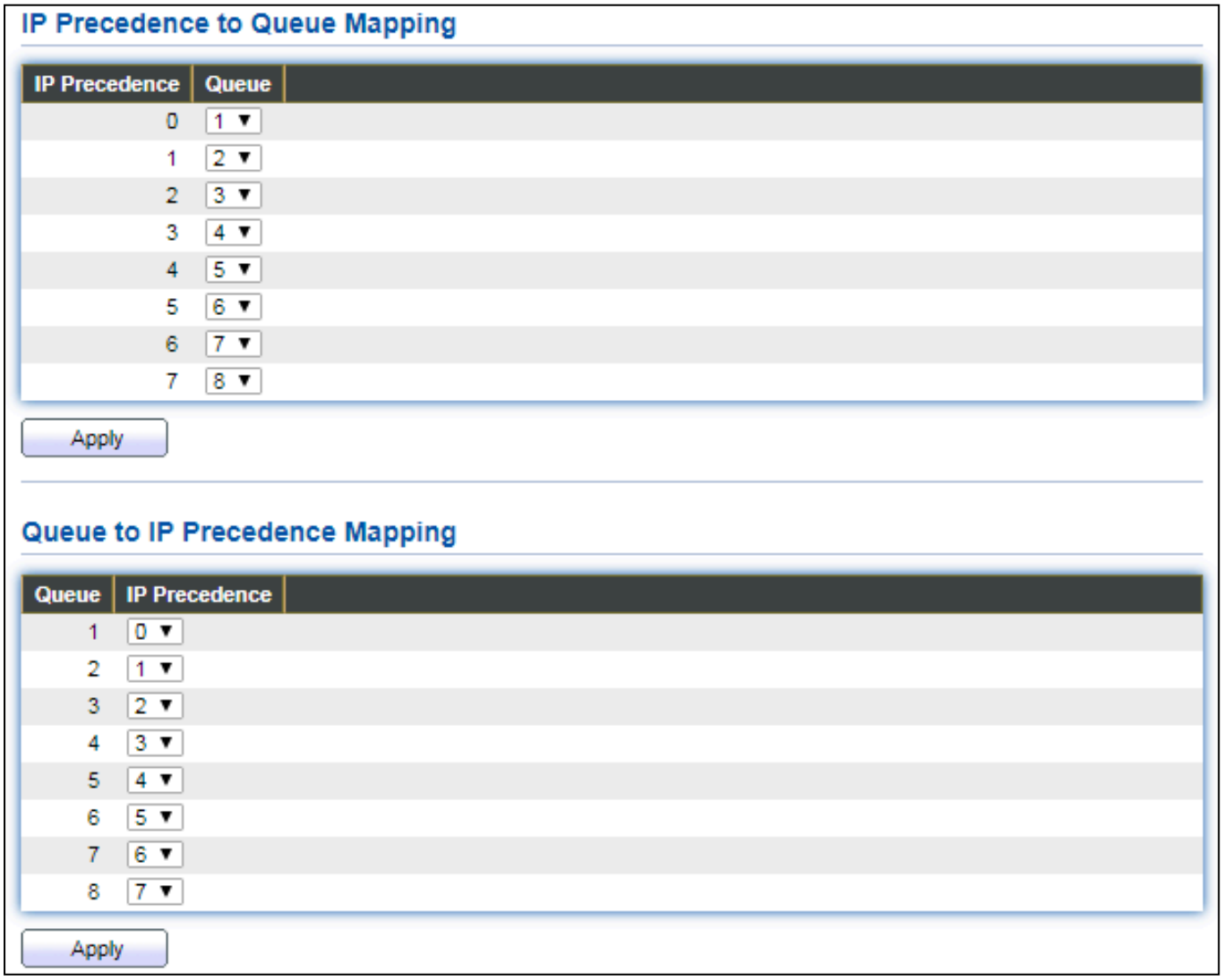


Figure 136 - QoS > General > IP Precdence Mapping

Item	Description
IP Precedence to Queue Mapping	
IP Precedence	IP Precedence value.
Queue	Queue value which IP Precedence is mapped.
Queue to IP Precedence Mapping	
Queue	Queue ID.
IP Precedence	IP Precedence value which queue is mapped.

IV-12-2 Rate Limit

Use the Rate Limit pages to define values that determine how much traffic the switch can receive and send on specific port or queue.

IV-12-2-1 Ingress/Egress Port

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.

To display Ingress / Egress Port web page, click **QoS > Rate Limit > Ingress / Egress Port**.

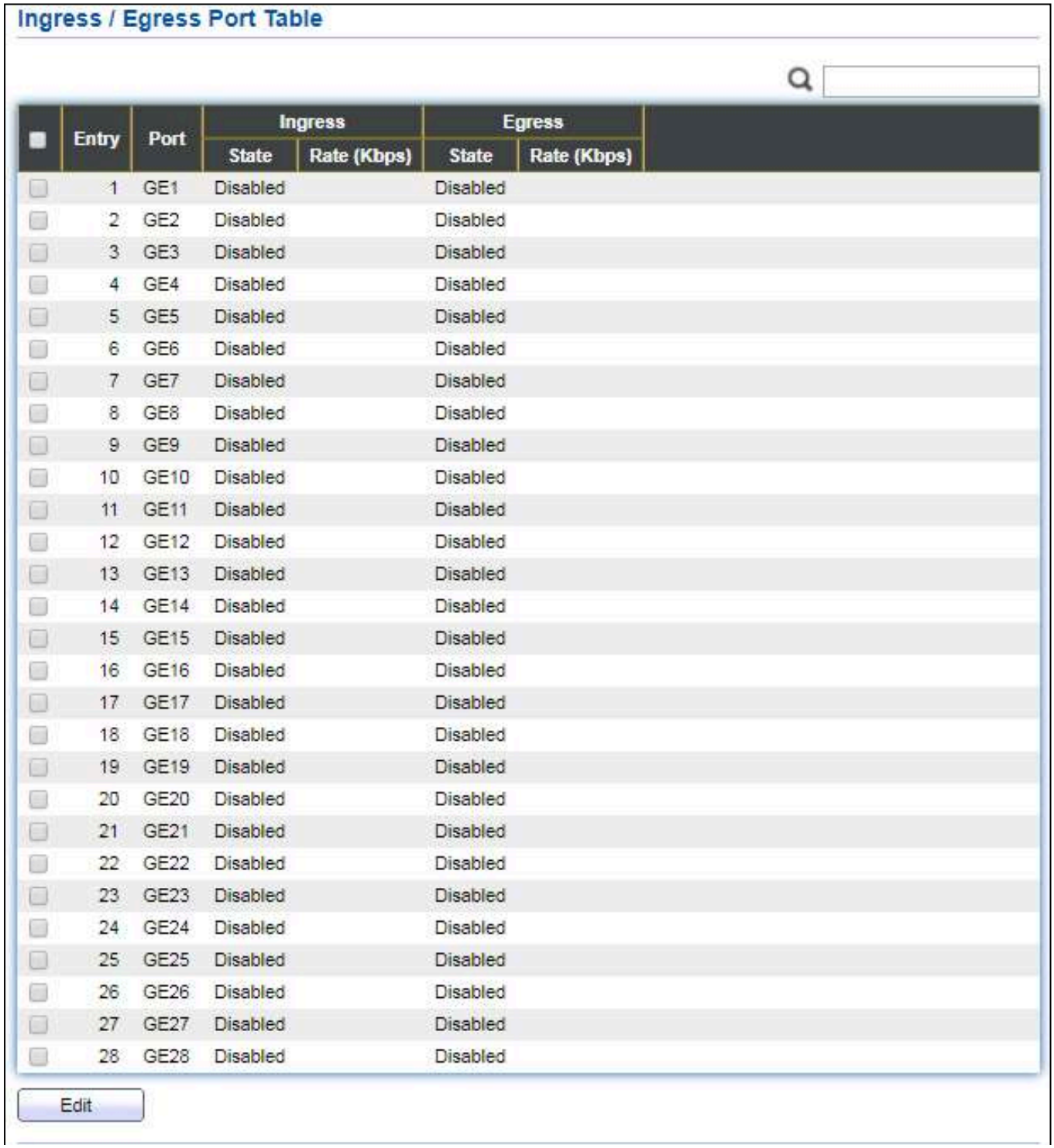


Figure 137 - QoS > Rate Limit > Ingress / Egress Port

Item	Description
Port	Port name.
Ingress (State)	Port ingress rate limit state ● Enabled: Ingress rate limit is enabled ● Disabled: Ingress rate limit is disabled
Ingress (Rate)	Port ingress rate limit value if ingress rate state is enabled.
IP Precedence	IP Precedence value which queue is mapped.
Egress (State)	Port egress rate limit state

	● Enabled: Egress rate limit is enabled ● Disabled: Egress rate limit is disabled
Egress (Rate)	Port egress rate limit value if egress rate state is enabled.

Click "**Edit**" button to view the Ingress / Egress Port menu.

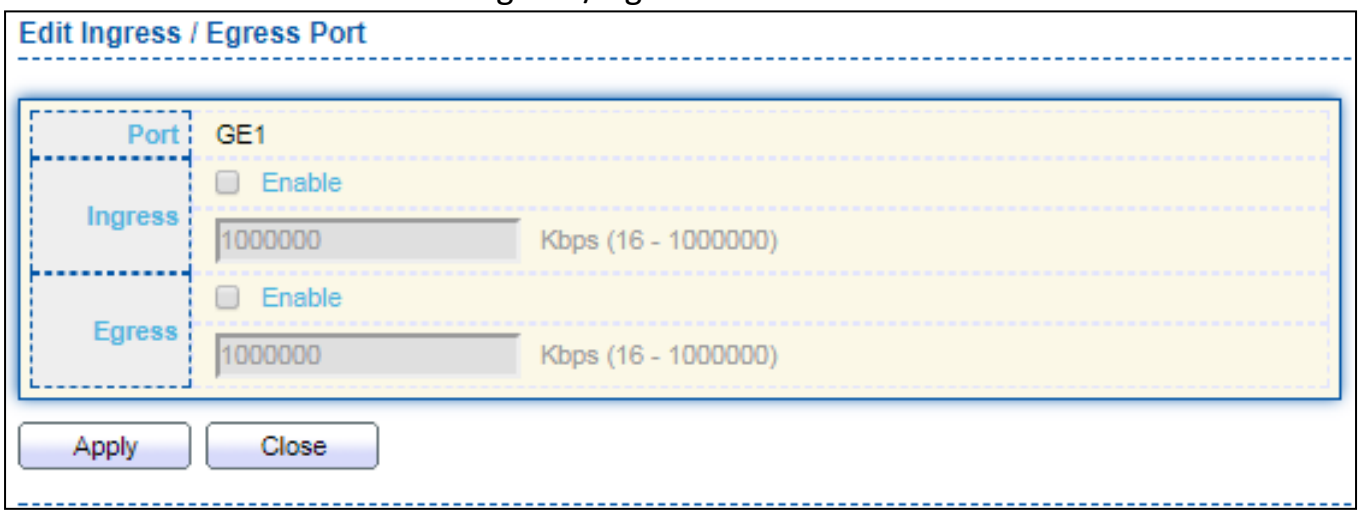


Figure 138 - QoS > Rate Limit > Ingress / Egress Port

Item	Description
Port	Select port list.
Ingress	Set checkbox to enable/disable ingress rate limit. If ingress rate limit is enabled, rate limit value need to be assigned.
Egress	Set checkbox to enable/disable egress rate limit. If egress rate limit is enabled, rate limit value need to be assigned.

IV-13 Diagnostics

Use the Diagnostics pages to configure settings for the switch diagnostics feature or operating diagnostic utilities.

IV-13-1 Logging

IV-13-1-1 Property

To enable/disable the logging service, click **Diagnostic > Logging > Property**.

Figure 139 - Diagnostics > Logging > Property

Item	Description
State	Enable/Disable the global logging services. 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.
Console Logging	
State	Enable/Disable the console logging service
Minimum Severity	The minimum severity for the console logging.
RAM Logging	
State	Enable/Disable the RAM logging service.
Minimum Severity	The minimum severity for the RAM logging.
Flash Logging	

State	Enable/Disable the flash logging service.
Minimum Severity	The minimum severity for the flash loggin.

IV-13-1-2 Remote Server

To configure the remote logging server, click **Diagnostic > Logging > Remote Server**.

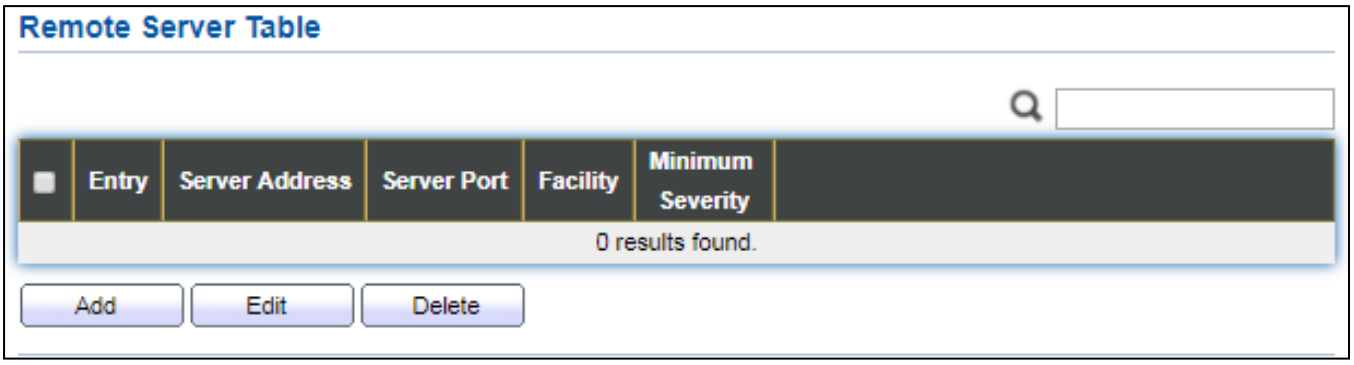


Figure 140 - Diagnostics > Logging > Remote Server

Item	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 local7.
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.

IV-13-2 Mirroring

To display Port Mirroring web page, click **Diagnostics > Mirroring**.

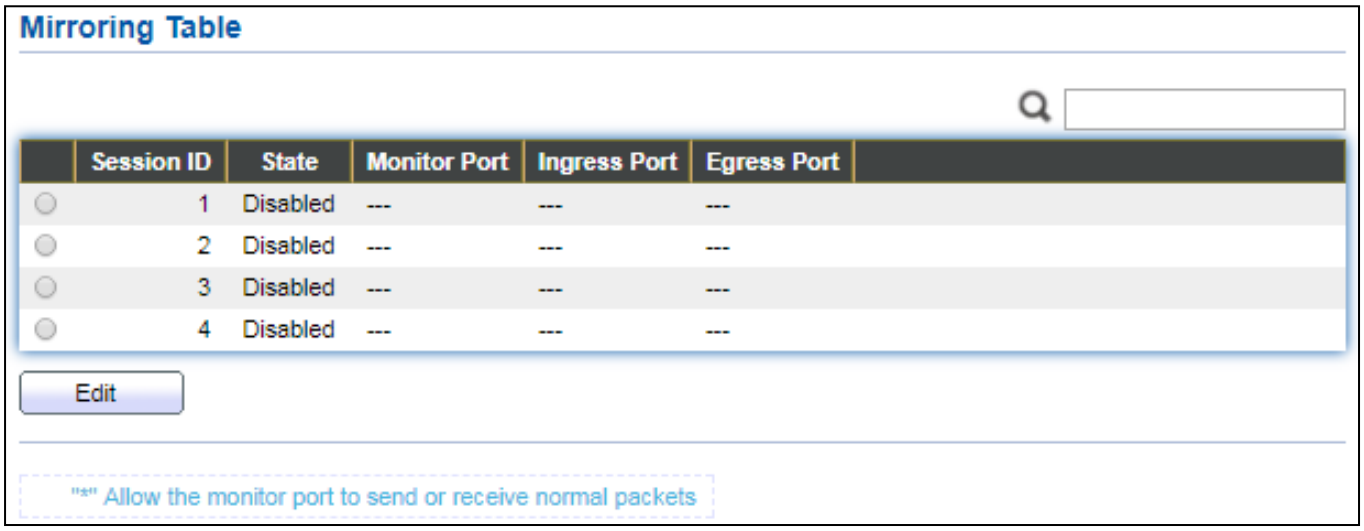


Figure 141 - Diagnostics > Mirroring

Item	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 port	Select mirror session source tx ports.

Click "**Edit**" button to view the Edit Mirroring menu.

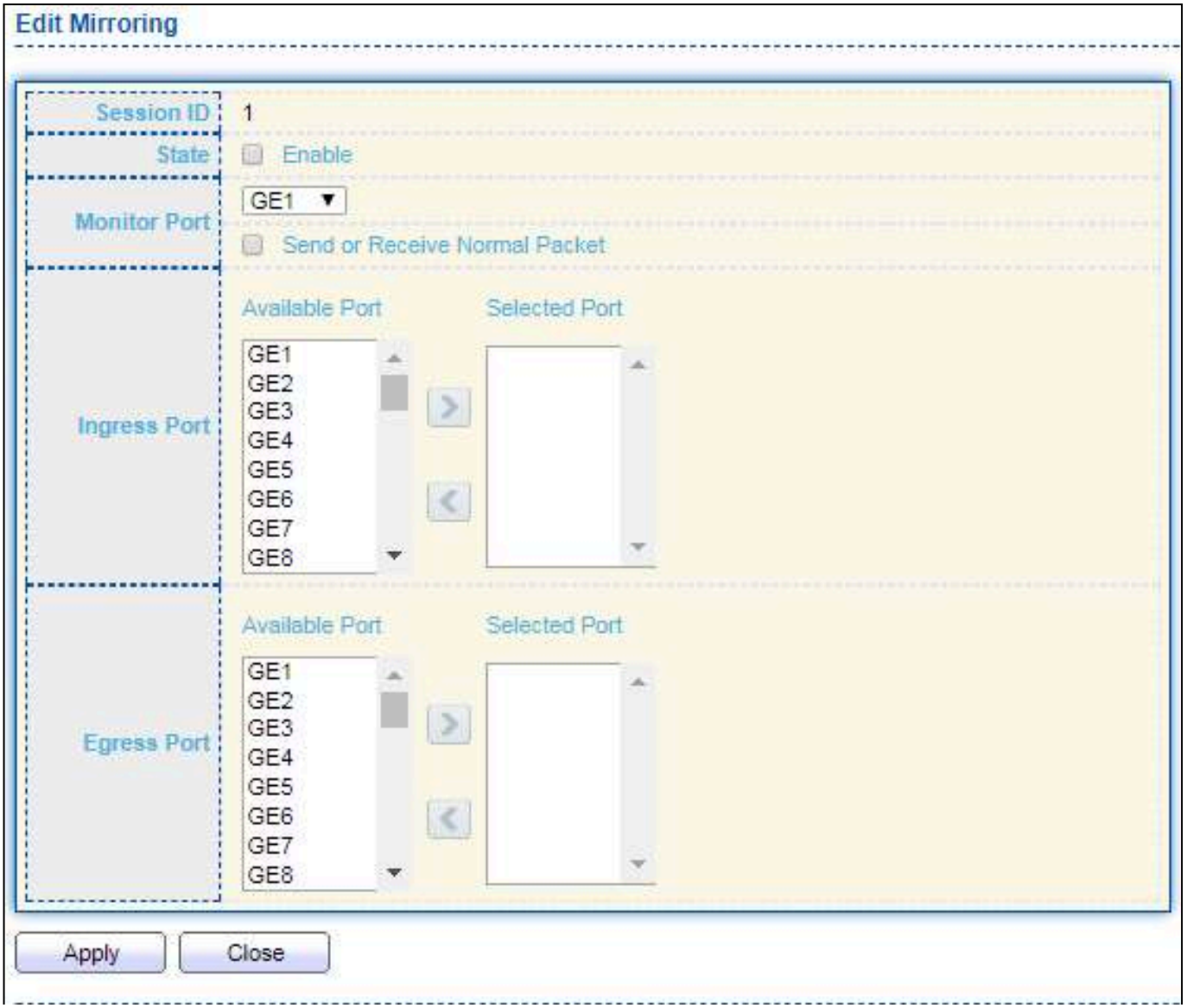


Figure 142 - Diagnostics > Mirroring > Edit Mirroring

Item	Description
Session ID	Selected 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 port	Select mirror session source tx ports.

IV-13-3 Ping

For the ping functionality, click **Diagnostic > Ping**.

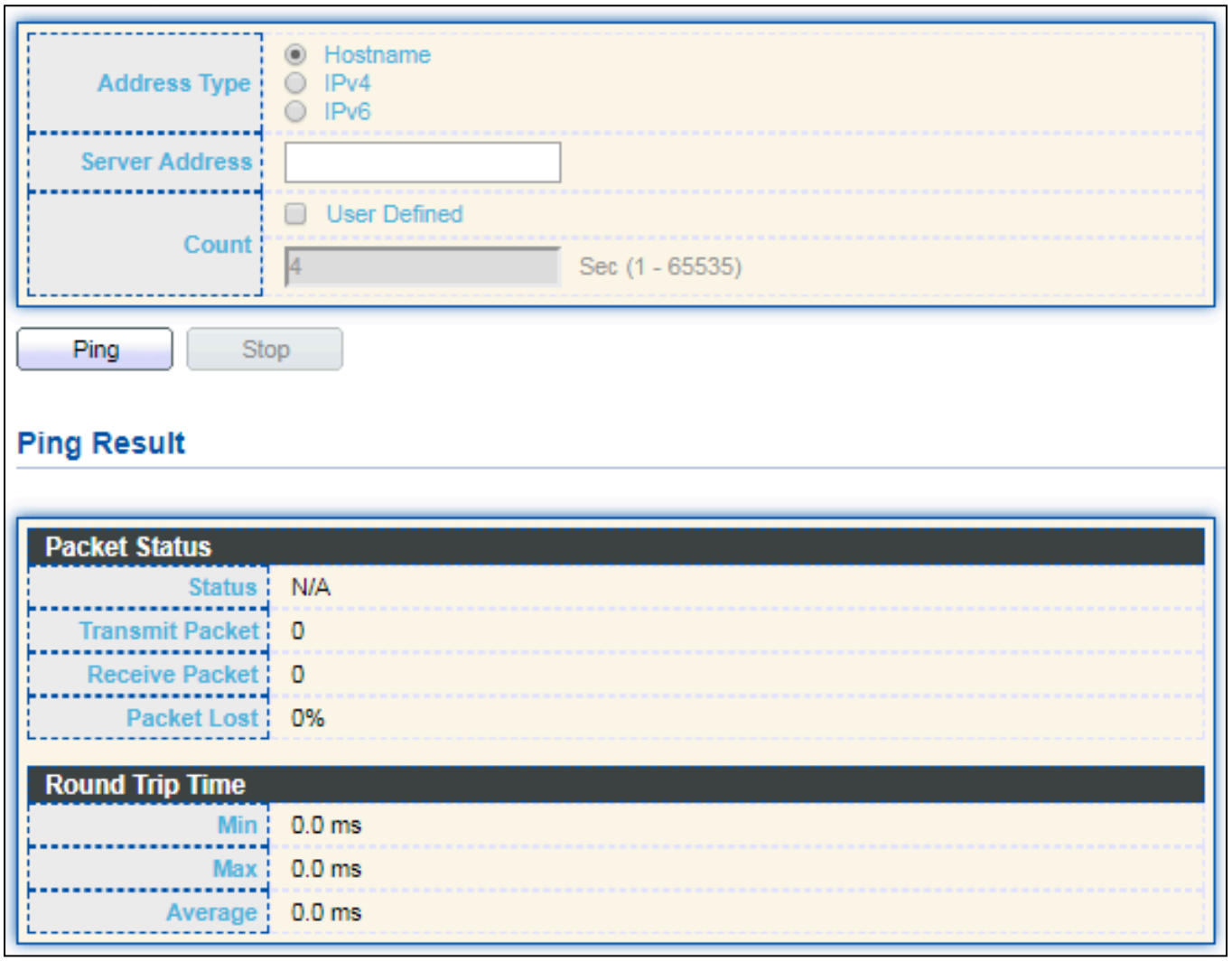


Figure 143 - Diagnostics > Ping

Item	Description
Address Type	Specify the address type to “Hostname”or “IPv4”.
Server Address	Specify the Hostname/IPv4 address for the remote logging server.
Count	Specify the numbers of each ICMP ping request.

