DIGISOL
DG-GS1512HP
12 Port Giga Smart Switch with 8 Giga PoE ports & 4 Giga Combo Ports

DG-GS1512HP

8 Port Giga PoE Ethernet WEB Smart Switch with 4 SFP Ports

User Manual

V1.0

2018-05-31

As our products undergo continuous development the specifications are subject to change without prior notice

COPYRIGHT

TRADEMARK

Table of Contents

Safety and Regulatory

Audience

This guide is for the networking professional managing the standalone DG-GS1512HP switch series. It is recommended that only professionals with experience working with networking devices who are familiar with the Ethernet and local area networking terminology, should service the equipment.

Conventions

The following conventions are used in this manual to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in boldface text.
- Arguments for which you supply values are in italic.
- Square brackets ([ ]) mean optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:

- Non printing characters, such as passwords or tabs, are in angle brackets (< >). Notes and cautions use the following conventions and symbols:

Note

Means additional information. Notes contain additional useful information or references to material available outside of this document.

Caution

Indicates that the reader must be careful. In a situation where a Caution is listed, a user may cause equipment damage or loss of data.

1. Introduction

Thank you for choosing a Digisol (PoE) WEB Smart Ethernet Switch. This device is designed to be operational right out-of-the-box as a standard bridge. In the default configuration, it will forward packets between connecting devices after powered up.

Before you begin installing the switch, make sure you have all of the package contents available, and a PC with a web browser for using web-based system management tools.

1.1. Overview

The Digisol DG-GS1512HP is a WEB Smart PoE switch with 8 Gigabit PoE+ ports + 4 SFP Ports respectively.

1.2. Package contents

Before using the product, check that the items listed below are included and in good condition. If any item does not accord with the table, please contact your dealer immediately.

- Digisol DG-GS1512HP WEB Smart PoE Switch
- Power Cord
- Manual CD
- Rack Mount Kit
- Foot pads
- QIG

1.3. Features

- Supports up to 12 10/100/1000Mbps Gigabit Ethernet ports and 4 SFP slots
- IEEE 802.3af/at PoE compliant to simplify deployment and installation
- Supports PoE up to 30W per port with 140W total power budget
- Automatically detects powered devices (PD) and power consumption levels

- IEEE 802.1Q VLAN allows network segmentation to enhance performance and security
- Supports Access Control List (ACL)
- Switch capacity: DG-GS1512HP: 24Gbps, Forwarding rate: 41.6Mpps
- Supports IGMP Snooping V1 / V2 / V3
- 8K MAC address table and 10K jumbo frames
- 19-inch rack-mountable metal case

1.4. Product Components

1.4.1. Ports

The following view applies to DG-GS1512HP.

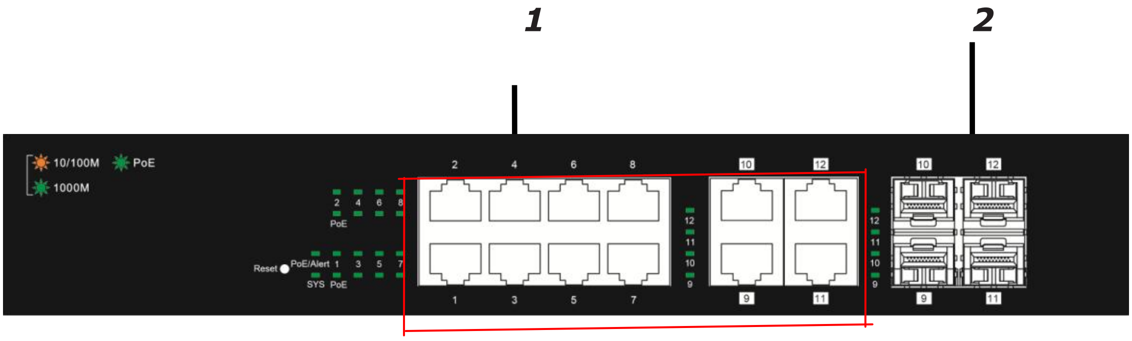


Figure 1 - Front View

No.	Name	Description
1	10/100/1000Mbps RJ-45 ports (1~12)	Designed to connect to network devices with a bandwidth of 10Mbps, 100Mbps or 1000Mbps. Each has a corresponding 10/100/1000Mbps LED.
2	SFP ports (SFP1, SFP2, SFP3, and SFP4)	Designed to install SFP modules and connect to network devices with a bandwidth of 1000Mbps. Each has a corresponding 1000Mbps LED.

The following view applies to DG-GS1512HP.