IV-13-4 Traceroute

For trace route functionality, click **Diagnostic > Traceroute**.

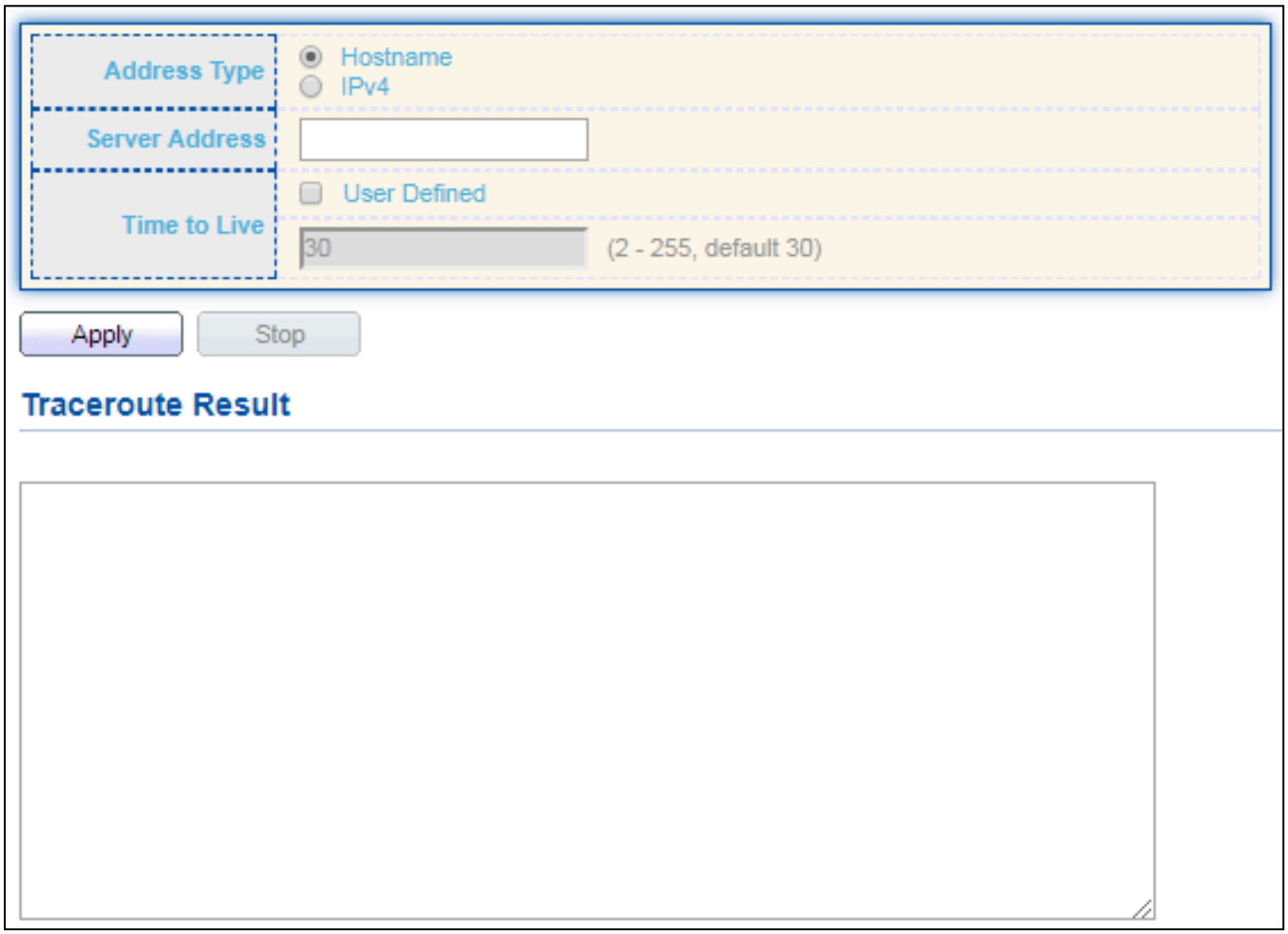


Figure 144 - Diagnostics > Traceroute

Item	Description
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	Specify the max hops of hosts for traceroute.

IV-13-5 Copper Test

For copper length diagnostic, click **Diagnostic > Copper Test**.

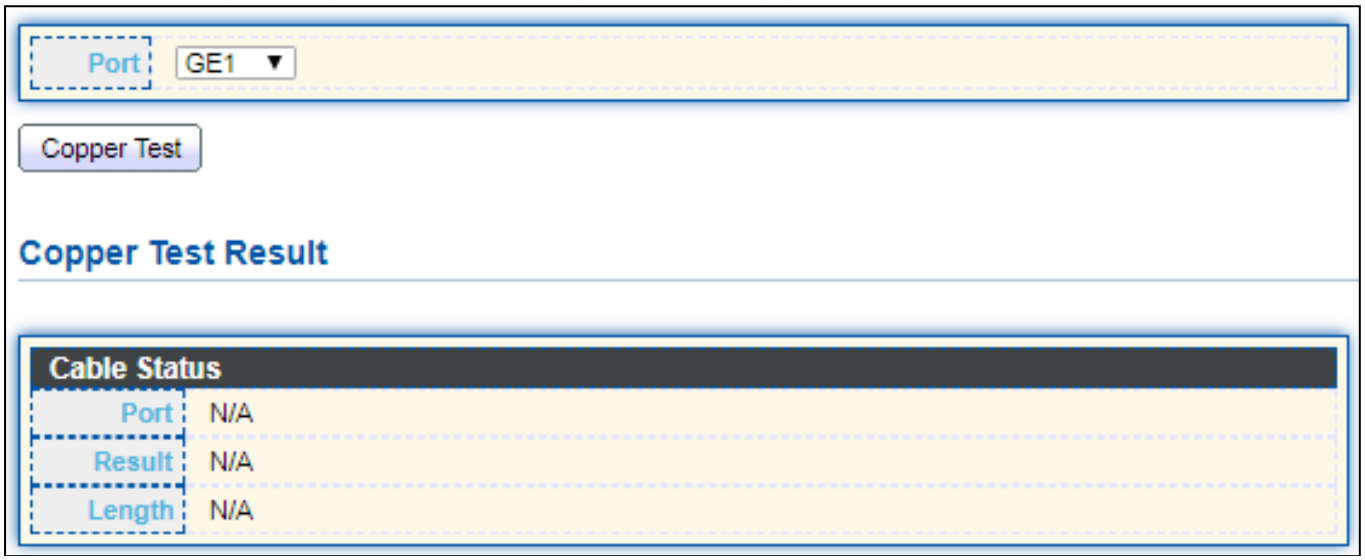


Figure 145 - Diagnostics > Logging>Copper Test

Item	Description
Port	Specify the interface for the copper test.
Copper Test Result	
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.
Length	Distance in meter from the port to the location on the cable where the fault was discovered.

IV-13-6 Fiber Module

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.

To display the Optical Module Diagnostic page, click **Diagnostic > Fiber Module**.

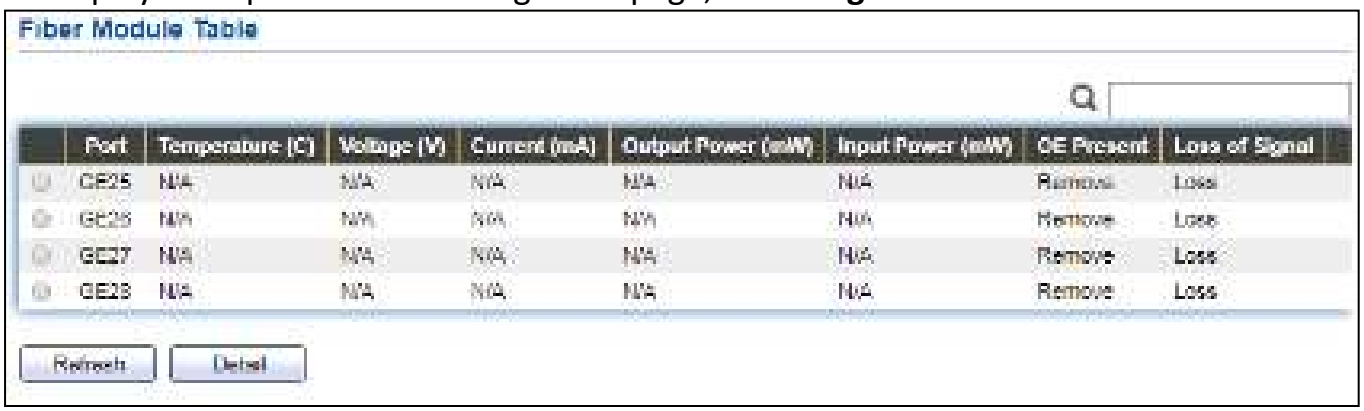


Figure 146 - Diagnostics > Logging>Fiber Module

Item	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 milliwatts.
Input Power	Measured RX received power in milliwatts.
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 "**Detail**" button to view the Fiber Module Status menu

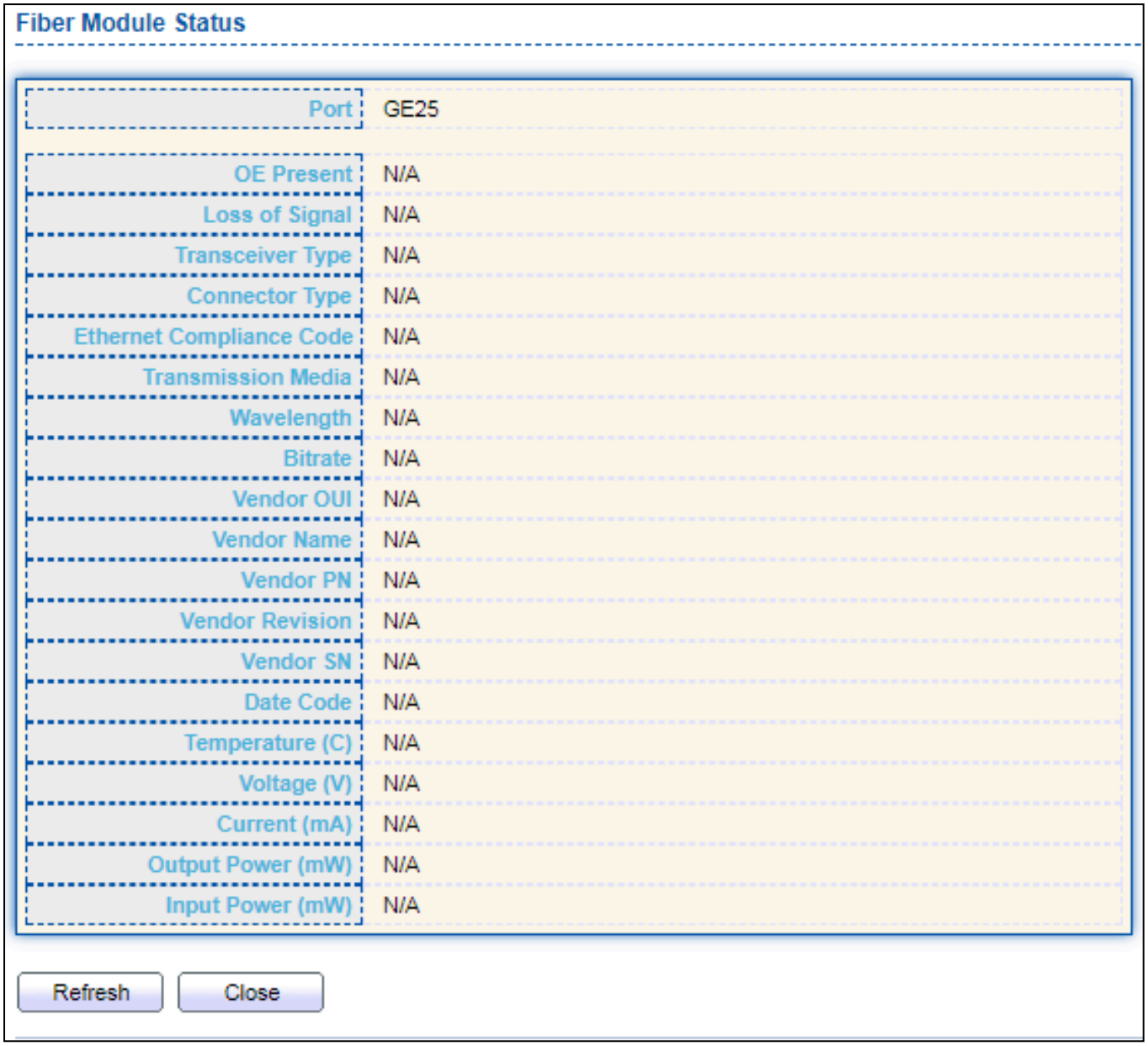


Figure 147 - Diagnostics > Logging>Fiber Module>Fiber Module Status

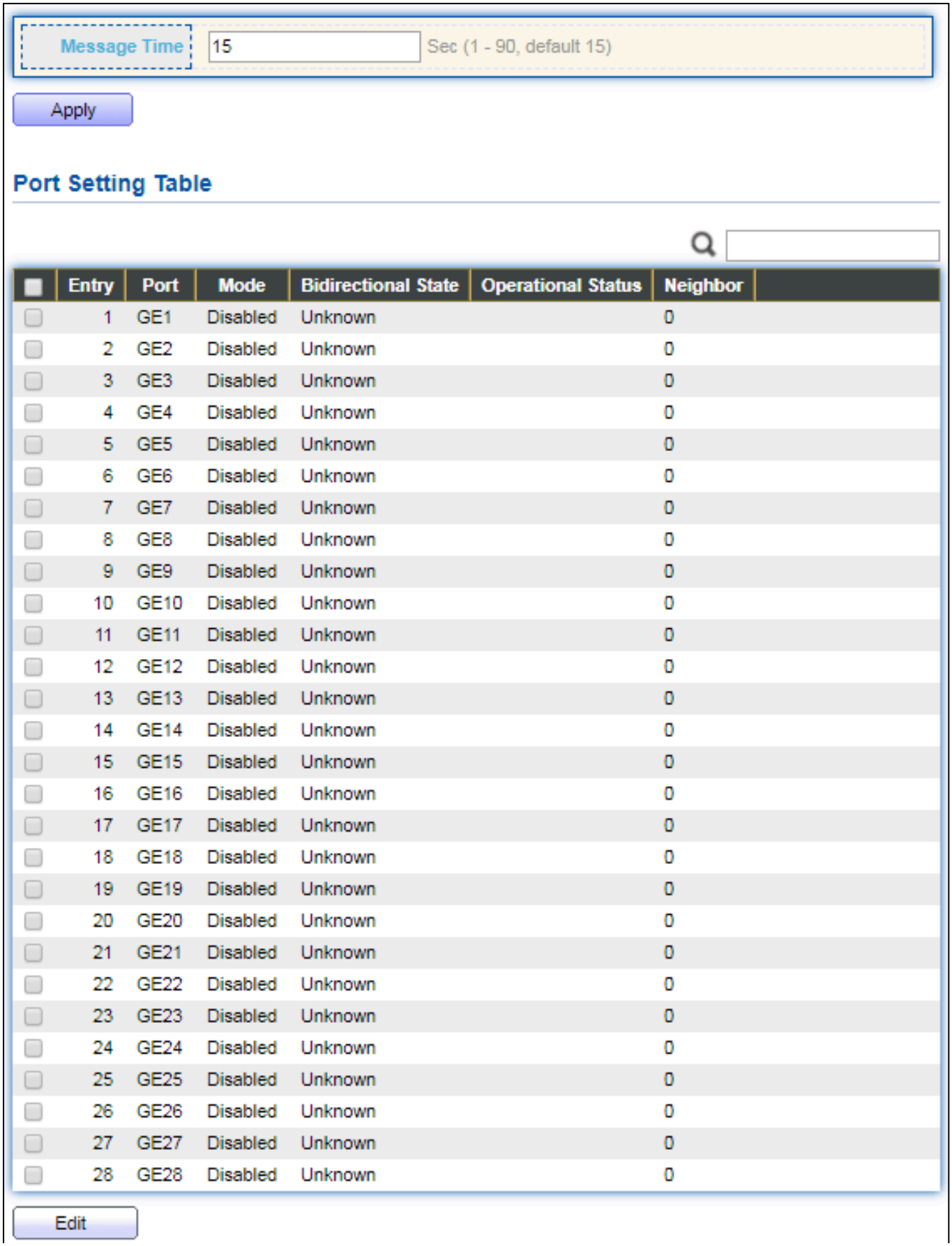
IV-13-7 UDLD

Use the UDLD pages to configure settings of UDLD function.

IV-13-7-1 Property

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

To display Property page, click **Diagnostics > UDLD > Property**.



Entry	Port	Mode	Bidirectional State	Operational Status	Neighbor
1	GE1	Disabled	Unknown		0
2	GE2	Disabled	Unknown		0
3	GE3	Disabled	Unknown		0
4	GE4	Disabled	Unknown		0
5	GE5	Disabled	Unknown		0
6	GE6	Disabled	Unknown		0
7	GE7	Disabled	Unknown		0
8	GE8	Disabled	Unknown		0
9	GE9	Disabled	Unknown		0
10	GE10	Disabled	Unknown		0
11	GE11	Disabled	Unknown		0
12	GE12	Disabled	Unknown		0
13	GE13	Disabled	Unknown		0
14	GE14	Disabled	Unknown		0
15	GE15	Disabled	Unknown		0
16	GE16	Disabled	Unknown		0
17	GE17	Disabled	Unknown		0
18	GE18	Disabled	Unknown		0
19	GE19	Disabled	Unknown		0
20	GE20	Disabled	Unknown		0
21	GE21	Disabled	Unknown		0
22	GE22	Disabled	Unknown		0
23	GE23	Disabled	Unknown		0
24	GE24	Disabled	Unknown		0
25	GE25	Disabled	Unknown		0
26	GE26	Disabled	Unknown		0
27	GE27	Disabled	Unknown		0
28	GE28	Disabled	Unknown		0

Figure 148 - Diagnostics > UDLD>Property

Item	Description
Message Time	Input the interval for sending message. Range is 1 -90 seconds.
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.

Click "**Edit**" button to view the Fiber Module Status menu

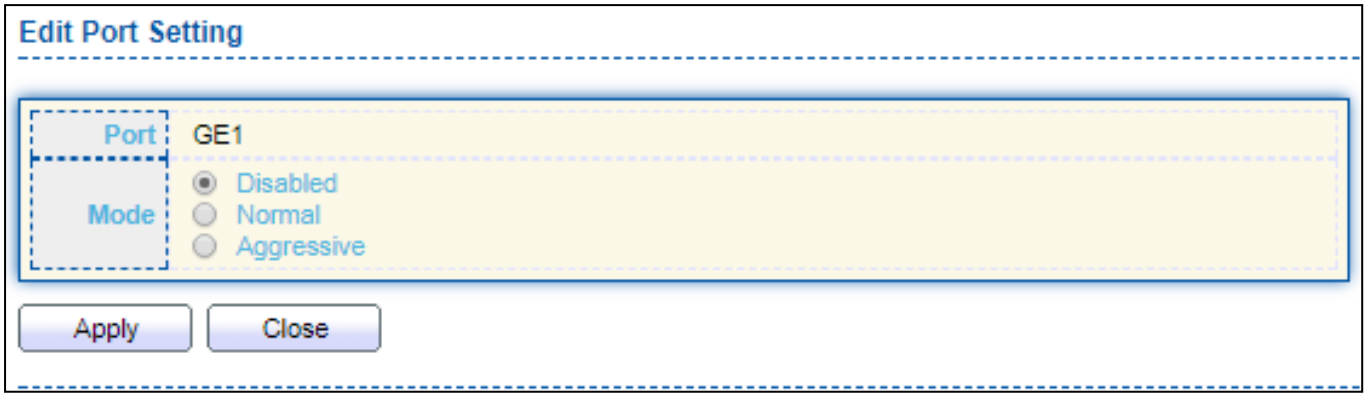


Figure 149 - Diagnostics > UDLD>Property>Edit

Item	Description
Port	Display selected port to be edited.
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.

IV-13-7-2 Neighbor

To display Neighbor page, click **Diagnostics > UDLD > Neighbor**

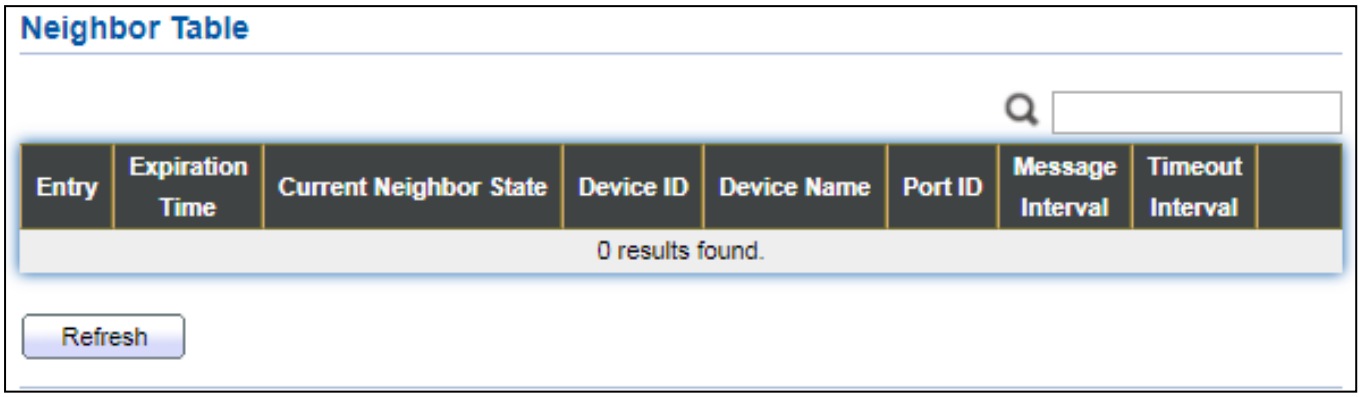


Figure 150 - Diagnostics > UDLD> Neigbor

Item	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.

IV-14 Management

Use the Management pages to configure settings for the switch management features.

IV-14-1 User Account

The default username/password is admin/admin. And default account is not able to be deleted.
Use this page to add additional users that are permitted to manage the switch or to change the passwords of existing users.

To display User Account web page, click **Management > User Account**.

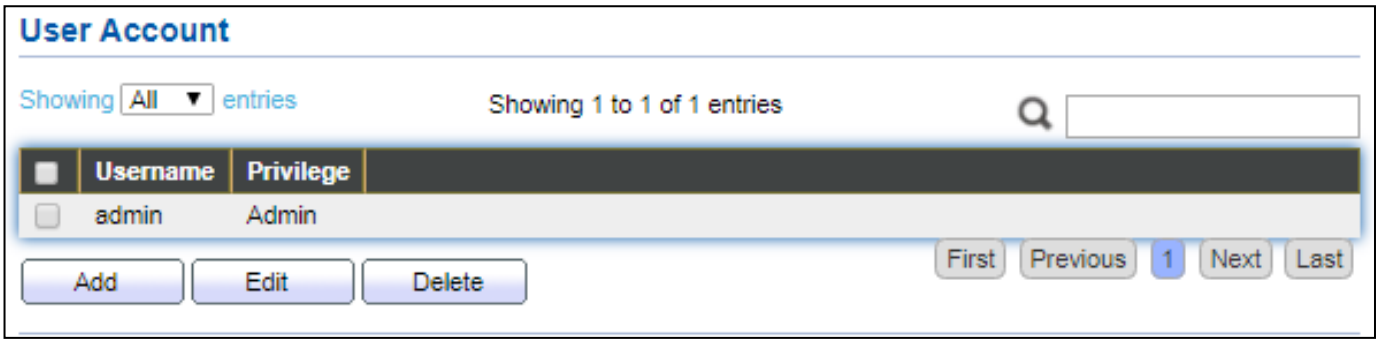


Figure 151 - Management > User Account

Item	Description
Username	User name of the account.
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 "**Add**" or "**Edit**" button to view the Add/Edit User Account menu.

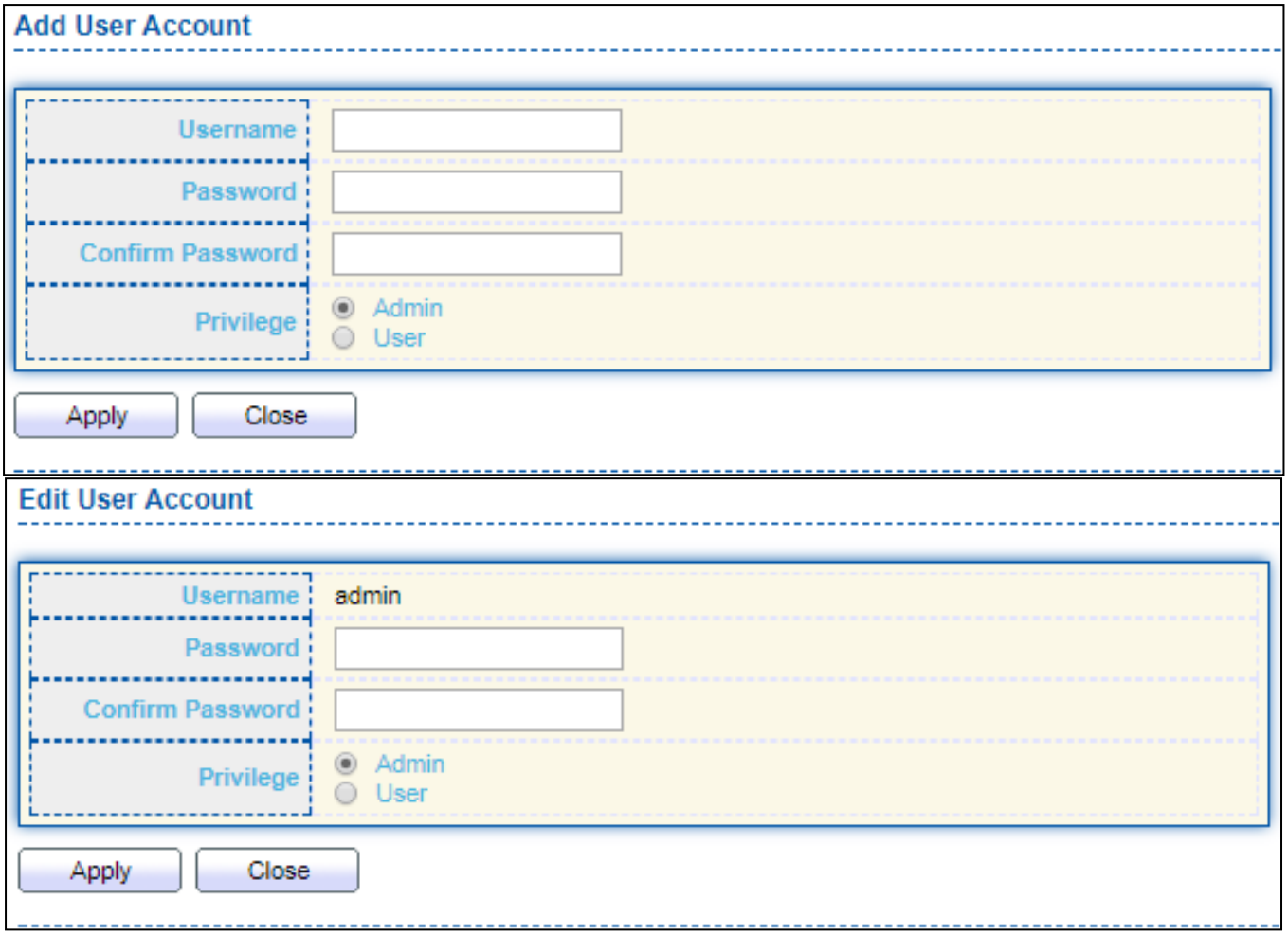


Figure 152 - Management > User Account > Add/Edit User Account

Item	Description
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.

IV-14-2 Fireware

IV-14-2-1 Upgrade / Backup

This page allow user to upgrade or backup firmware image through HTTP or TFTP server.

To display firmware upgrade or backup web page, click **Management > Firmware > Upgrade/Backup**.

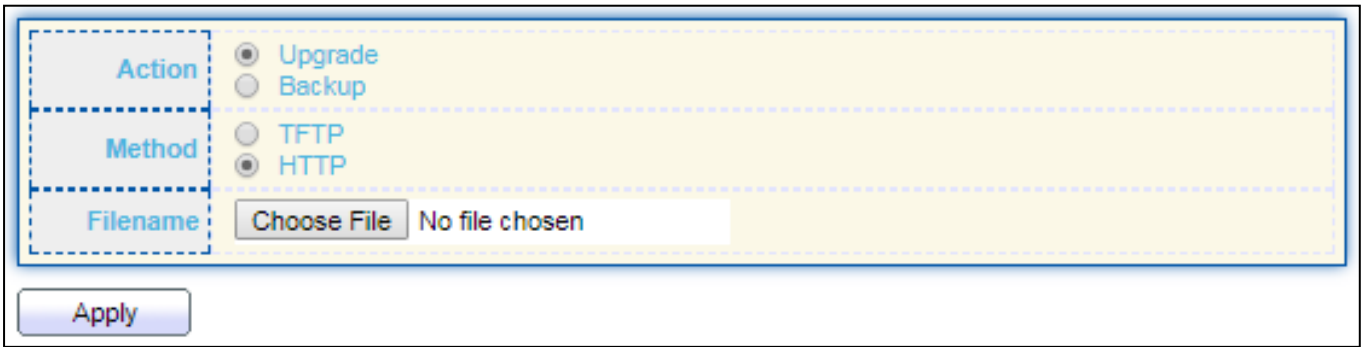


Figure 153 - Management > Fireware > Upgrate/Backup

Item	Description
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.

To display firmware upgrade or backup web page, click **Management > Firmware > Upgrade/Backup**.

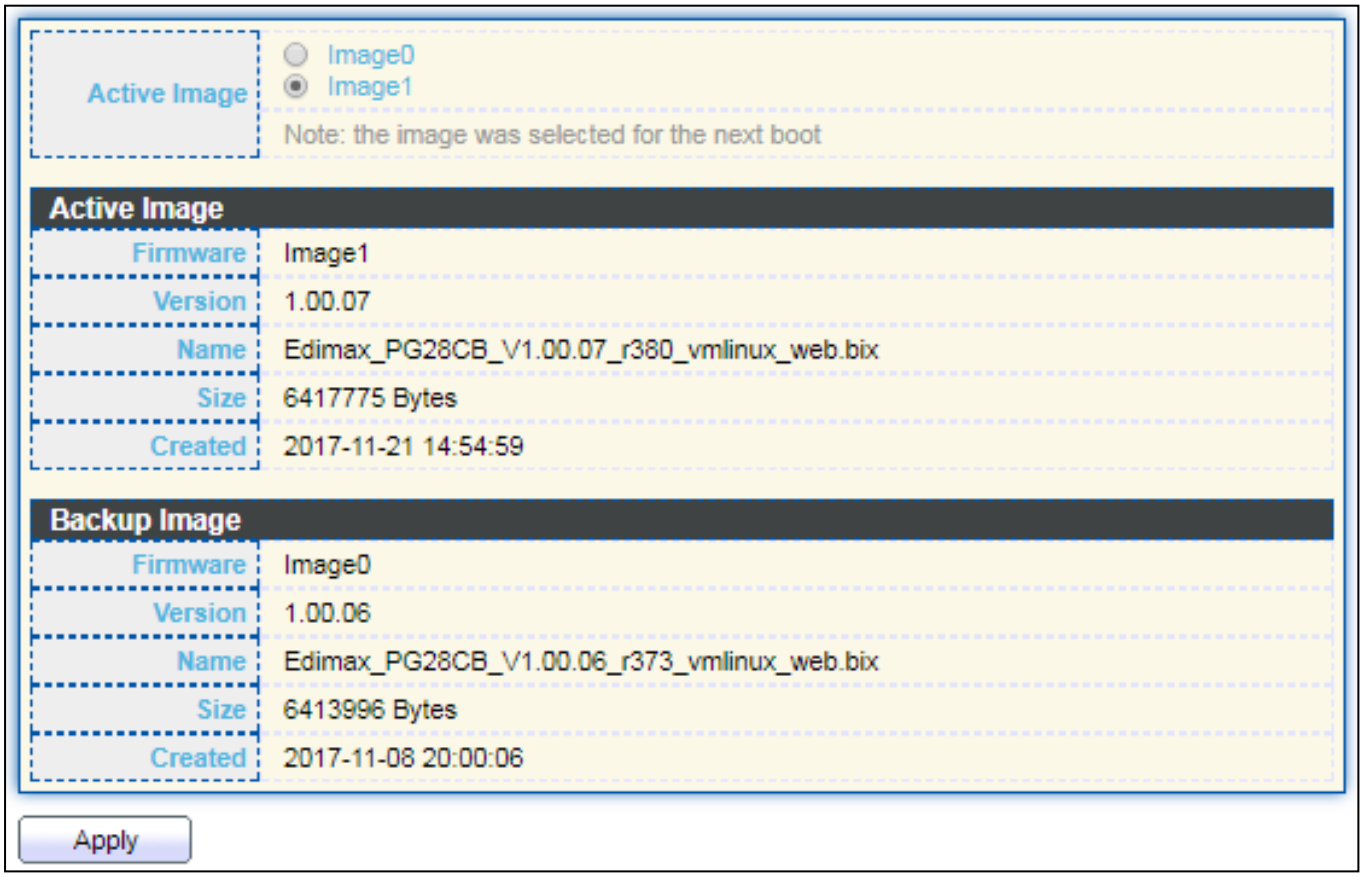


Figure 154 - Management > Fireware > Upgrate/Backup

Item	Description
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.
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

To display firmware upgrade or backup web page, click **Management > Firmware > Upgrade/Backup**.

Figure 155 - Management > Fireware > Upgrate/Backup

Item	Description
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

To display the Fireware Upgrate/Backup web page, click **Management > Fireware > Upgrate/Backup**.

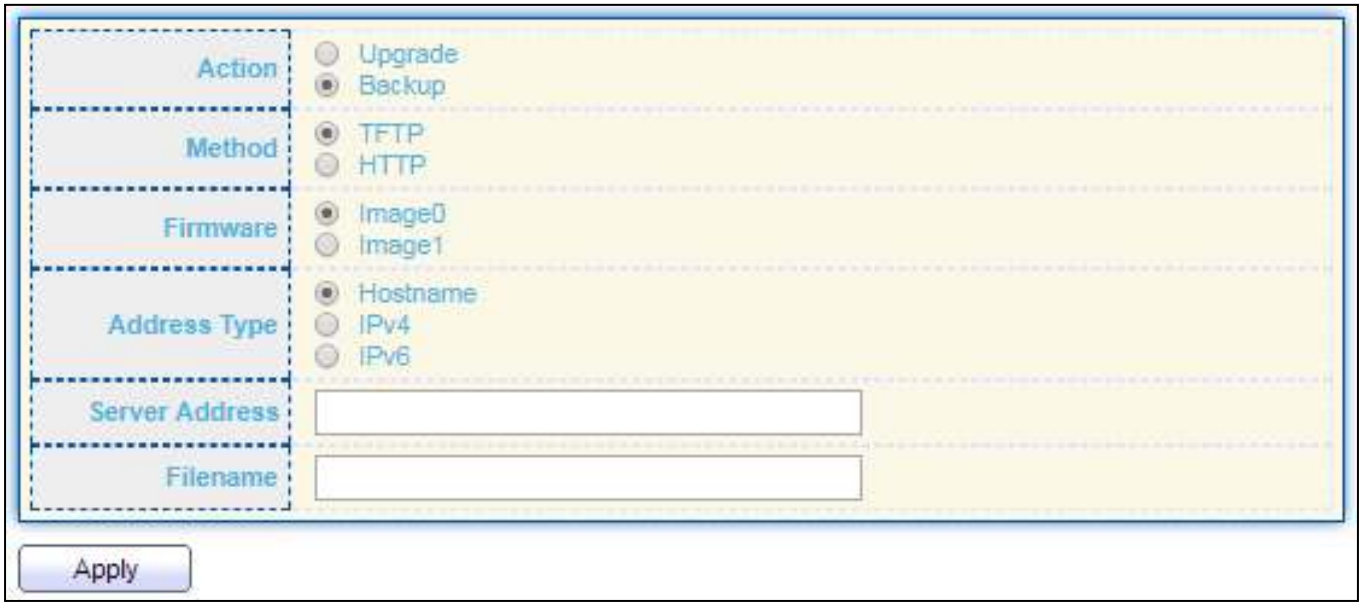


Figure 156 - Management > Fireware >Upgrate/Backup

Item	Description
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 address.
Filename	File name saved on remote TFTP server.

IV-14-2-2 Active Image

This page allow user to select firmware image on next booting and show firmware information on both flash partitions.

To display the Active Image web page, click **Management > Firmware > Active Image**.

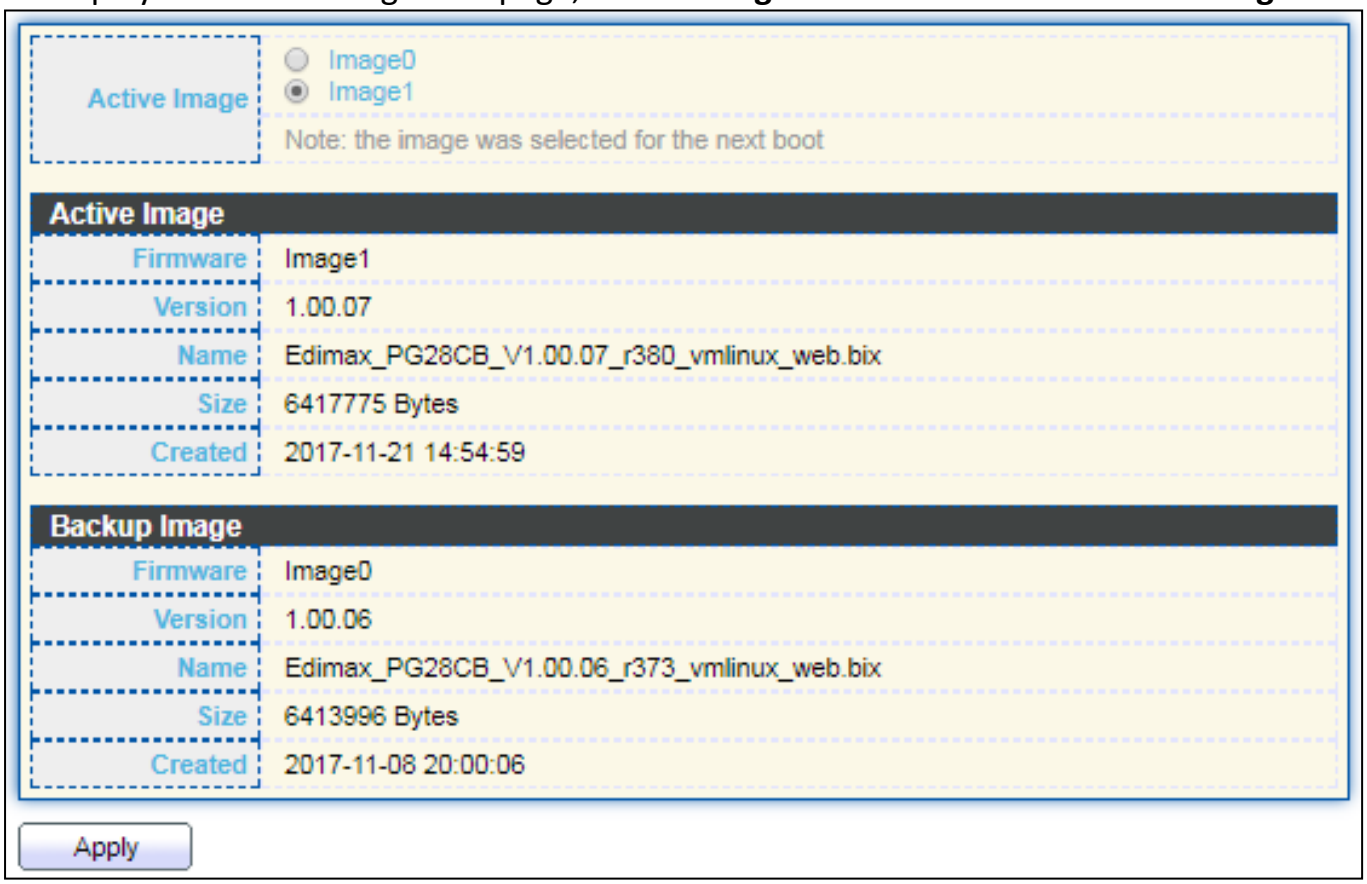


Figure 157 - Management > Fireware > Active Image

Item	Description
Active Image	Select firmware image to use on next booting
Firmware	Firmware flash partition name.
Version	Firmware version.
Name	Firmware name.
Size	Firmware image size.
Created	Firmware image created date.

IV-14-3 Configuration

IV-14-3-1 Upgrade / Backup

This page allow user to upgrade or backup configuration file through HTTP or TFTP server.

To display firmware upgrade or backup web page, click **Management > Configuration > Upgrade/Backup**.

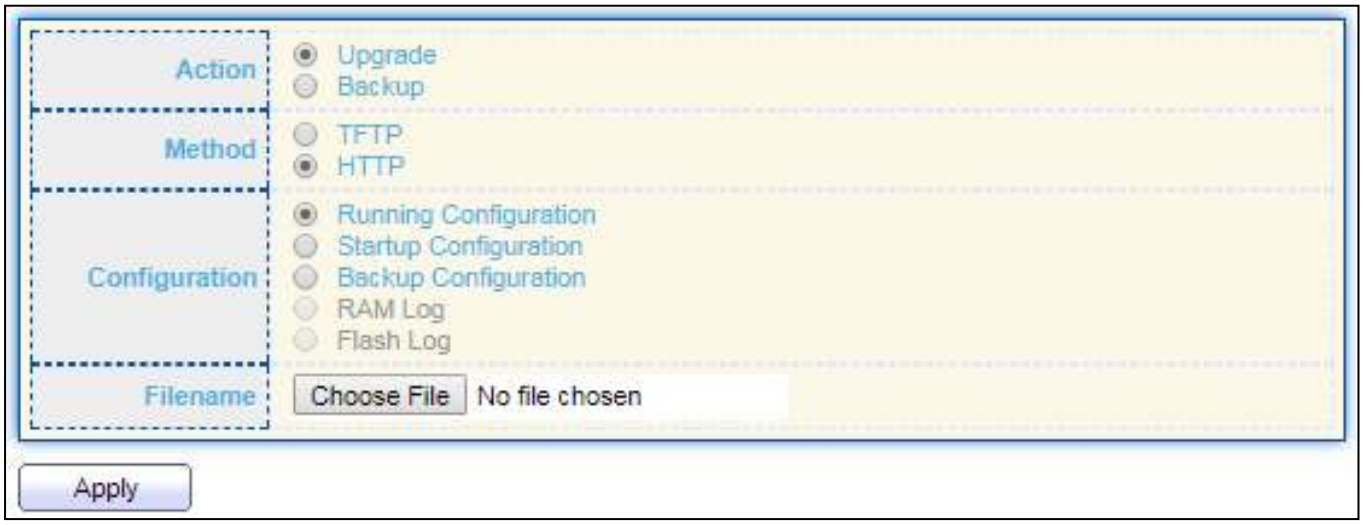


Figure 158 - Management > Configuration > Upgrade/Backup

Item	Description
Action	Configuration operations ● Upgrade: Upgrade firmware from remote host to DUT ● Backup: Backup firmware image from DUT to remote host
Method	Configuration upgrade / backup method ● TFTP: Using TFTP to upgrade/backup firmware ● HTTP: Using WEB browser to upgrade/backup firmware
Configuration	Configuration types ● Running Configuration: Merge to current running configuration file ● Startup Configuration: Replace startup configuration file ● Backup Configuration: Replace backup configuration file
Filename	Use browser to upgrade configuration, you should select configuration file on your host PC.

To display firmware upgrade or backup web page, click **Management > Configuration > Upgrade/Backup**.

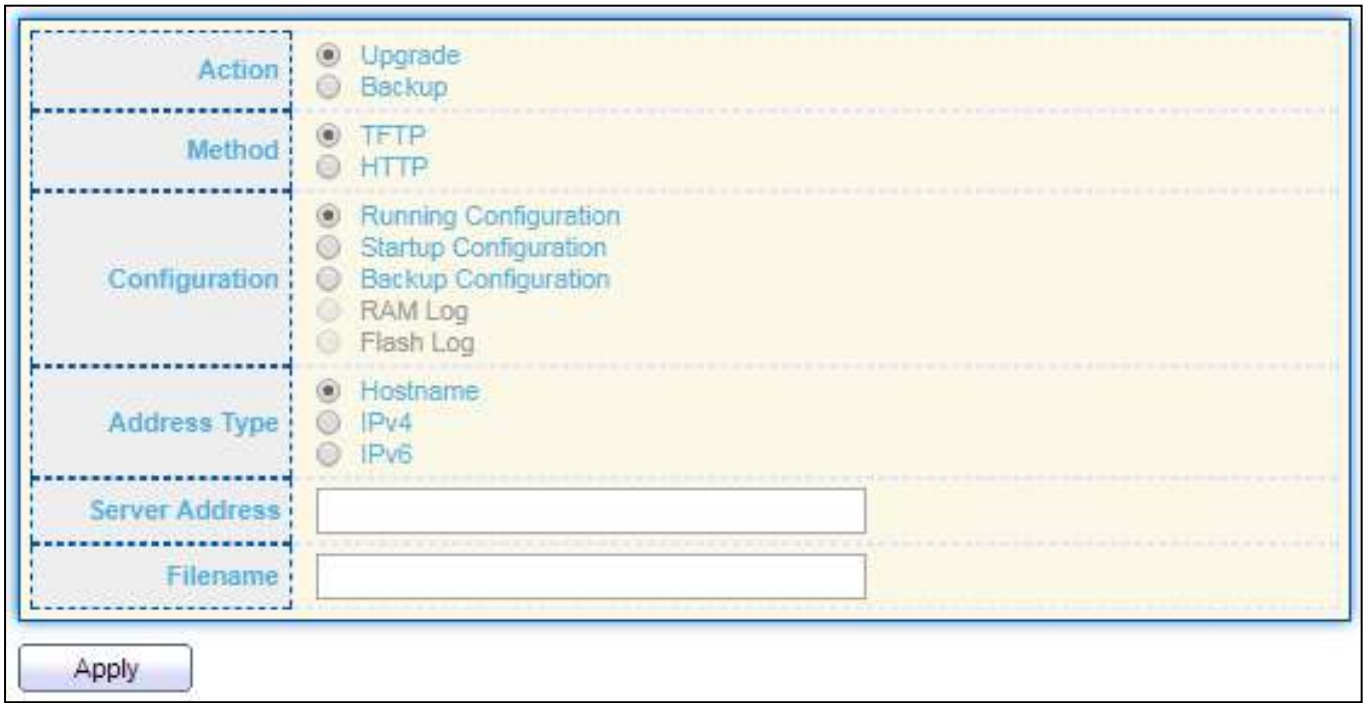


Figure 159 - Management > Configuration > Upgrade/Backup

Item	Description
Action	Configuration operations ● Upgrade: Upgrade firmware from remote host to DUT ● Backup: Backup firmware image from DUT to remote host
Method	Configuration upgrade / backup method ● TFTP: Using TFTP to upgrade/backup firmware ● HTTP: Using WEB browser to upgrade/backup firmware
Configuration	Configuration types ● 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 address
Filename	File name saved on remote TFTP server

To display firmware upgrade or backup web page, click **Management > Configuration > Upgrade/Backup**.

Figure 160 - Management > Configuration > Upgrade/Backup

Item	Description
Action	Configuration operations ● Upgrade: Upgrade firmware from remote host to DUT ● Backup: Backup firmware image from DUT to remote host
Method	Configuration upgrade / backup method ● TFTP: Using TFTP to upgrade/backup firmware ● HTTP: Using WEB browser to upgrade/backup firmware
Configuration	Configuration types ● 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.

To display firmware upgrade or backup web page, click **Management > Configuration > Upgrade/Backup**

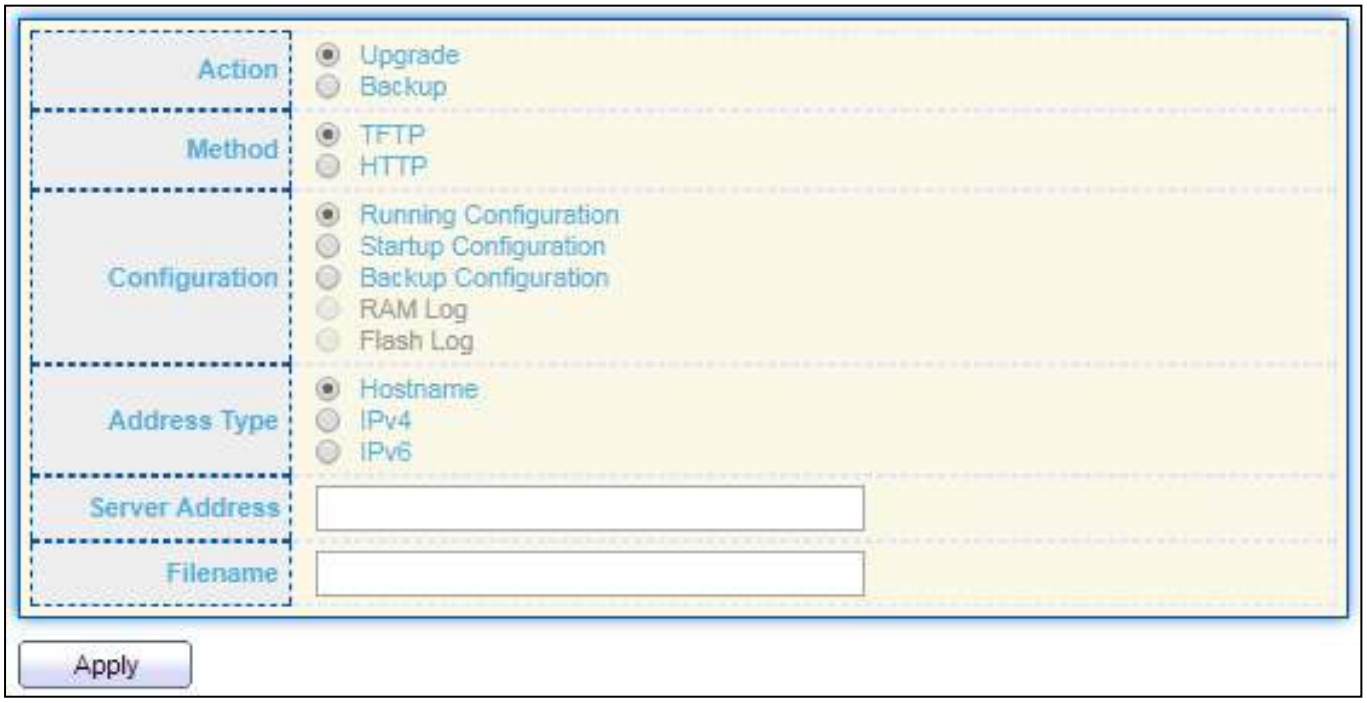


Figure 161- Management > Configuration > Upgrade/Backup

Item	Description
Action	Configuration operations ● Upgrade: Upgrade firmware from remote host to DUT ● Backup: Backup firmware image from DUT to remote host
Method	Configuration upgrade / backup method ● TFTP: Using TFTP to upgrade/backup firmware ● HTTP: Using WEB browser to upgrade/backup firmware
Configuration	Configuration types ● 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.
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 address.
Filename	File name saved on remote TFTP server.

IV-14-3-2 Save Configuration

This page allow user to manage configuration file saved on DUT and click "**Restore Factory Default**" button to restore factory defaults.

To display the Save Configuration web page, click **Management > Configuration > Save Configuration**.

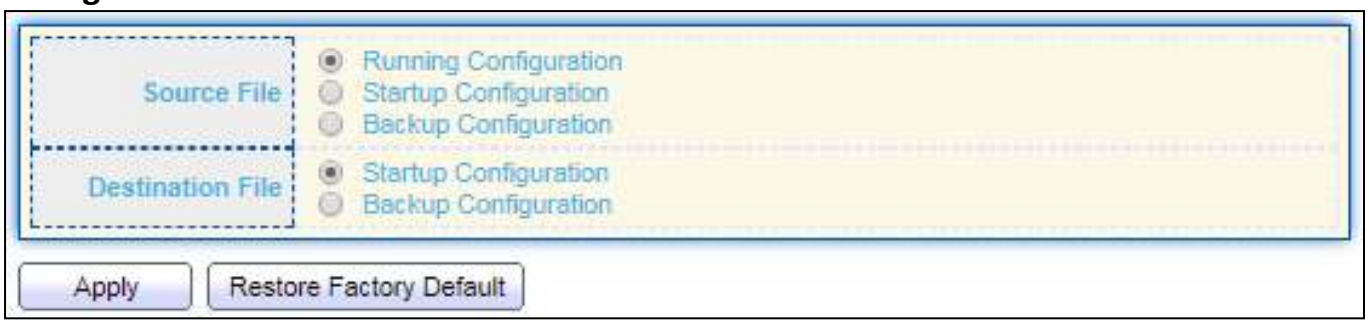


Figure 162 - Management > Configuration > Save Configuration

Item	Description
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 ● Startup Configuration: Save file as startup configuration. ● Backup Configuration: Save file as backup configuration.

IV-14-4 SNMP

IV-14-4-1 View

To configure and display the SNMP view table, click **Management > SNMP > View**.

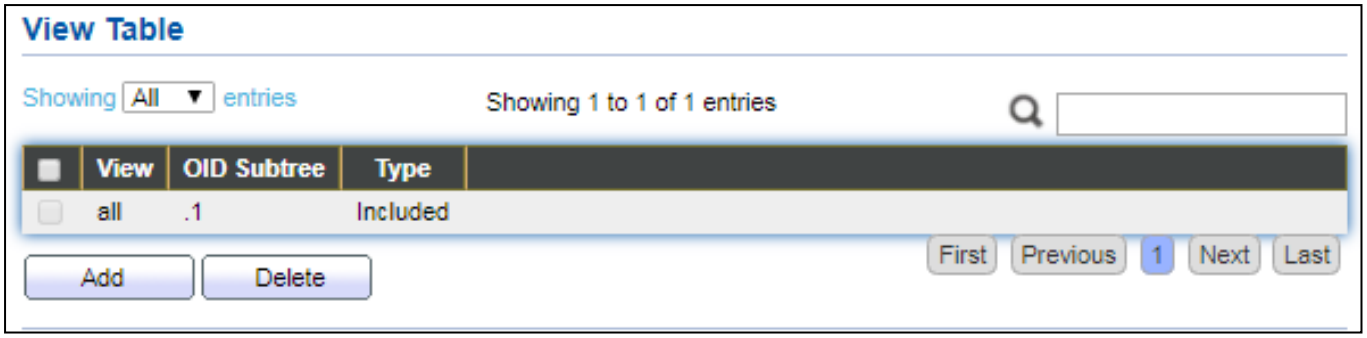


Figure 163 - Management > SNMP > View

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

IV-14-4-2 Group

To configure and display the SNMP group settings, click **Management > SNMP > Group**.

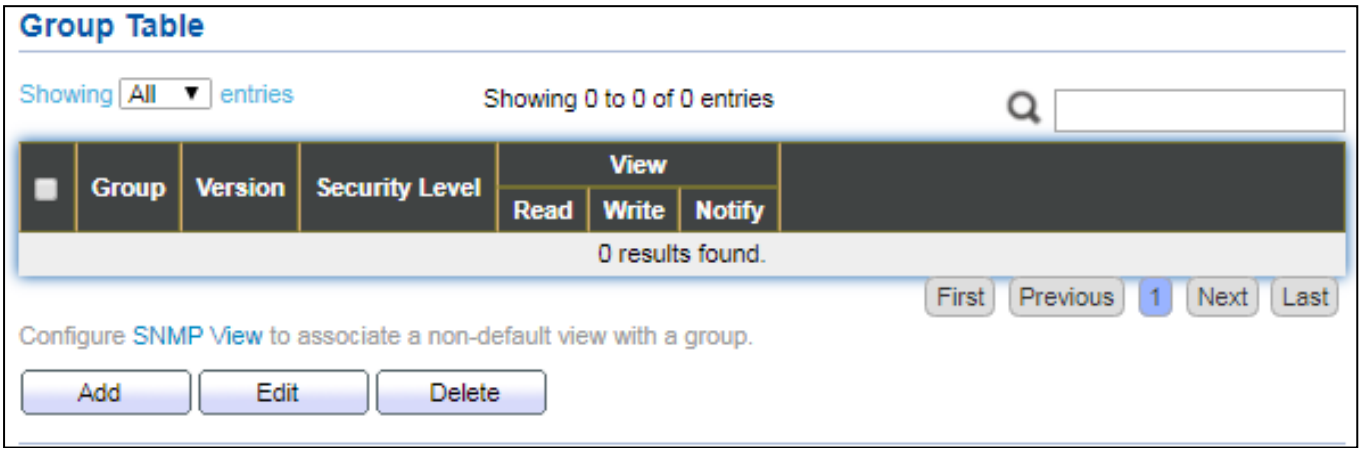


Figure 164 - Management > SNMP > Group

Item	Description
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 2. ● 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 encryption is performed.
View	
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.

Click "**Add**" or "**Edit**" button to view the Add/Edit Group menu.

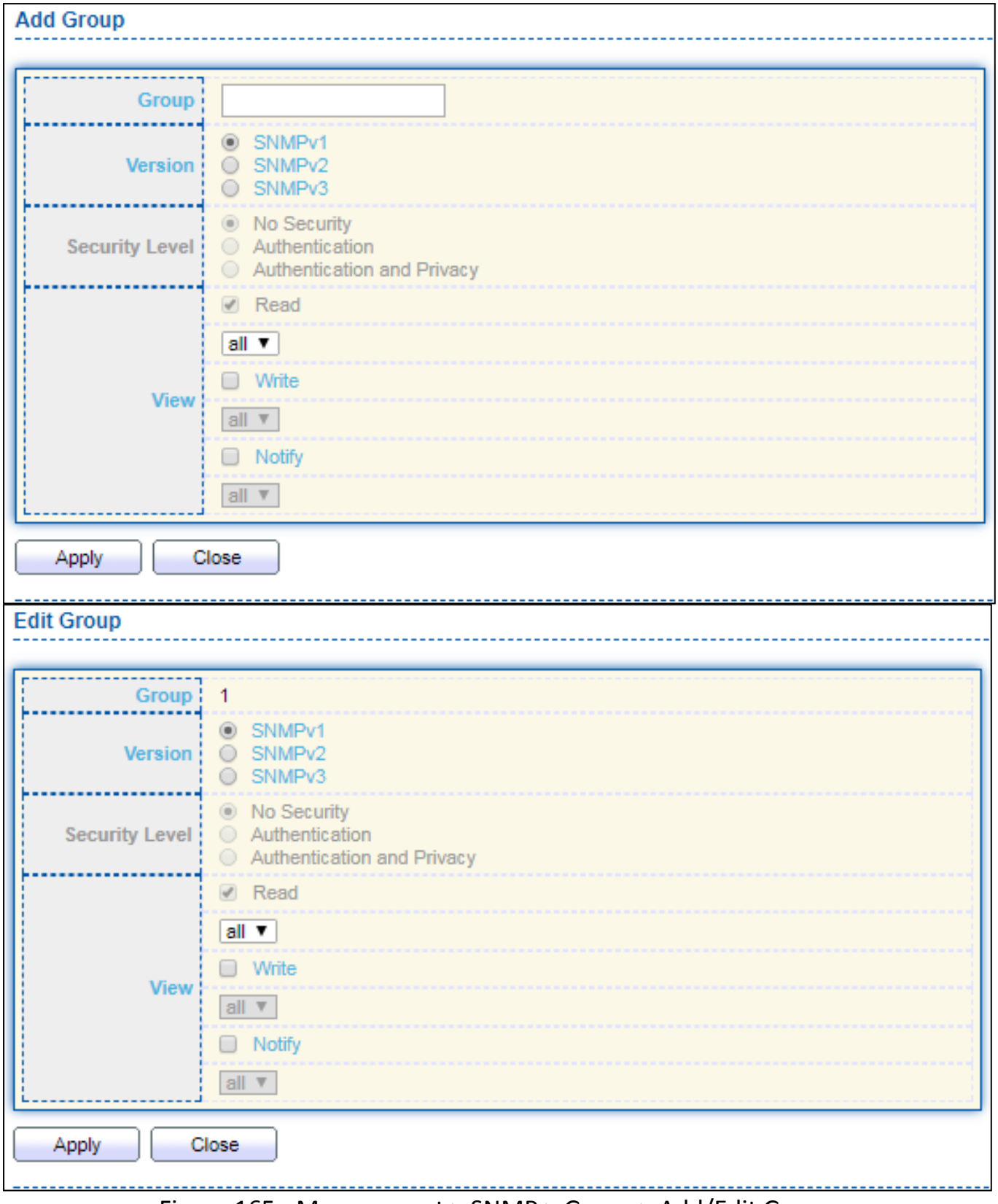


Figure 165 - Management > SNMP > Group > Add/Edit Group

Item	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 2. ● 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 encryption 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.

IV-14-4-3 Community

To configure and display the SNMP community settings, click **Management > SNMP > Community**.

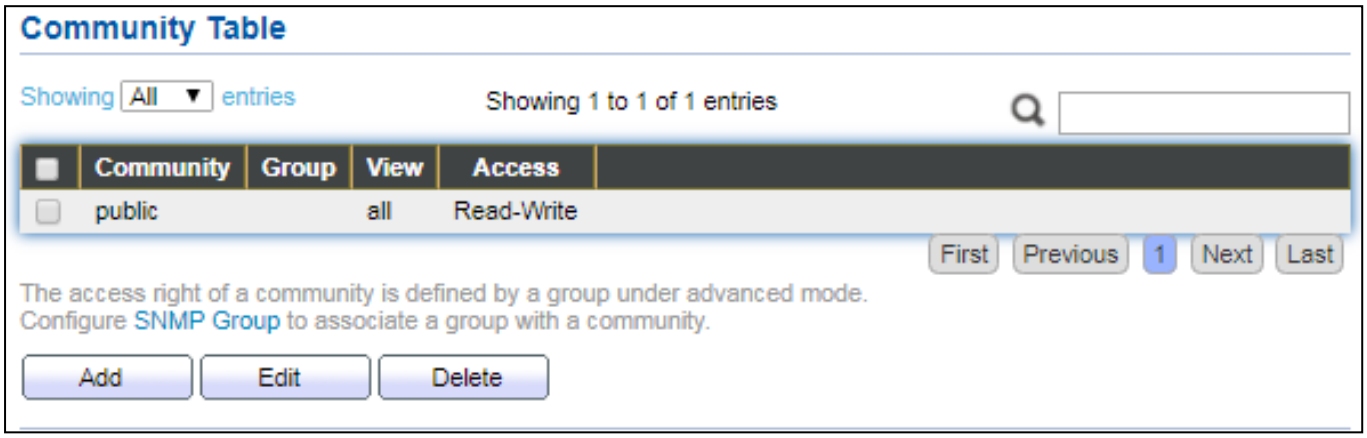


Figure 166 - Management > SNMP > Community

Item	Description
Community	The SNMP community name. Its maximum length is 20 characters.
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.

Click "**Add**" or "**Edit**" button to view the Add/Edit Community menu.

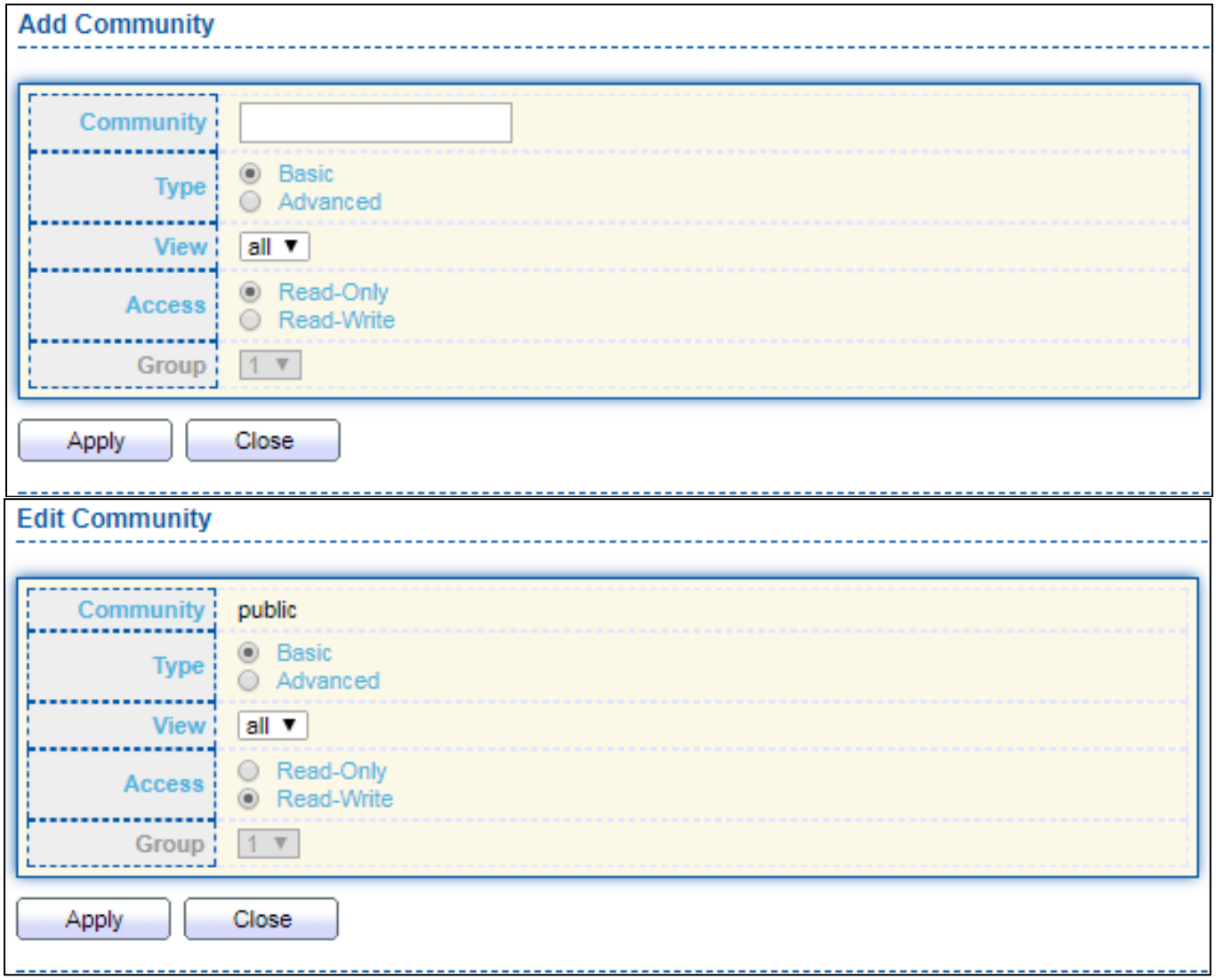


Figure 167 - Management > SNMP > Group > Add/Edit Community

Item	Description
Community	The SNMP community name. Its maximum length is 20 characters.
Type	SNMP Community mode ● Basic: SNMP community specifies view and access right. ● Advanced: SNMP community specifies group.
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.
Group	Specify the SNMP group configured by the command snmp group to define the object available to the community.

IV-14-4-4 User

To configure and display the SNMP users, click **Management > SNMP > User**.

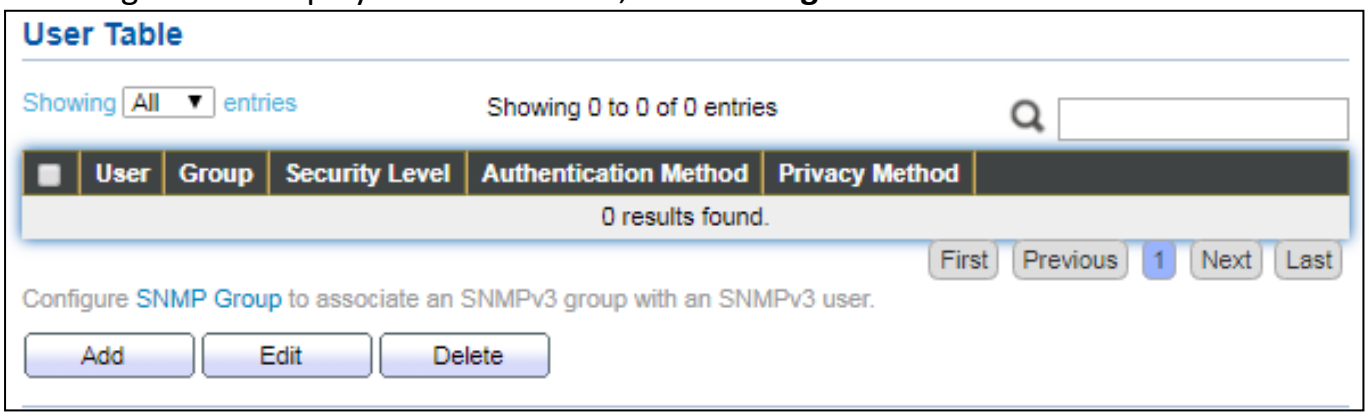


Figure 168 - Management > SNMP > User

Item	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 algorithm

Click "**Add**" or "**Edit**" button to view Add/Edit User menu.

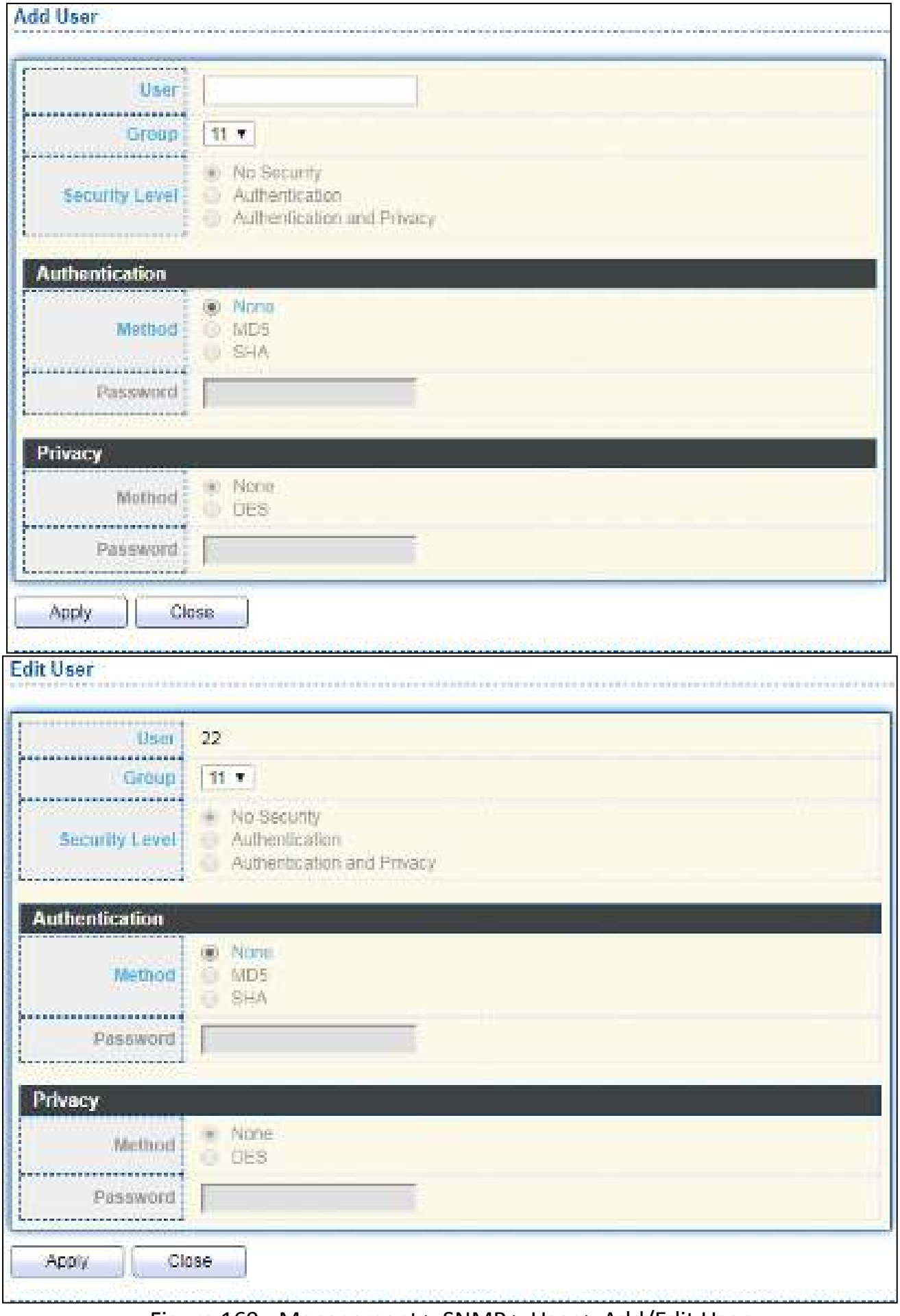


Figure 169 - Management > SNMP > User > Add/Edit User

Item	Description
User	Specify the SNMP user name on the host that connects to the SNMP agent. The max character is 30 characters.
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.
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
Password	The privacy password, The number of character range is 8 to 64 characters.

IV-14-4-5 Engine ID

To configure and display SNMP local and remote engine ID, click Management > SNMP > Engine ID.

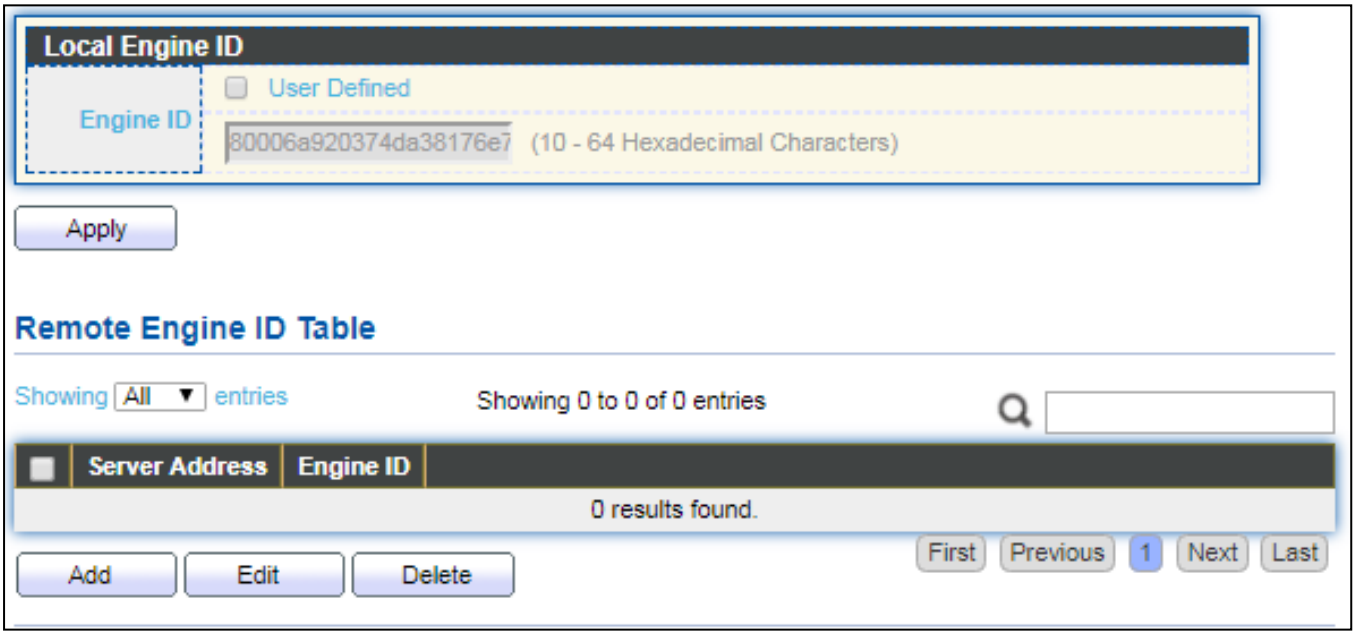


Figure 170 - Management > SNMP > Engine ID

Item	Description
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.
Remote Engine ID Table Table	
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 "**Add**" button to view Add Remote Engine ID menu.

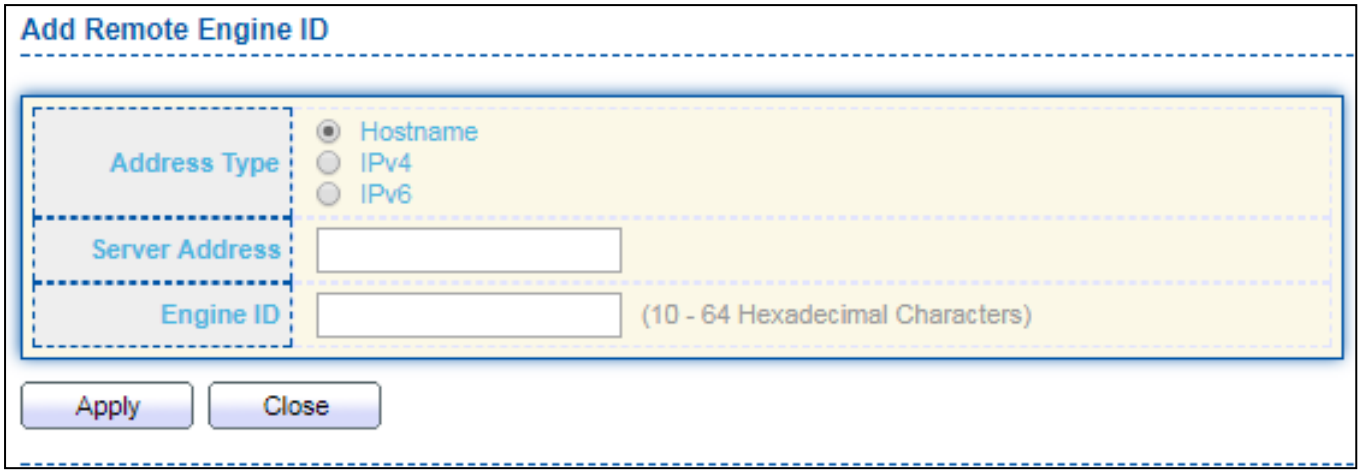


Figure 171 - Management > SNMP > Add Engine ID

Item	Description
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 "**Edit**" button to view Edit Remote Engine ID menu.

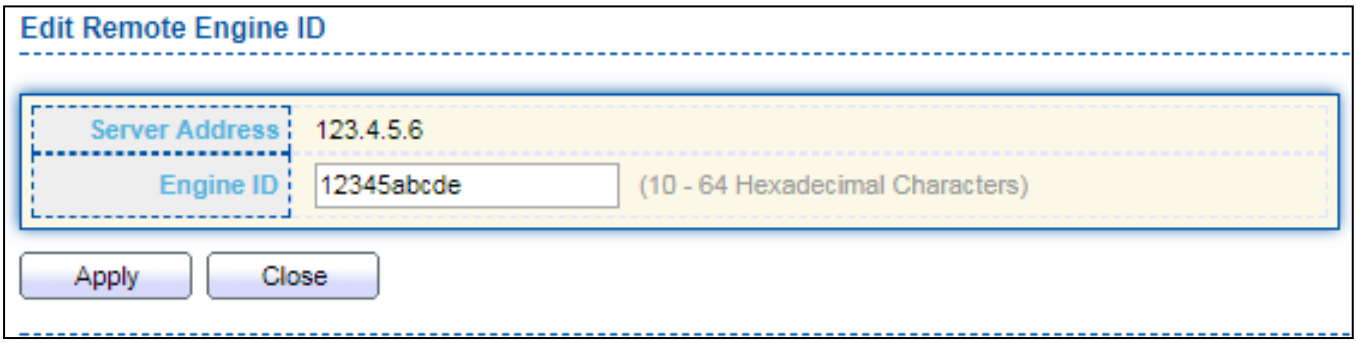


Figure 172 - Management > SNMP >Edit Engine ID

Item	Description
Server Address	Edit Remote host address
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.

IV-14-4-6 Trap Event

To configure and display SNMP trap event, click **Management > SNMP > Trap Event**.

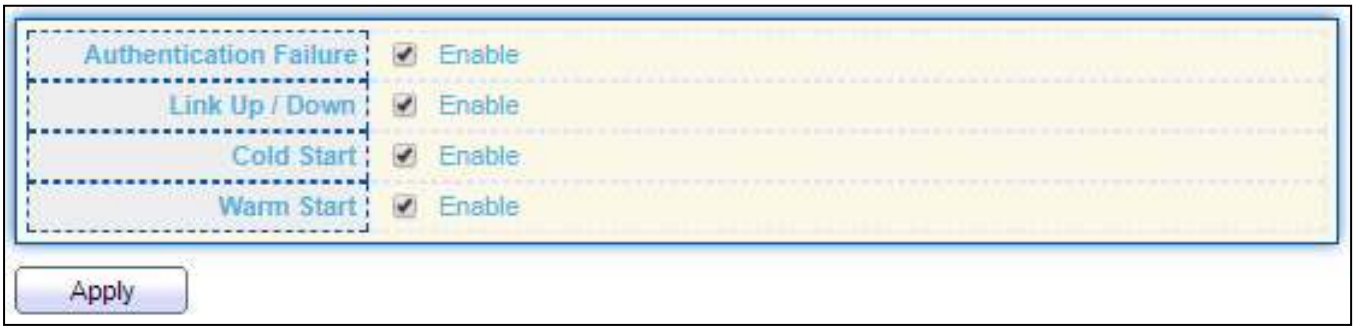


Figure 173 - Management > SNMP > Trap Event

Item	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.

IV-14-4-7 Notification

To configure the hosts to receive SNMPv1/v2/v3 notification, click **Management > SNMP > Notification**.

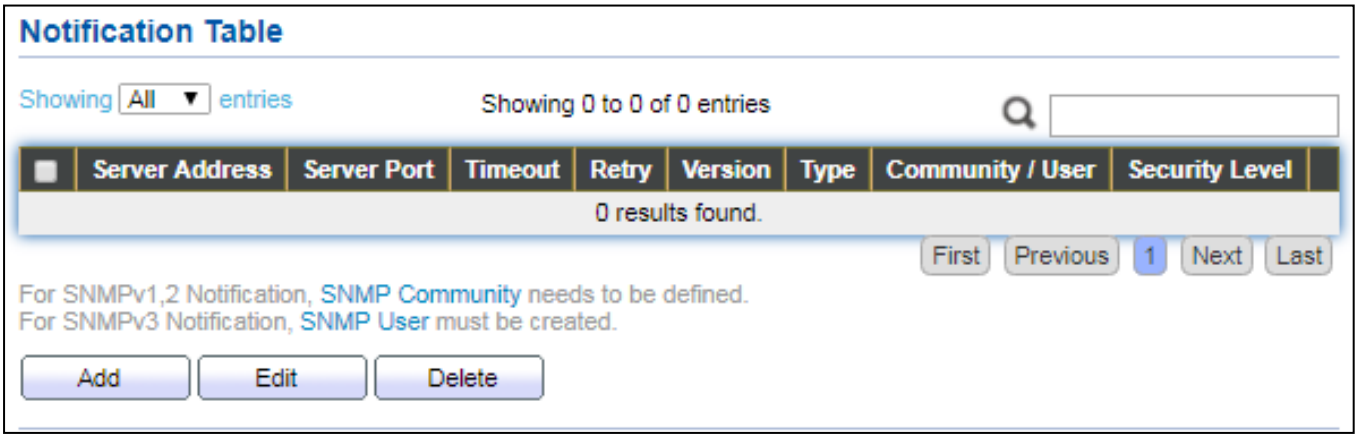


Figure 174 - Management > SNMP > Notification

Item	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 encryption is performed.

Click "**Add**" button to view the Notification menu.

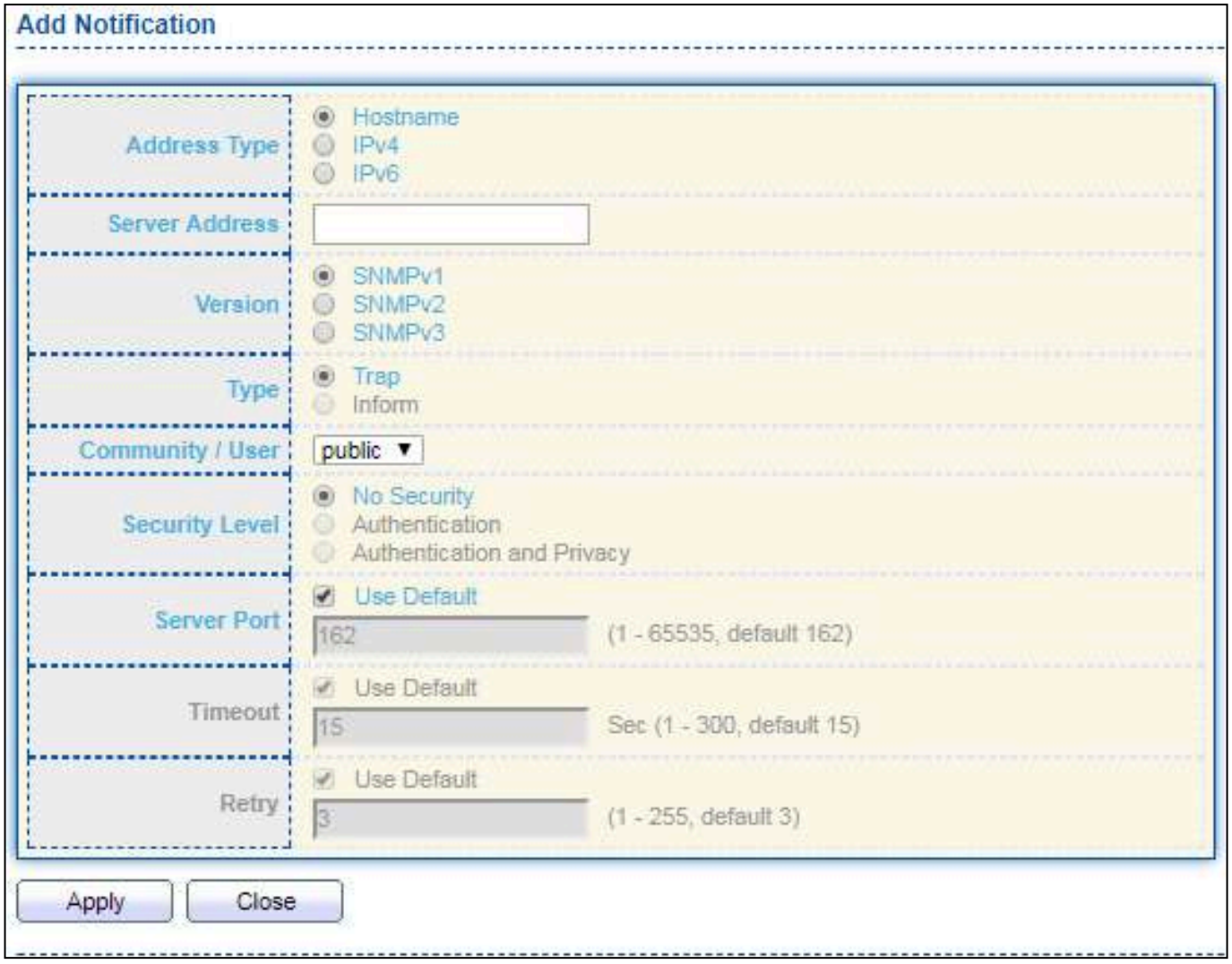


Figure 175 - Management > SNMP > Notification > Add Notification

Item	Description
Address Type	Notify recipients host address type.
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 "**Edit**" button to view the Edit Notification menu.

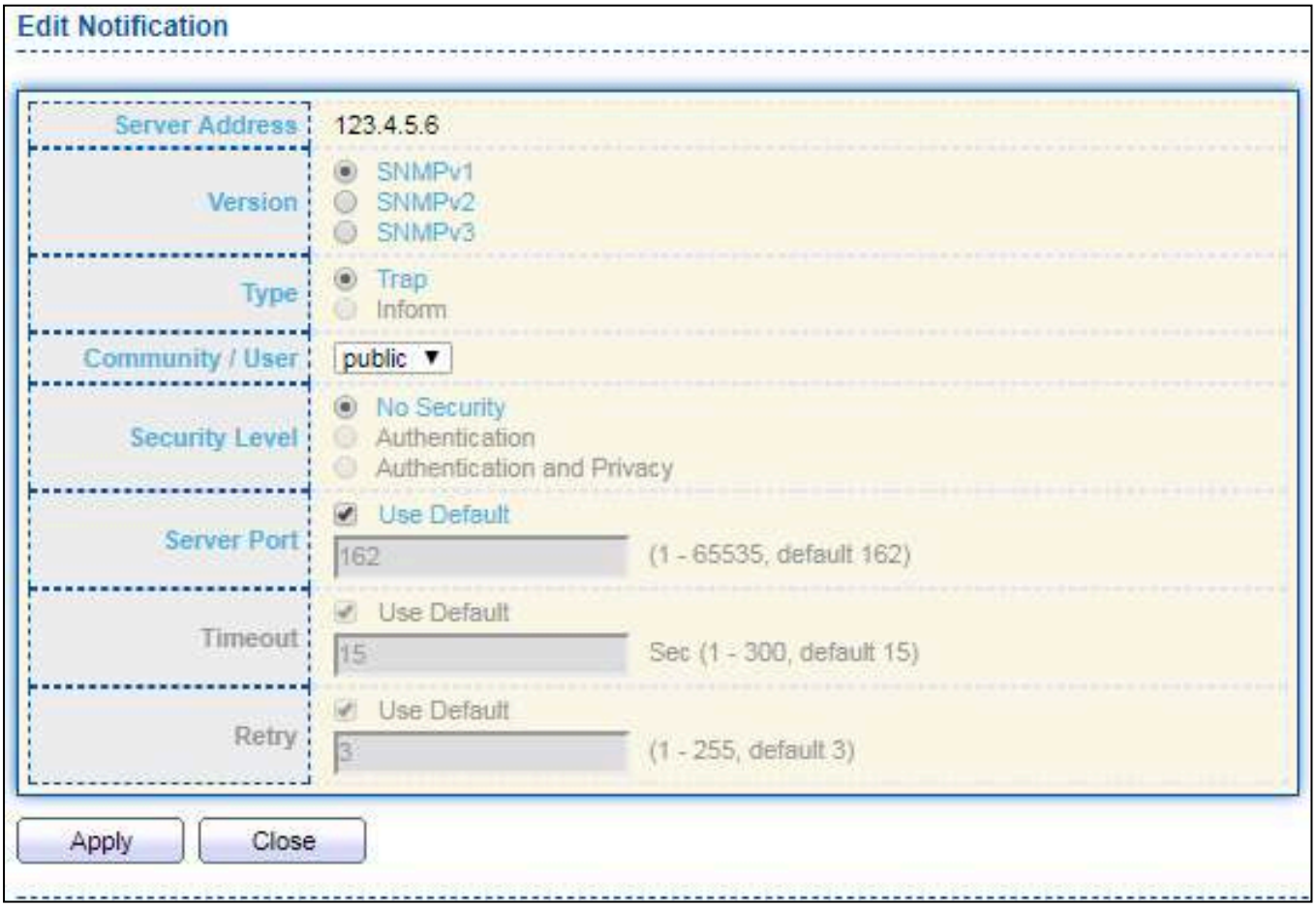


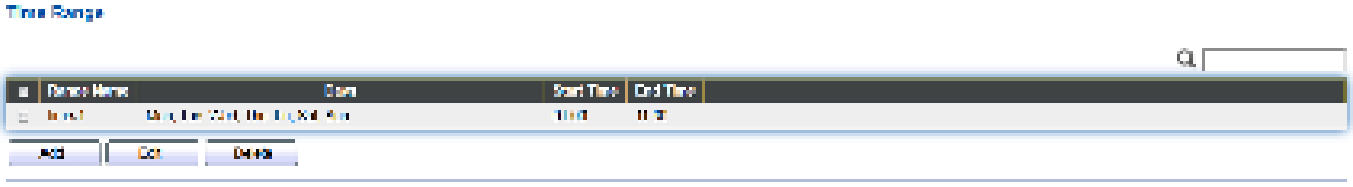
Figure 176 - Management > SNMP > Notification > Edit Notification

Item	Description
Server Address	Edit SNMP notify recipients address
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.
Community 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.

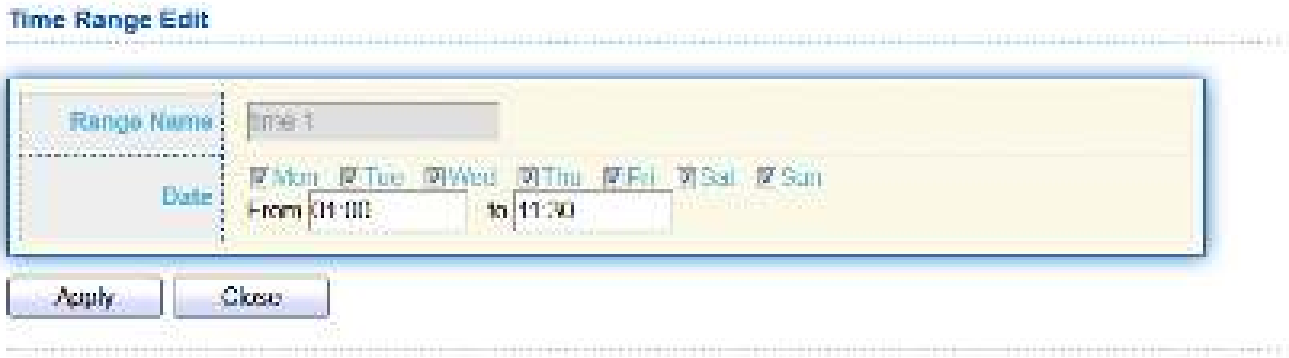
Server Port	Recipients server UDP port number, if “use default” checked the value is 162, else user configure.
Timeout	Specify the SNMP informs timeout, if “use default” checked the value is 15, else user configure.
Retry	Specify the SNMP informs retry count, if “use default” checked the value is 3, else user configure.

IV-14-5 Time Range

This page shows the information of days, start time and end time of the time range.



To view the Time Range Edit page, please click the ‘Edit” button.



V Surveillance Mode

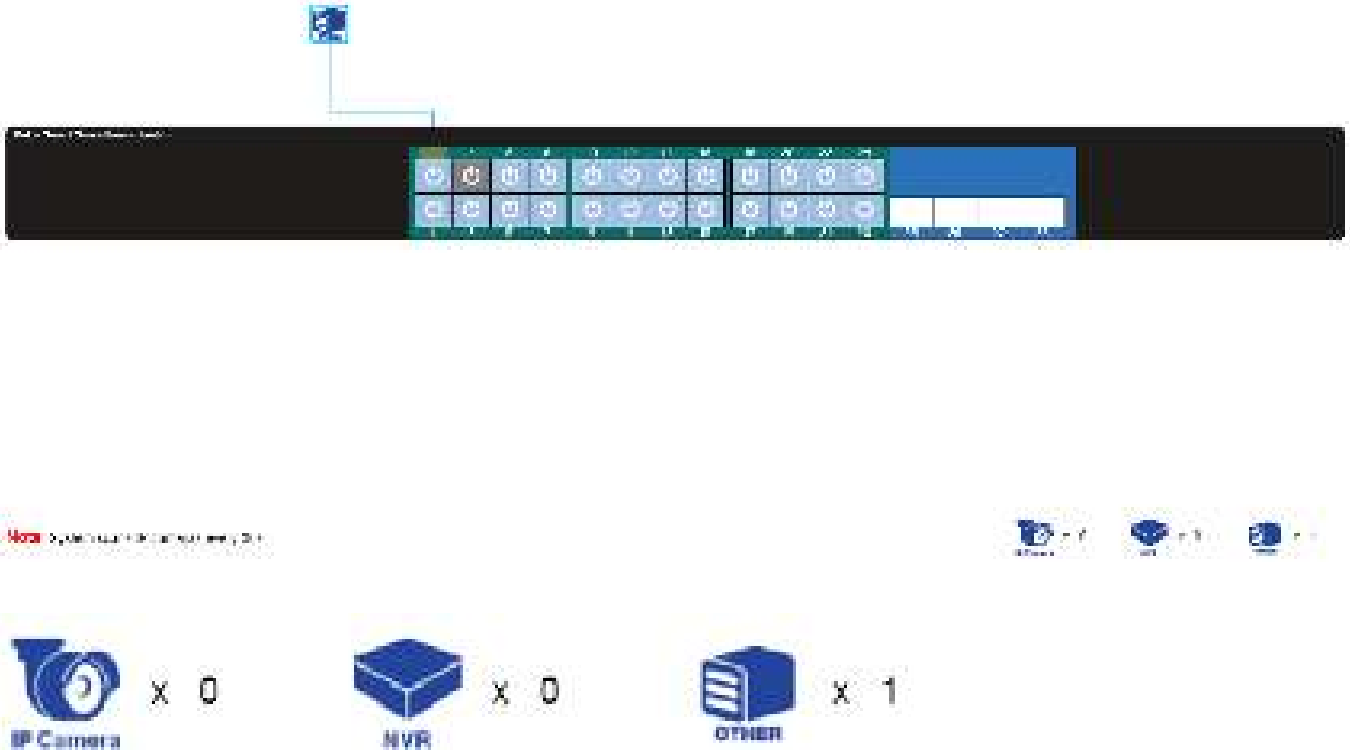
The simple and intuitive GUI of Surveillance Mode provides real-time device and network information

V-1 Home Page

The figure below shows the user interface.

V-1-1 Overview

This page displays information and configuration options for the switch. It contains a diagram of the switch, including an overview of the devices connected to the switch.



There is a device count at the bottom of the page, listing the number of connected IP-Cameras, NVRs and other (unrecognized devices).

NOTE: System scans IP camera every 30s.

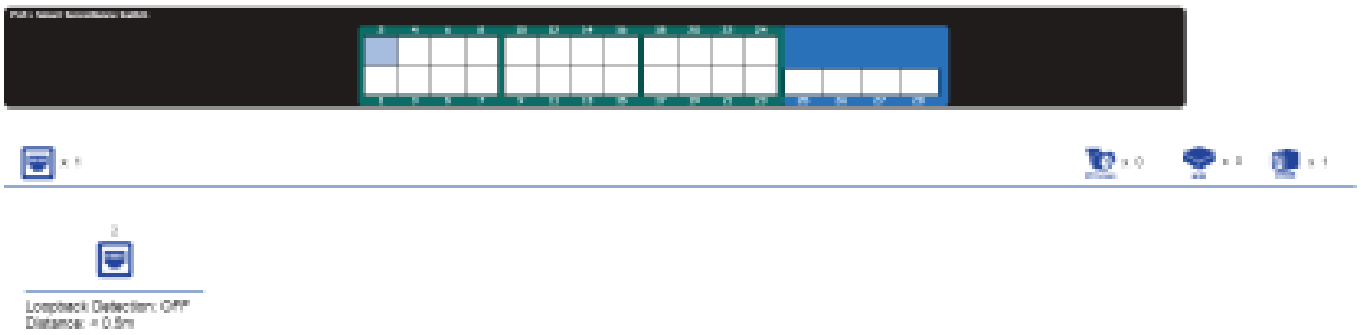
You can remote control the PoE port by clicking the power button  on the switch

Item	Description
	The total number of IP-Cameras connected to the switch.
	The total number of NVRs connected to the switch.
	The number of unknown devices connected to the switch.

Item	Description
	PoE is enabled on the port.
	PoE is disabled on the port.

V-1-2 Port Info

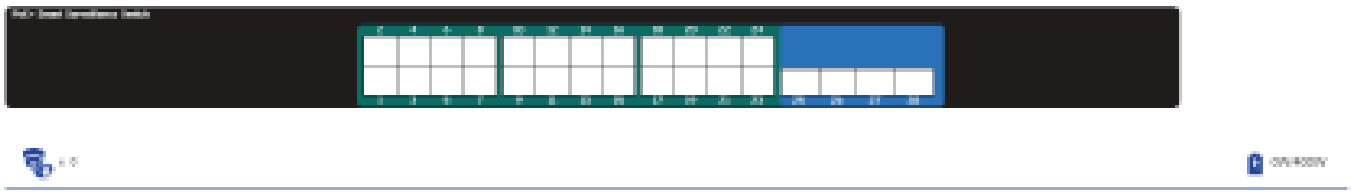
In this page you can check the status of PoE port, loopback detection and the range of the distance.



Item	Description
PoE port	Shows the PoE port is connected with IP camera, NVR or others
loopback detection	Loopback Detection (LBD) provides protection against loops by transmitting loop protocol packets out of ports on which loop protection has been enabled. When the switch sends out a loop protocol packet, and then receives the same packet, it shuts down the port that received the packet.
Distance	It shows the cable length (in meters)

V-1-3 IP Camera Info

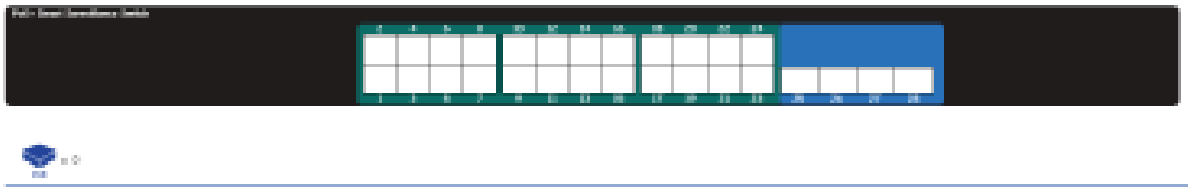
The IP-Camera Information section provides information on each camera connected to the switch.



Item	Description
	The PoE consumption of the switch. This is listed as one negative integer and one positive integer. The negative integer is the power being consumed by the PoE devices connected to the switch. The positive integer is the total PoE budget for the ports currently using PoE, based on the type of PoE in use.
	The total number of ONVIF IP-Cameras connected to the switch.

V-1-4 NVR Info

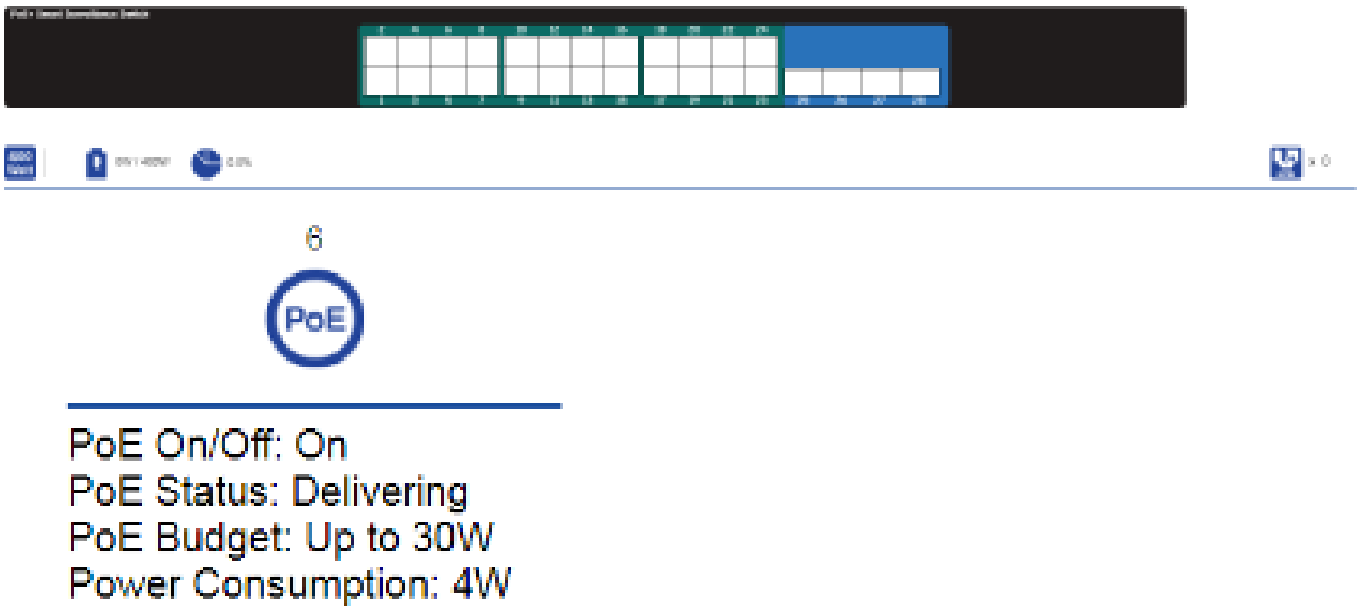
The NVR Information section provides information on each NVR connected to the switch.



Item	Description
	The total number of NVRs connected to the switch.

V-1-5 PoE Info

The PoE Information section provides information on the PoE usage of each port.



There is a PoE status at the bottom of the page, listing the PoE status, budget and consumption.

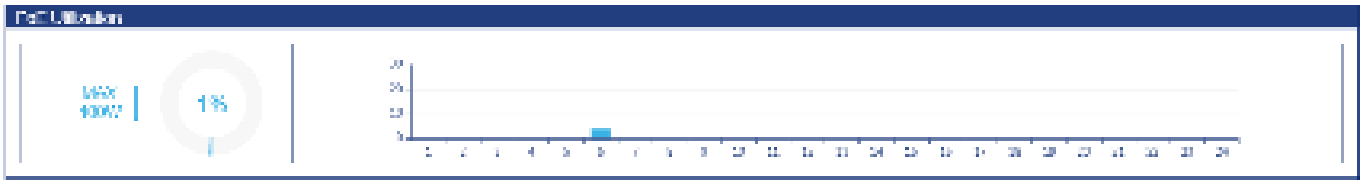
Item	Description
	The total power budget.
	The PoE consumption of the switch. This is listed as one negative integer and one positive integer. The negative integer is the power being consumed by the PoE devices connected to the switch. The positive integer is the total PoE budget for the ports currently using PoE, based on the type of PoE in use.
	The current utilization of PoE total power budget.

V-1-6 Status

This is the main page on the Surveillance page and is divided into 3 areas, device information section, PoE utilization section and bandwidth usage section.

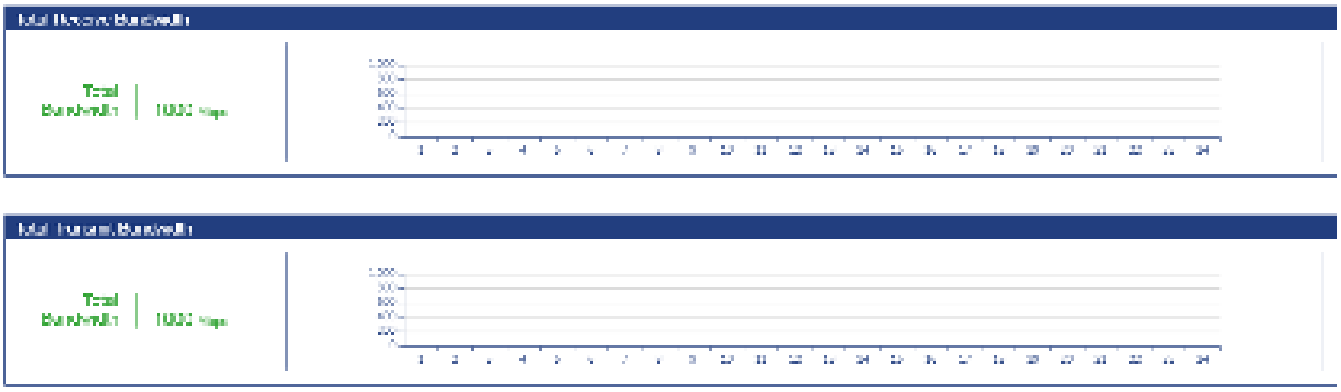
And the device information section is sub-divided into 3 sections, switch information, web information and system information.

PoE Utilization:



The PoE Utilization area contains PoE utilization statistics for the switch. On the left is the total PoE utilization, with the total power budget and overall utilization shown. On the right is a per-port usage graph, showing the PoE utilization for each individual port.

Total Receive/Transmit Bandwidth:



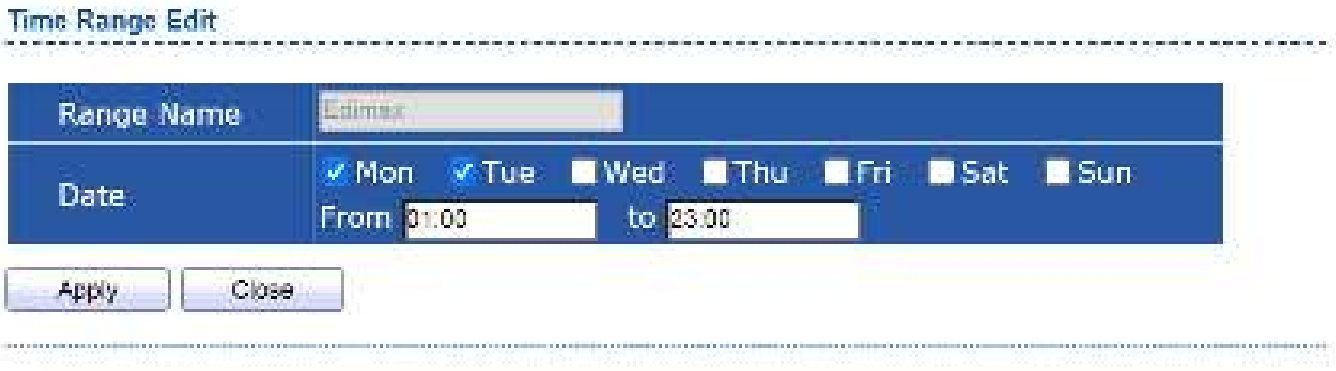
The bandwidth usage section contains bandwidth utilization for the switch. On the left the total bandwidth shows the total inbound traffic on all ports. There is also a per-port bandwidth utilization graph on the right, showing the inbound traffic for each individual port.

V-2 PoE Scheduling

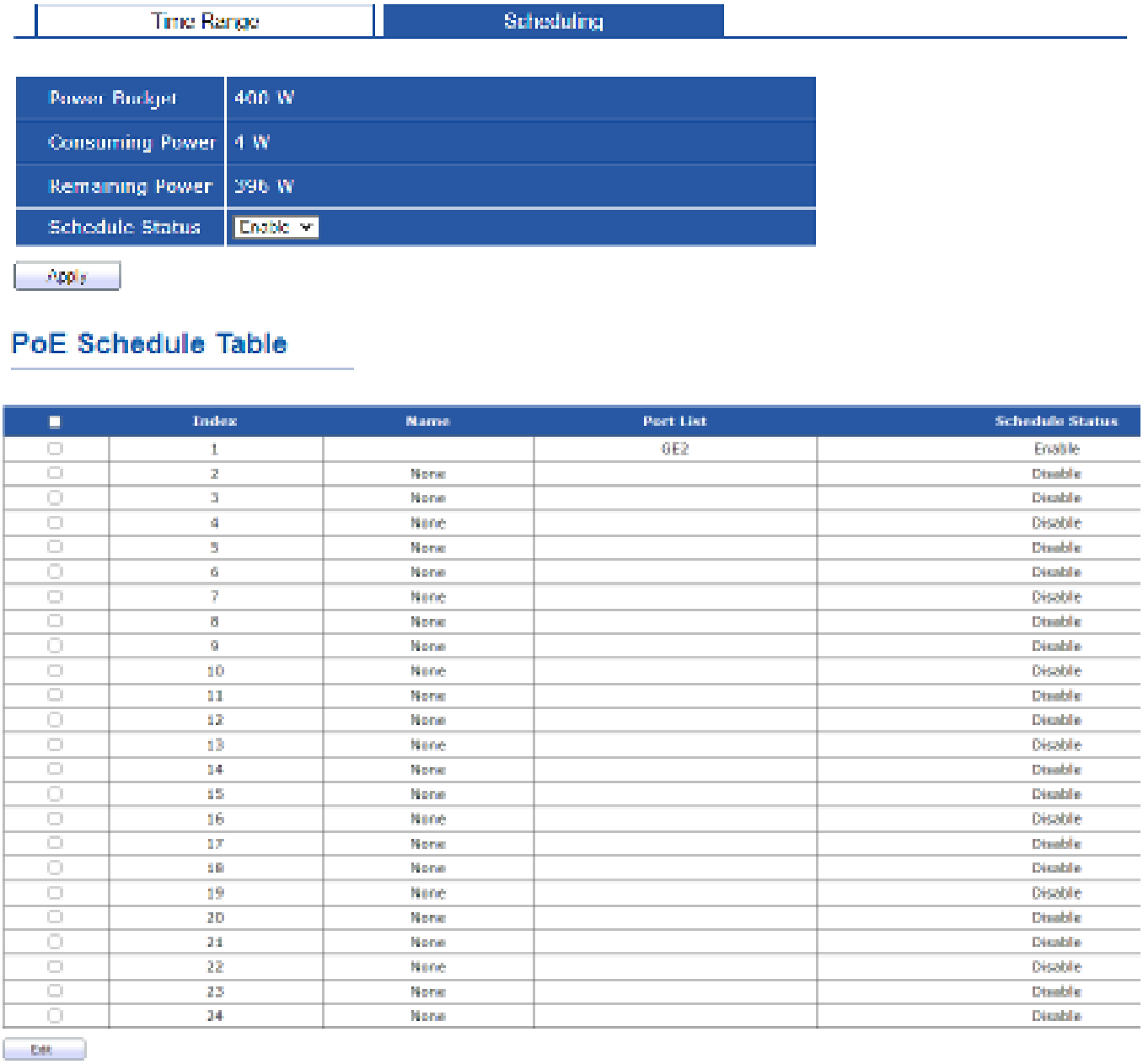
PoE Scheduling which allows you to specify the amount of time that power is delivered to a PoE port. This can be used to save power when devices are not in use, or as a security feature to prevent wireless access from being available outside of business hours.

Click "**Add**" button to view the “Time Range Edit” menu.

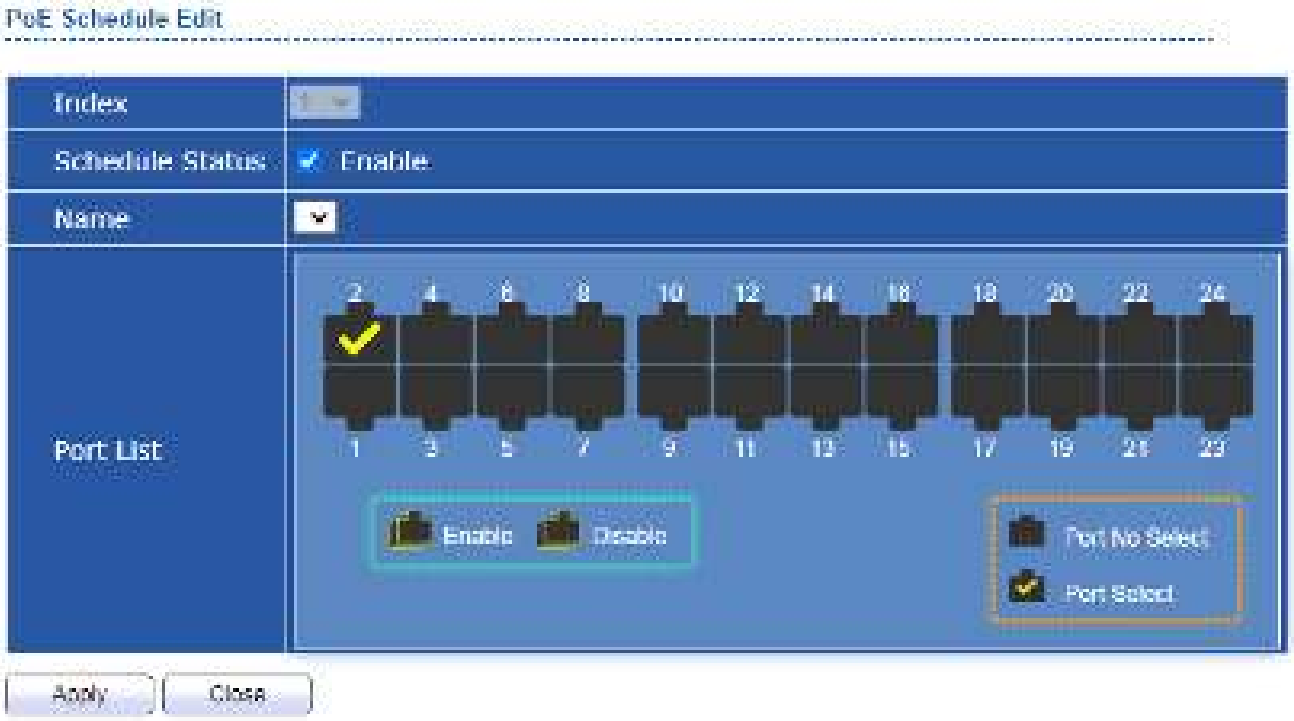
You can name your PoE schedule and choose date/time from Mon ~ Sun.



To view the following page, click on the **"Scheduling"** link in the menu:



Click "**Edit**" button to view the “PoE Schedule Edit” menu.
In this page you can enable/disable the PoE ports from the port list.

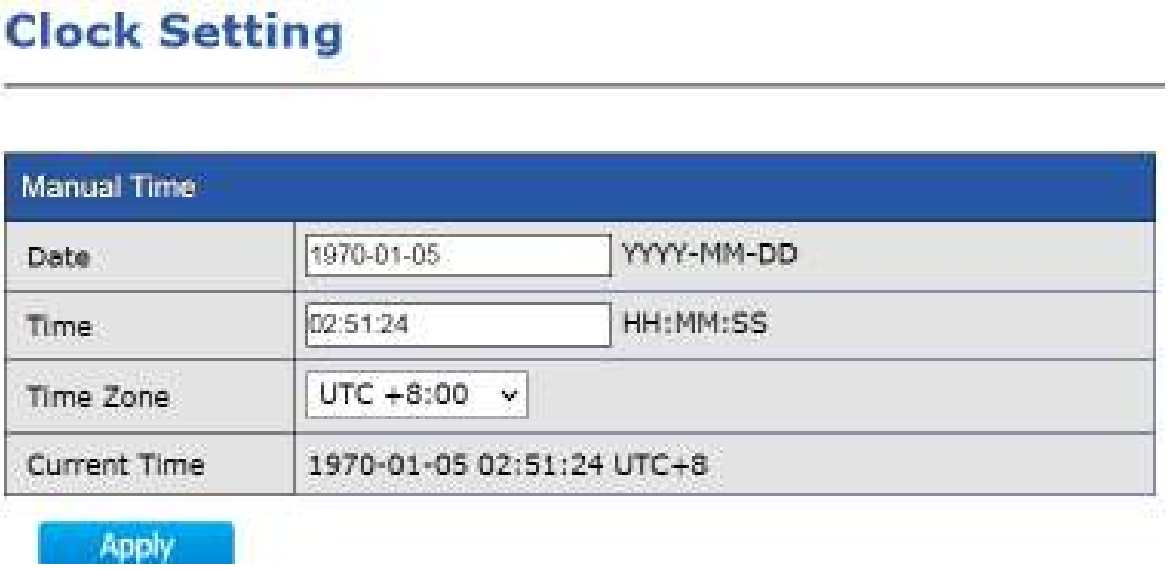


V-3 Time

In this section you can configure the setting of the clock and SNTP Server.

V-3-1 Clock Settings

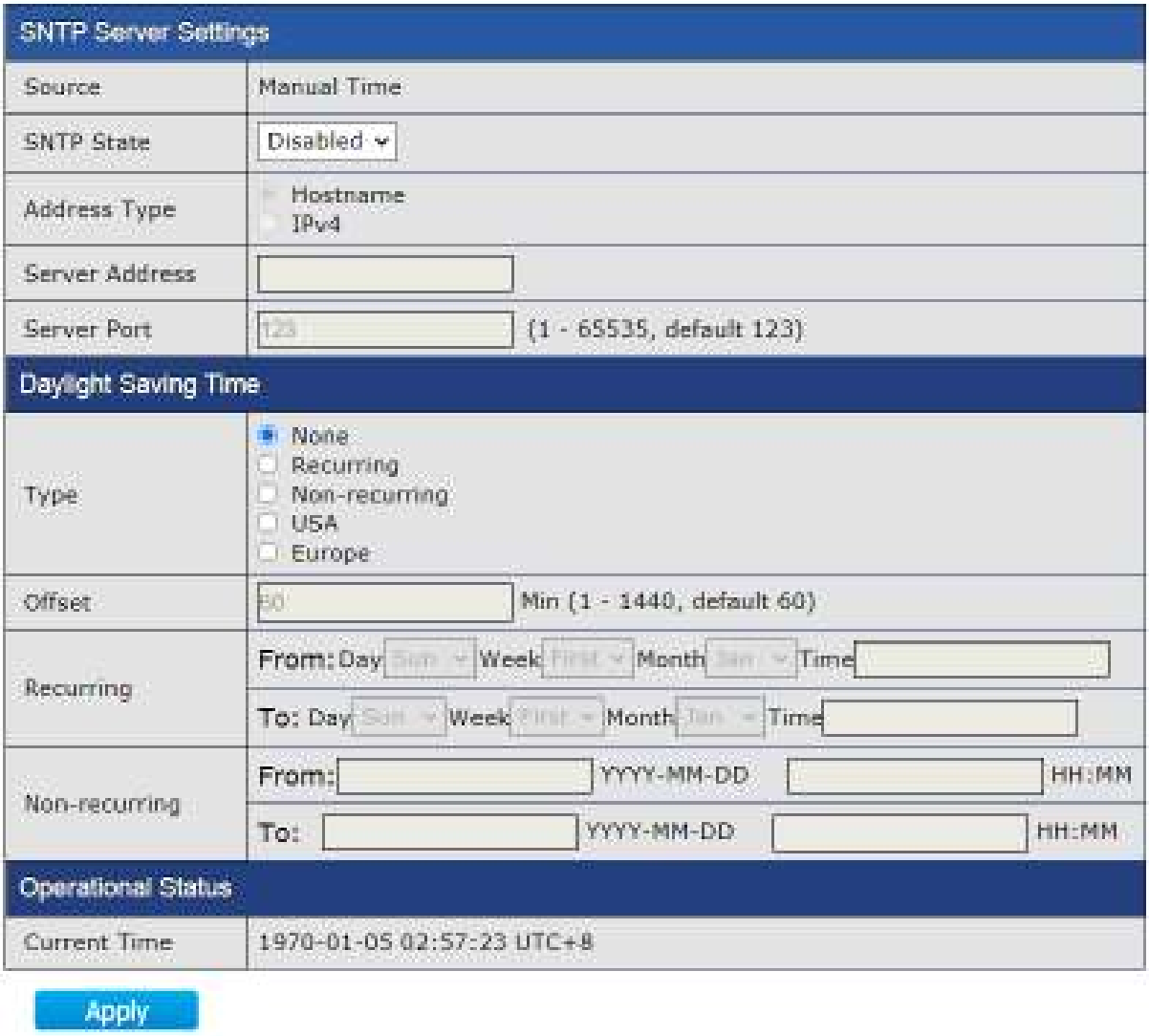
The fields that can be configured for the **Clock Settings** are described below:



Item	Description
Date	Set the date in the format (DD / MM / YYYY).
Time	Set the system time in the format (HH:MM:SS).
Time Zone	Set the time zone for your switch.
Current Time	It shows the current time for the switch.

V-3-2 SNTP Settings

. Simple Network Time Protocol (SNTP) is a lightweight version of the NTP protocol and can be used to keep the system clock in-sync by using a network-based time source.

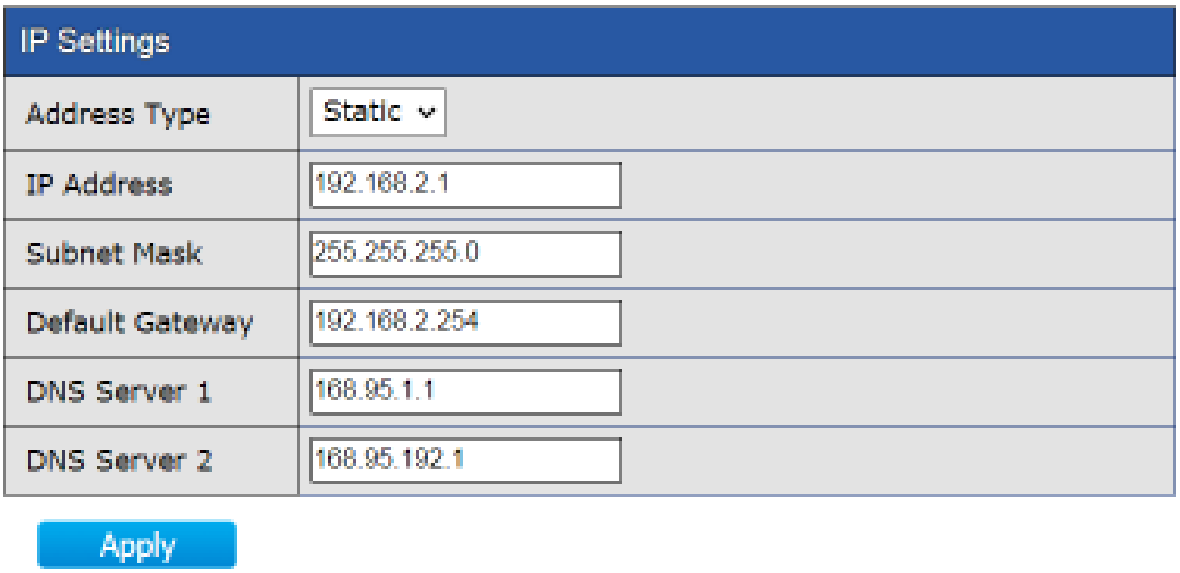


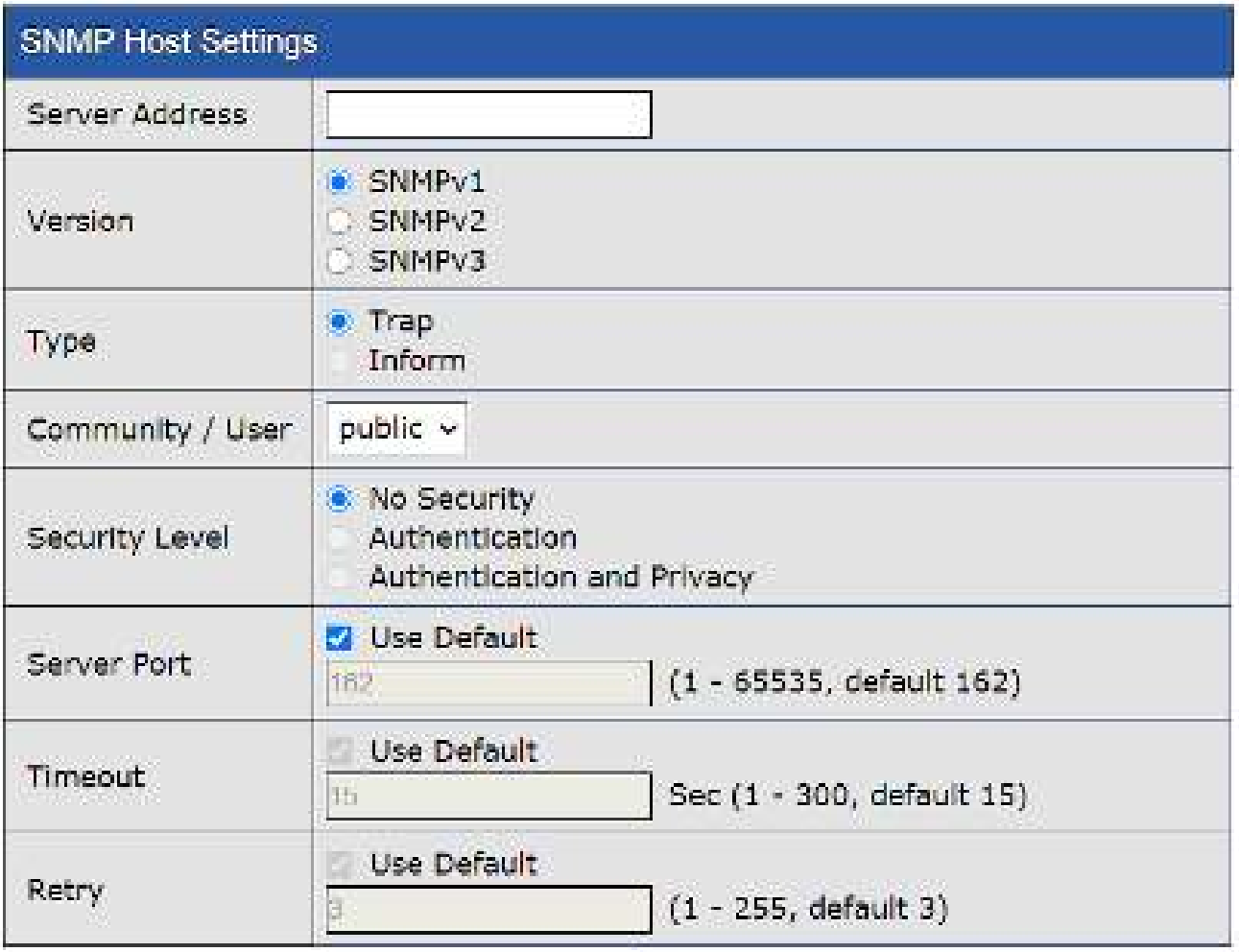
Item	Description
SNTP State	Enable/Disable
Address Type	Choose Hostname or IPv4
Server Address	Enter the IP address of the SNTP server you would like to synchronize with.
Server Port	Enter the server port (1-65535)
Daylight Saving Time	
Type	Choose the daylight saving type in none, recurring, non-recurring, USA or Europe
Offset	Enter the offset in minute (1-1440)
Operational Status	
Current Time	It shows the current time for the switch.

NOTE:
- Recurring (always occurs, with no defined stopping point).
For example, the United States started using recurring daylight savings rules in 2007.
- Nonrecurring (defined for a specific period of time).

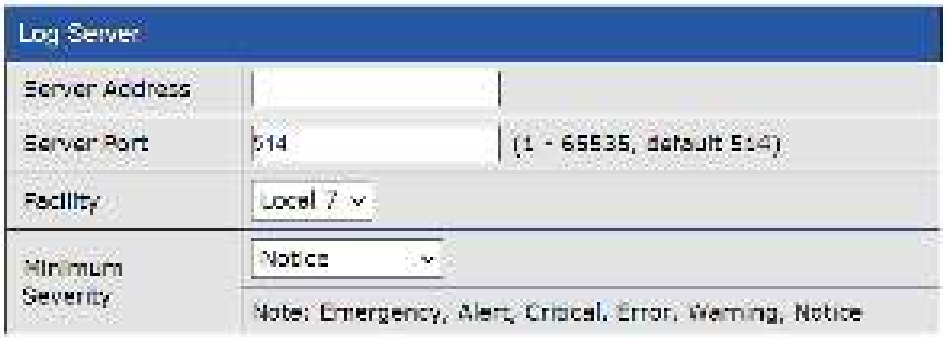
V-4 Surveillance Settings

The Surveillance Settings page is used to configure the settings for the Surveillance IP, SNMP host, log server and password.




SNMP Host Settings
Server Address
Version
SNMPv1
SNMPv2
SNMPv3
Type
Trap
Inform
Community / User
public
Security Level
No Security
Authentication
Authentication and Privacy
Server Port
Use Default
162
(1 - 65535, default 162)
Timeout
Use Default
15
Sec (1 - 300, default 15)
Retry
Use Default
3
(1 - 255, default 3)


Server Address
Server Port
Timeout
Retry
Version
Type
Community / User
Security Level
0 results found
Add
Delete
Edit
Apply


Log Server
Server Address
Server Port
514
(1 - 65535, default 514)
Facility
Local 7
Minimum Severity
Notice
Note: Emergency, Alert, Critical, Error, Warning, Notice

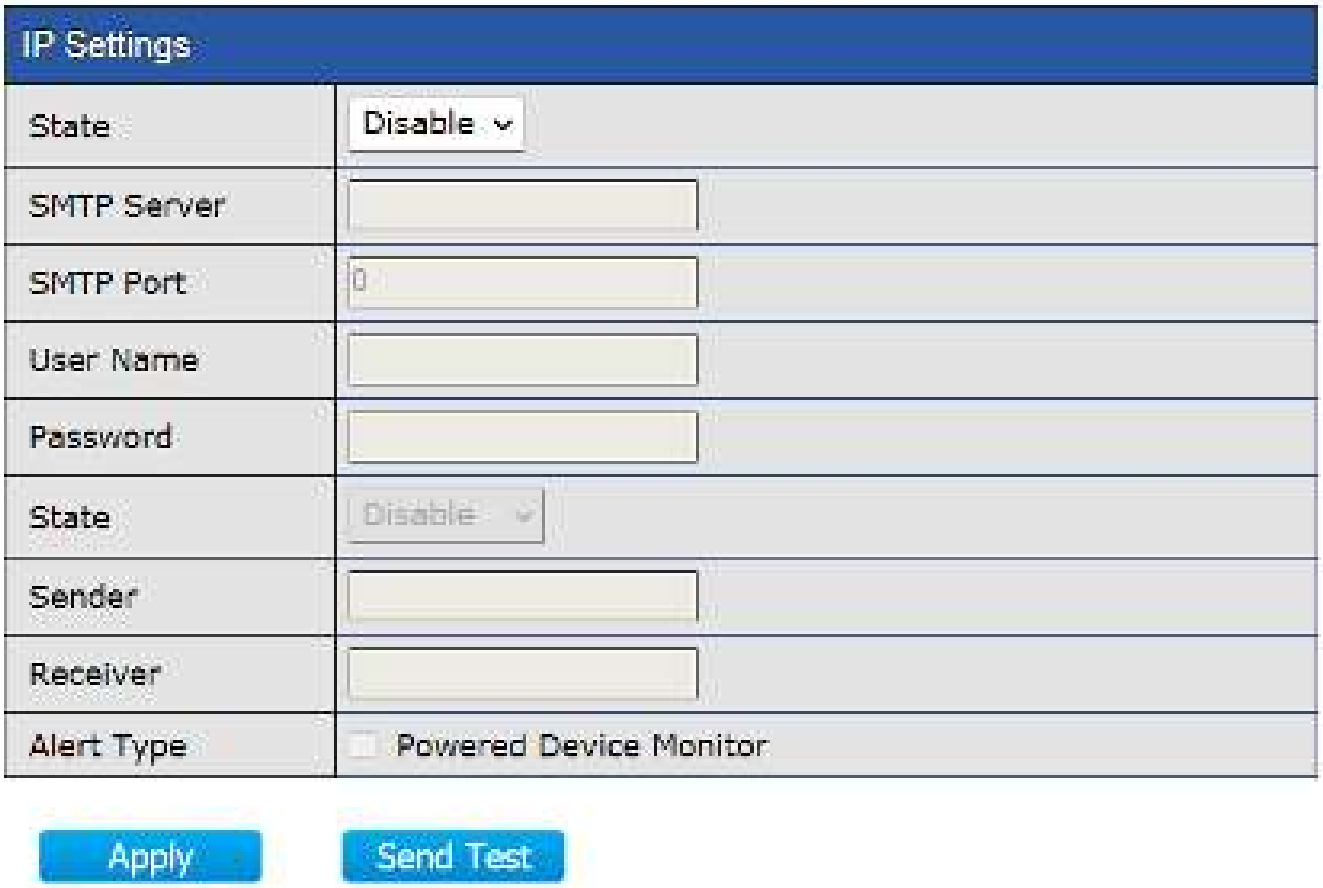

Entry
Server Address
Server Port
Facility
Minimum Severity
0 results found
Add
Delete
Edit
Apply
Password Settings
Password
Confirm Password
Apply

Item	Description
Address Type	The address type of switch IP configuration including, Static: Static IP configured by users will be used. Dynamic: Enable the DHCP to obtain the IP address from a DHCP server.
IP Address	Specify the switch static IP address on the static configuration.
Subnet Mask	Specify the switch subnet mask on the static configuration.
Default Gateway	Specify the default gateway on the static configuration. The default gateway must be in the same subnet with switch IP address configuration.
DNS Server 1	Specify the primary user-defined IPv4 DNS server configuration.
DNS Server 2	Specify the secondary user-defined IPv4 DNS server configuration.
SNMP Host Settings	
Server Address	Enter the IP address of the SNMP Network Management Server which will receive SNMP Traps from this device.
Version	The principal SNMP protocol versions including, SNMPv1: This is the initial version of SNMP. SNMPv2: This version uses a community-based form of security, just like SNMPv1, replacing the Party-based Administrative and Security Framework of SNMPv2. SNMPv3: This is an interoperable standards-based protocol defined in RFC2273, 2274, and 2275. It provides secure access to devices by authenticating and encrypting packets over the network. Due to the security vulnerabilities of other versions of SNMP, it is recommended to use SNMPv3.
Type	SNMP Agent devices translate information into a format that can be interpreted by the SNMP manager. The notifications are to the SNMP manager, and are called Trap notifications or Inform requests.

	- Trap: The notifications are sent by the SNMP agent device when a specific parameter is reached by the device and the trap messages can be improper user authentication, CPU usage, link status, and other significant events. This helps the administrator address network issues. - Inform: Inform is only available on SNMPv2 and v3.
Security Level	The security level of SNMP including, - No security: Unsecured SNMP requests - Authentication: Confirmation of the sender's identity and of the timeliness of the request, with the content of the request visible to the network. - Authentication and privacy: With the content of the request encrypted.
Server Port	Enter the server port (1-65535)
Timeout	Set default timeout value.
Retry	Set default retry number.
Log Server	
Server Address	Enter the server address
Server Port	Enter the server port (1-65535)
Facility	The Facility value is a way of determining which process of the machine created the message.
Minimum Severity	The system log SNMP severity command sets the minimum severity level of log events sent as SNMP traps. Log events of lower severity are not sent.
Password Settings	
Password	Configure the password that will be used to restrict access to the device via the Web UI.
Confirm Password	Confirm the password that will be used to restrict access to the device via the Web UI.

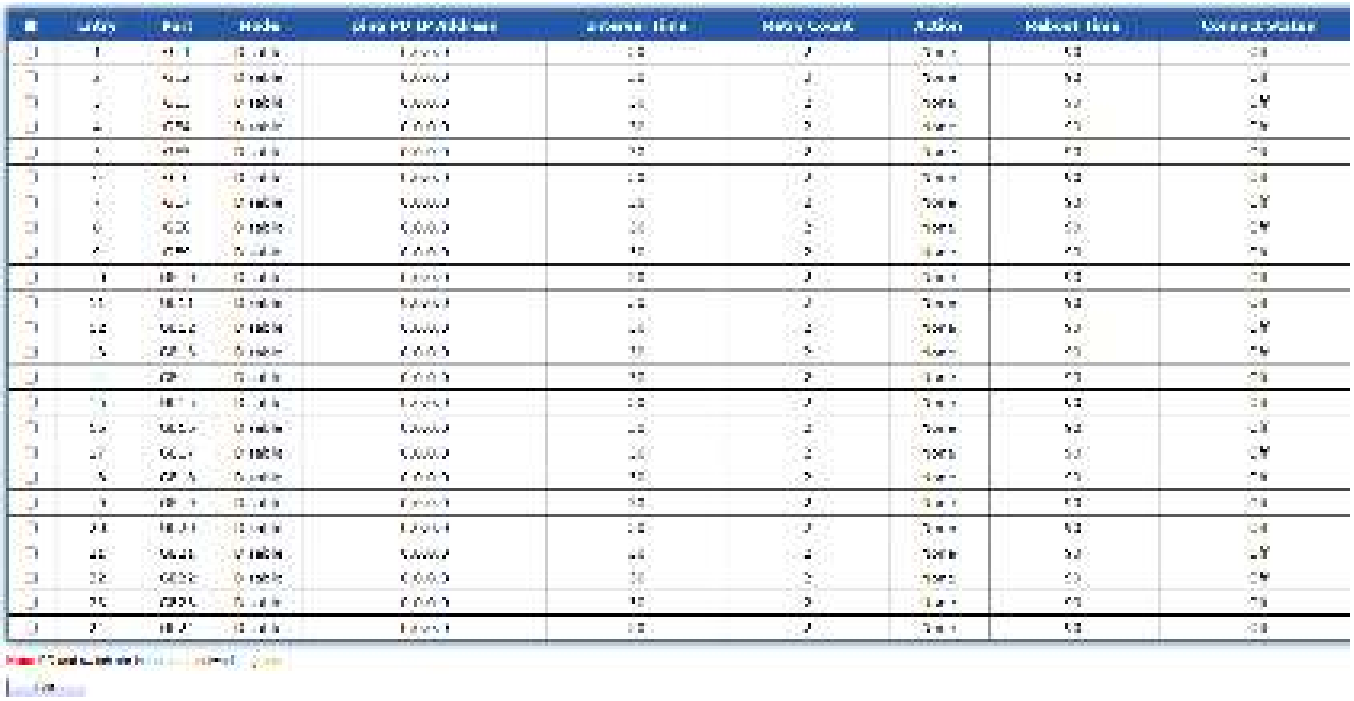
V-5 Mail Alert

SMTP stands for Simple Mail Transfer Protocol. It handles the sending of emails. The ability to support email services. This allows the user to send outgoing mail and retrieve incoming mail, respectively.

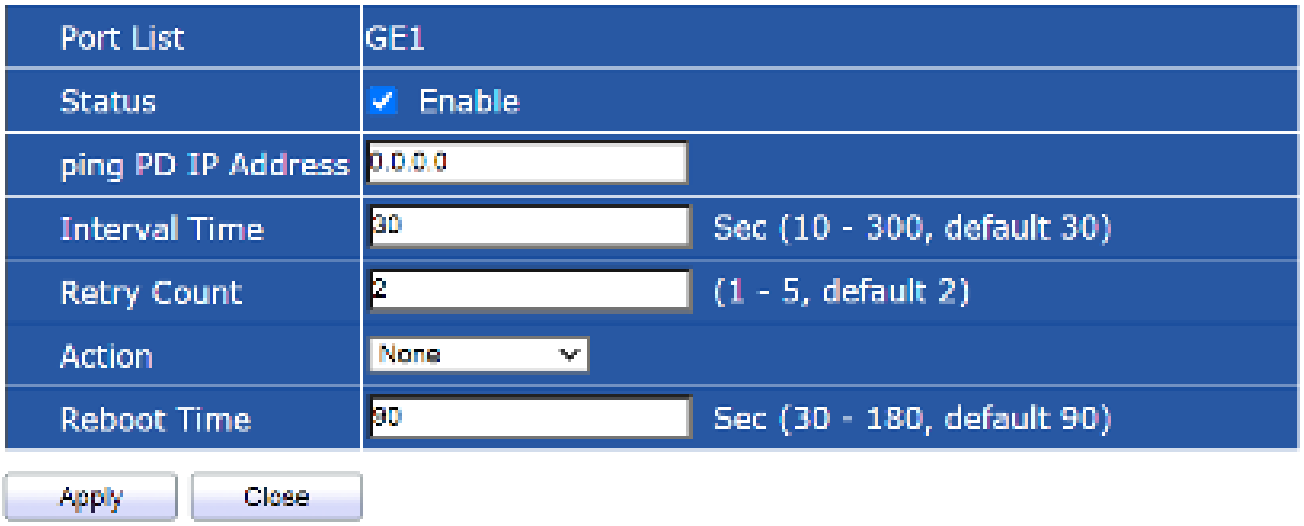


Item	Description
State	Enable or disable.
SMTP Server	This is the domain name or IP address of your external e-mail serve.
SMTP Port	This is the port used by your e-mail provided for sending email.
User Name	This is your username for your email account.
Password	This is the password for your email account.
State	This needs to be enabled if your email provider requires TLS authentication.
Sender	This is your email address.
Receiver	This is the e-mail address of recipient for the SMTP server.
Alert Type	Enable/disable Powered Device Monitor.

V-6 Powered Device Monitor



Click “Edit” to view the Powered Device Monitor page.



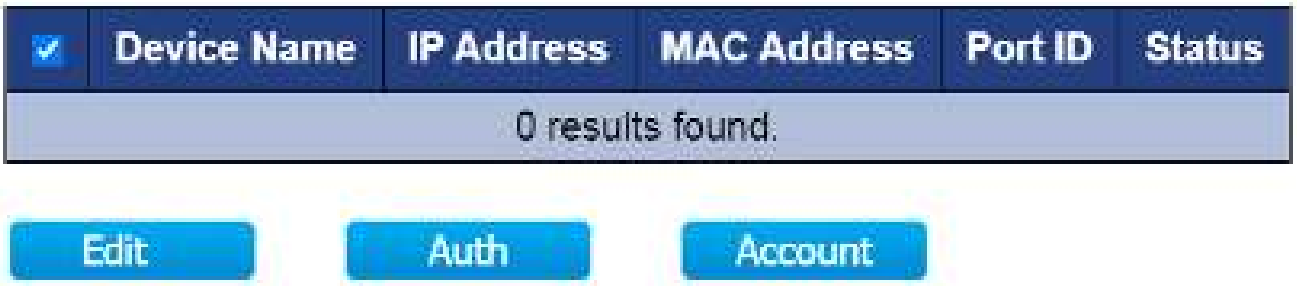
Item	Description
Status	Enable/Disable
ping PD IP Address	Input IP address of the PD
Interval Time	The default setting about Interval (30 seconds) will make switch detect the PD status by performing ping requests every 30 seconds.
Retry Count	If there is no ping reply from the PD, retry count starts to count from 1. Once retry count is reached to 2 times, the switch will perform the action in which you defined.
Action	The Action including none, PD reboot, Reboot & Alarm and Alarm
Reboot Time	Set the reboot time from 30-180 seconds (default is 90 seconds)

V-7 ONVIF

The ONVIF page including two sections,
- IPC Discover
- NVR Discover

V-7-1 IPC Discover

It shows the information of device name, IP address, Mac address, port ID and status of IPC.



V-7-2 NVR Discover

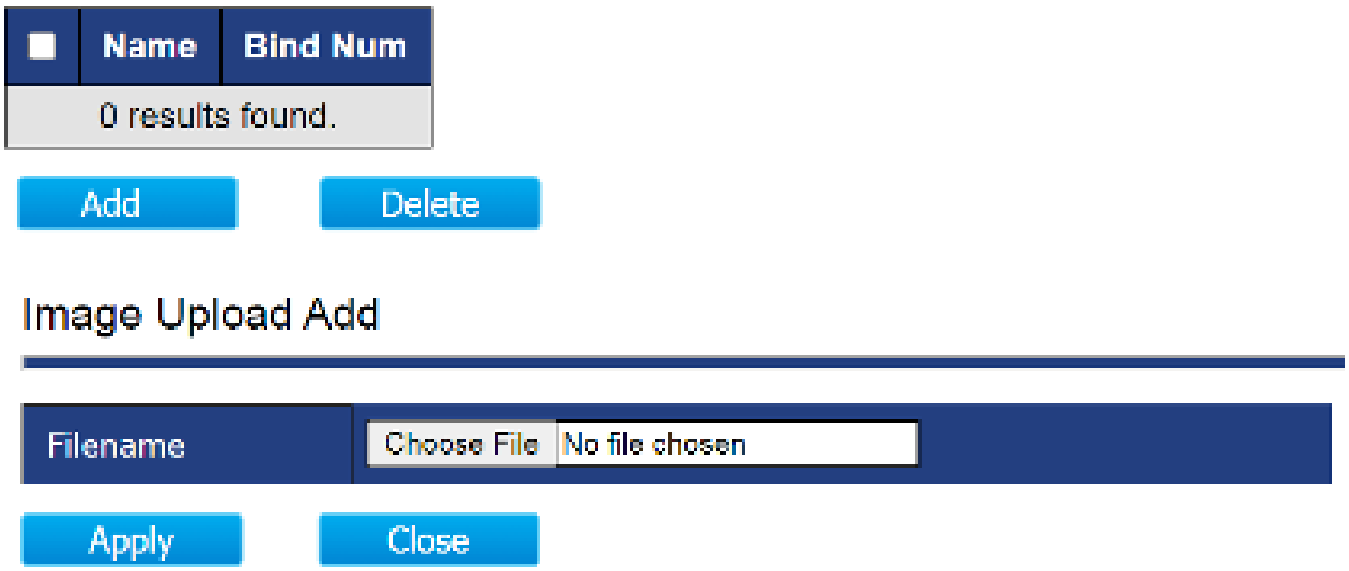
It shows the information of device name, IP address, Mac address, port ID, group ID and group number of NVR.

V-8 E-map Management

The E-map management will allow you to import a layout of your building to graphically layout your switches.

V-8-1 Image Upload

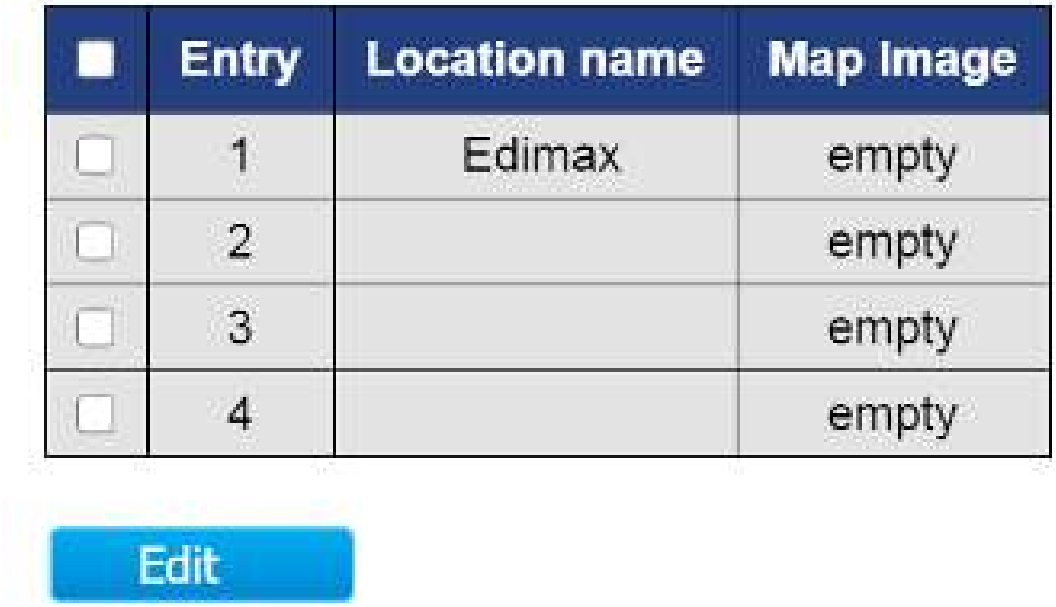
In this page you can upload the image for your E-map.



NOTE: Images are automatically scaled when uploaded. The image formats are JPG and PNG. Maximum file size for images is 1.5MB. The recommended resolution for images is 1024 x 768 pixels.

V-8-2 Image Settings

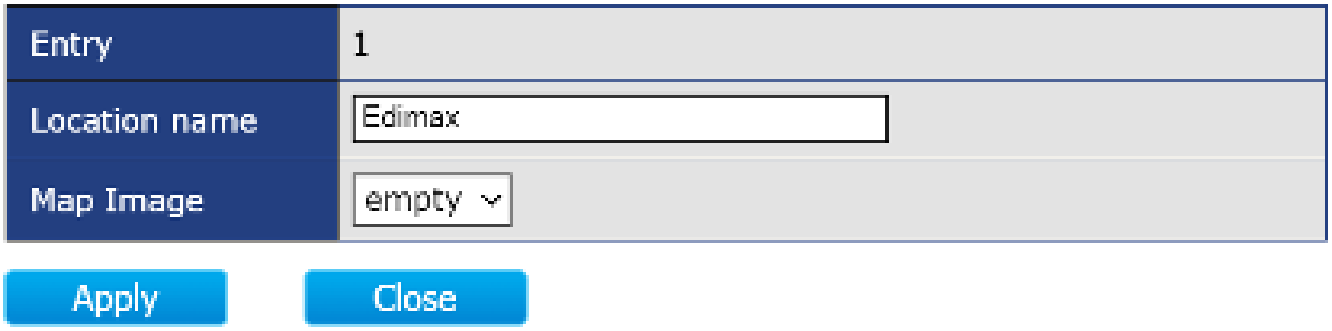
In this page you can view and edit the location name.



	Entry	Location name	Map Image
☐	1	Edimax	empty
☐	2		empty
☐	3		empty
☐	4		empty

Edit

Click the Edit button to view the Image Setting page,

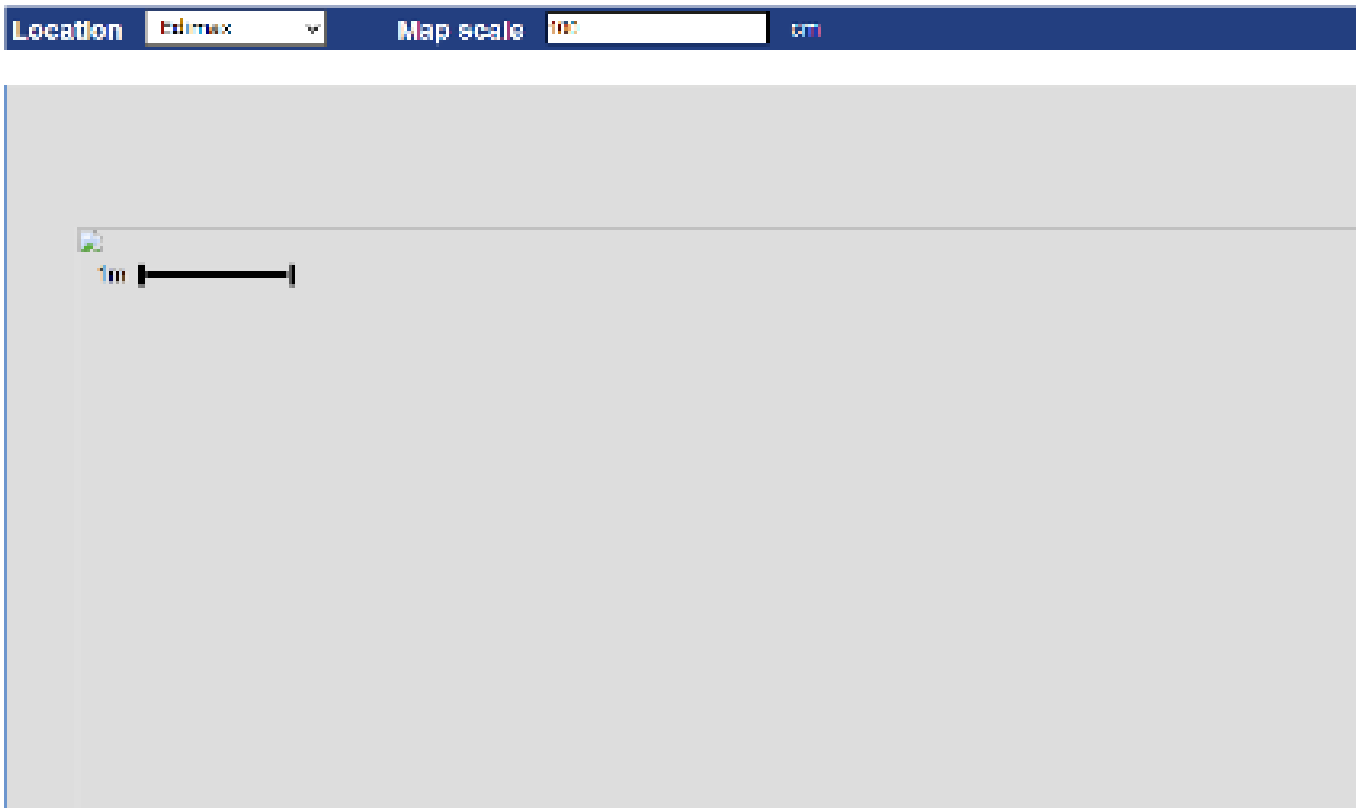


Entry	1
Location name	Edimax
Map Image	empty

Apply Close

V-8-3 E-map View

You can view E-Maps of multiple locations.



V-9 Tools

In this section you can check if you have the latest version on your switch or backup/restore the configuration etc…

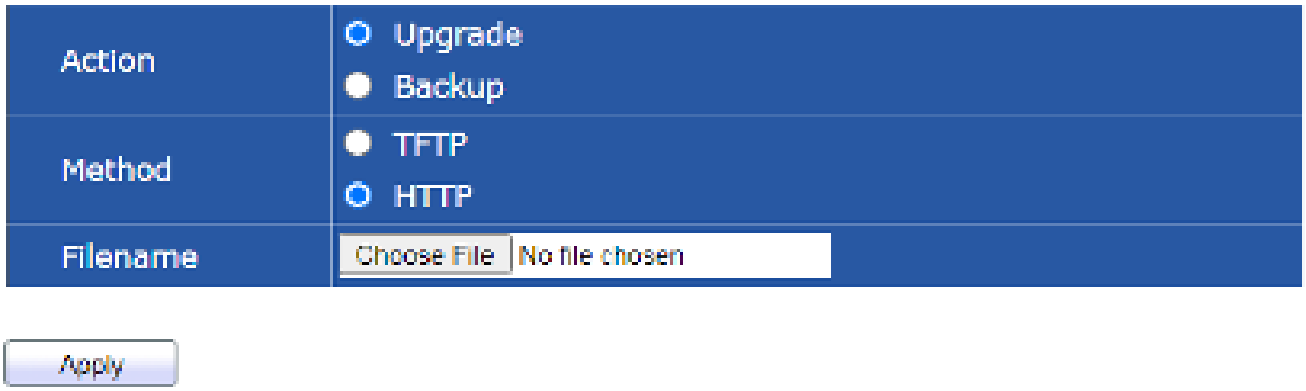
V-9-1 Firmware Information

In this page you can check the firmware version, size or update time.

Version	1.0.3
Size(Byte)	9761472
Update Time	Aug 22 2020 - 14:36:05

V-9-2 Firmware Upgrade & Backup

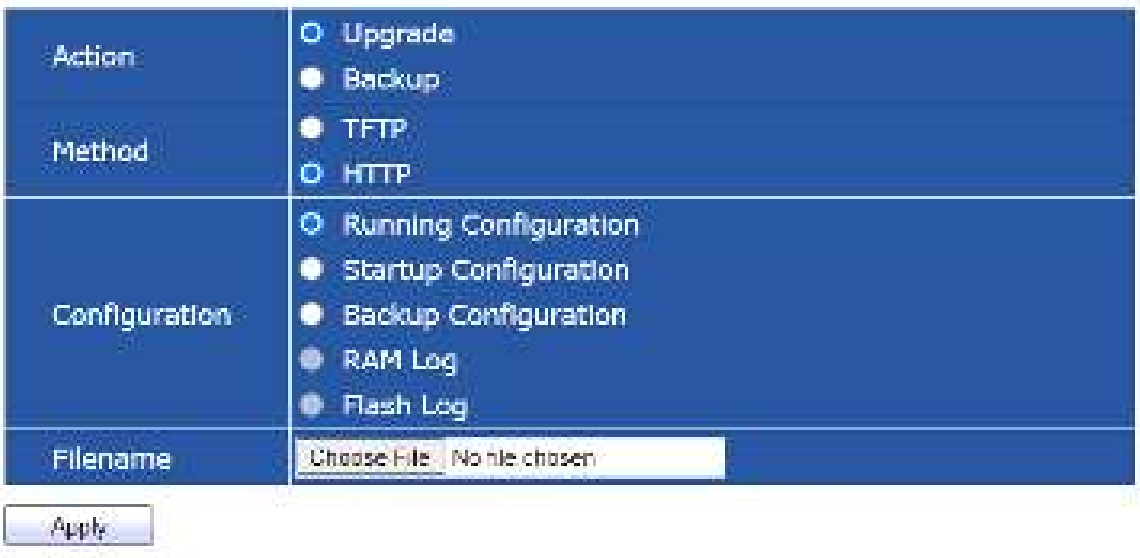
Firmware upgrades can be done via either Trivial FileTransfer Protocol (TFTP) or Hypertext Transfer Protocol/with Secure Sockets (HTTP/HTTPS).



Item	Description
TFTP	TFTP is an unsecure file transfer protocol typically used to distribute software upgrades and configuration files. When using the TFTP client, the file will be downloaded from a TFTP server on your network.
HTTP	HTTP is an application protocol that runs on top of the TCP/IP suite of protocols (the foundation protocols for the Internet)

V-9-3 Configuration Restore & Backup

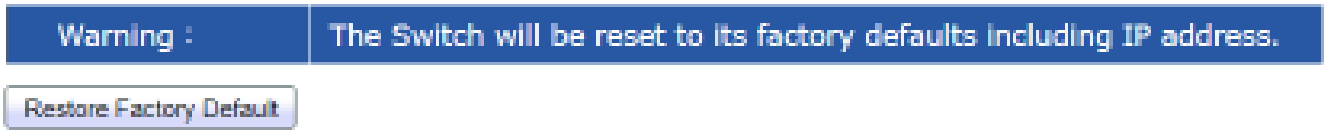
You can restore or backup the configuration from HTTP/TFTP in this page.



Item	Description
TFTP	TFTP is an unsecure file transfer protocol typically used to distribute software upgrades and configuration files. When using the TFTP client, the file will be downloaded from a TFTP server on your network.
HTTP	HTTP is an application protocol that runs on top of the TCP/IP suite of protocols (the foundation protocols for the Internet)

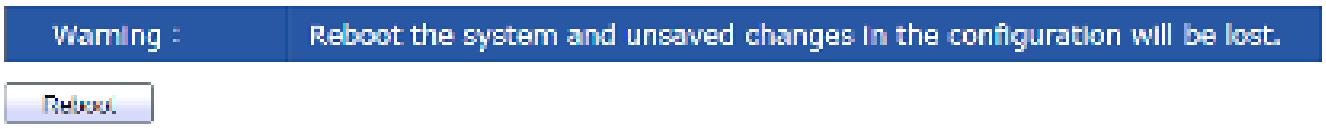
V-9-4 Reset

This page allows users to restore the switch to factory default.



V-9-5 Reboot System

You can reboot the switch via the web UI.



COPYRIGHT

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 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 radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules. This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and consider removing the no-collocation statement.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) this device may not cause harmful interference, and
(2) this device must accept any interference received, including interference that may cause undesired operation.

Caution!

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 2014/30/EU OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE). The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Bulgaria, Cyprus, Czech, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Turkey, and United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not Intended for Use

None

EU Declaration of Conformity

English: This equipment is in compliance with the essential requirements and other relevant provisions of Directive 2014/30/EU.

Français: Cet équipement est conforme aux exigences essentielles et autres dispositions de la directive 2014/30/EU.

Čeština: Toto zařízení je v souladu se základními požadavky a ostatními příslušnými ustanoveními směrnic 2014/30/EU.

Polski: Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE 2014/30/EU.

Română: Acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 2014/30/EU.

Русский: Это оборудование соответствует основным требованиям и положениям Директивы 2014/30/EU.

Magyar: Ez a berendezés megfelel az alapvető követelményeknek és más vonatkozó irányelveknek (2014/30/EU).

Türkçe: Bu cihaz 2014/30/EU. direktifleri zorunlu istekler ve diğer hükümlerle ile uyumludur.

Українська: Обладнання відповідає вимогам і умовам директиви 2014/30/EU.

Slovenčina: Toto zariadenie spĺňa základné požiadavky a ďalšie príslušné ustanovenia smerníc 2014/30/EU.

Deutsch: Dieses Gerät erfüllt die Voraussetzungen gemäß den Richtlinien 2014/30/EU.

Español: El presente equipo cumple los requisitos esenciales de la Directiva 2014/30/EU.

Italiano: Questo apparecchio è conforme ai requisiti essenziali e alle altre disposizioni applicabili della Direttiva 2014/30/EU.

Nederlands: Dit apparaat voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van richtlijn 2014/30/EU.

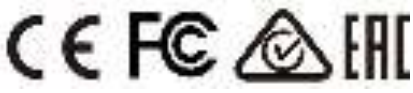
Português: Este equipamento cumpre os requesitos essênciais da Directiva 2014/30/EU.

Norsk: Dette utstyret er i samsvar med de viktigste kravene og andre relevante regler i Direktiv 2014/30/EU.

Svenska: Denna utrustning är i överensstämmelse med de väsentliga kraven och övriga relevanta bestämmelser i direktiv 2014/30/EU.

Dansk: Dette udstyr er i overensstemmelse med de væsentligste krav og andre relevante forordninger i direktiv 2014/30/EU.

suomen kieli: Tämä laite täyttää direktiivien 2014/30/EU. oleelliset vaatimukset ja muut asiaankuuluvat määräykset.



WEEE Directive & Product Disposal

At the end of its serviceable life, this product should not be treated as household or general waste. It should be handed over to the applicable collection point for the recycling of electrical and electronic equipment, or returned to the supplier for disposal.

Declaration of Conformity

We, Edimax Technology Co., Ltd., declare under our sole responsibility, that the equipment described below complies with the requirements of the European R&TTE directives.

Equipment: 24-Port Gigabit PoE, Long rang, 10GbE uplinks Switch
Model No.: GS-5424PLX

The following European standards for essential requirements have been followed:

Directives 2014/30/EU

EMC : EN 55032:2015+AC:2016
EN 61000-3-2:2014 Class A
EN 61000-3-3:2013
EN 55035:2017

Safety (LVD) : EN 62368-1:2014+A11:2017

Edimax Technology Europe B.V.
Fijenhof 2,
5652 AE Eindhoven,
The Netherlands

a company of :
Edimax Technology Co., Ltd.
No. 278, Xinhu 1st Rd.,
Neihu Dist., Taipei City,
Taiwan

Signature:

Printed Name: David Huang
Title: Director
Edimax Technology Europe B.V.

CE

Date of Signature: Sep., 2020
Signature:

Printed Name: Albert Chang
Title: Director
Edimax Technology Co., Ltd.

Notice According to GNU General Public License Version 2

This product includes software that is subject to the GNU General Public License version 2. The program is free software and distributed without any warranty of the author. We offer, valid for at least three years, to give you, for a charge no more than the costs of physically performing source distribution, a complete machine-readable copy of the corresponding source code.

Das Produkt beinhaltet Software, die den Bedingungen der GNU/GPL-Version 2 unterliegt. Das Programm ist eine sog. „Free Software“, der Autor stellt das Programm ohne irgendeine Gewährleistungen zur Verfügung. Wir bieten Ihnen für einen Zeitraum von drei Jahren an, eine vollständige maschinenlesbare Kopie des Quelltextes der Programme zur Verfügung zu stellen – zu nicht höheren Kosten als denen, die durch den physikalischen Kopiervorgang anfallen.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation’s software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author’s protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors’ reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone’s free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The ‘“Program’“, below, refers to any such program or work, and a ‘“work based on the Program’“ means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term ‘“modification’“.) Each licensee is addressed as ‘“you’“.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program’s source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep

intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and '"any later version'", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM '"AS IS'" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.