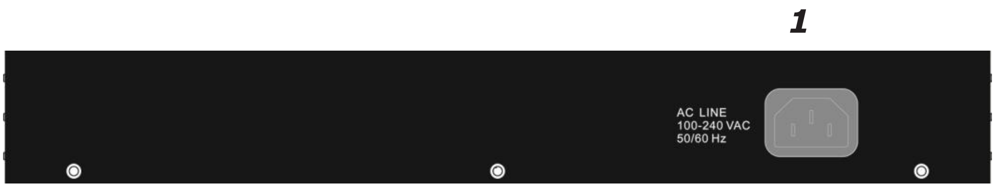


Figure 2 - Rear View

No.	Name	Description
1	AC power in	Supports AC 100 – 240V, 50-60Hz.

1.4.2. LED Indicators

The following view applies to DG-GS1512HP.

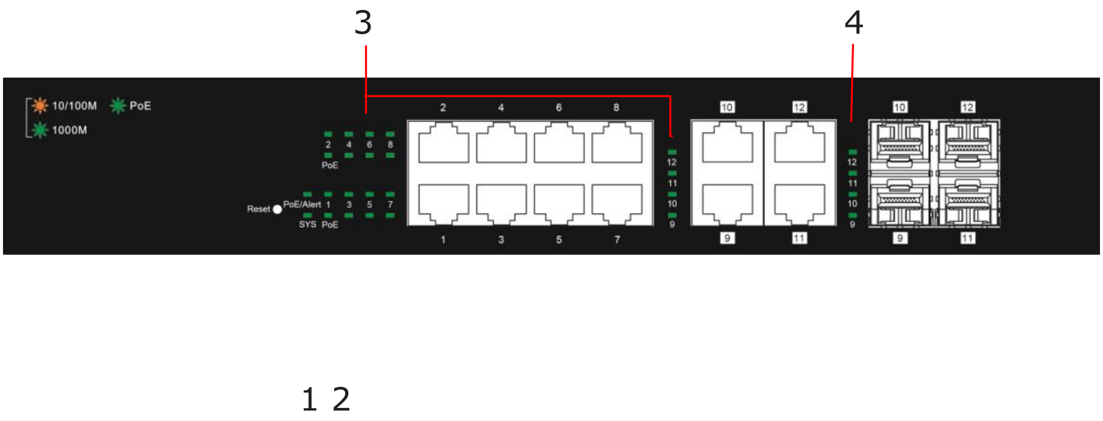


Figure 3 - Front View LED Indicators

No.	Name	Description
1	System	• Off: system not ready • On: system ready Blinking: system boot-up

2	Power	• Off: power off • On: power on
3	Port LED	LINK/ACT bi-color LED: • Off: port disconnected or link fail • Green on: 1000Mbps connected, PoE power output on • Amber on: 10/100Mbps connected • Blinking: sending or receiving data
4	SFP LED	• Off: port disconnected or link fail • Green on: 1000Mbps connected

2. Installation

This chapter describes how to install and connect your DG-GS1512HP Switch. Read the following topics and perform the procedures in the correct order. Incorrect installation may cause damage to the product.

2.1. 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).

2.1.1. 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.

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

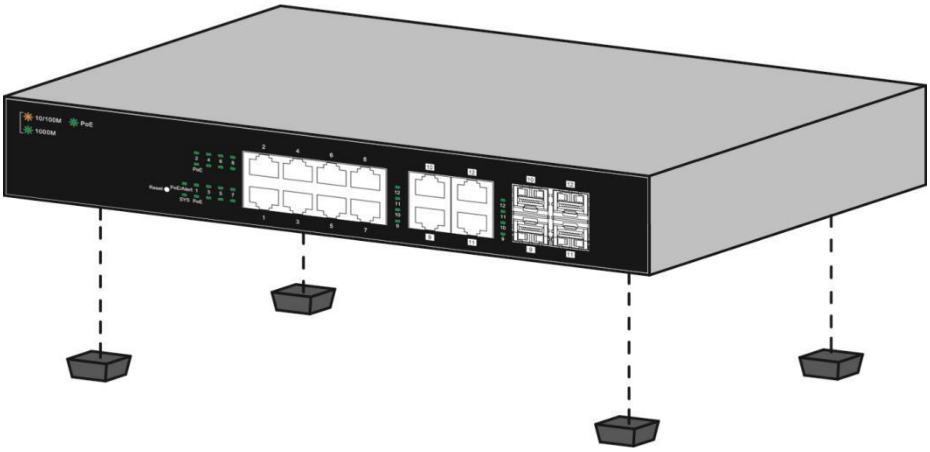


Figure 4 - Desktop Installation

2.1.2. 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.

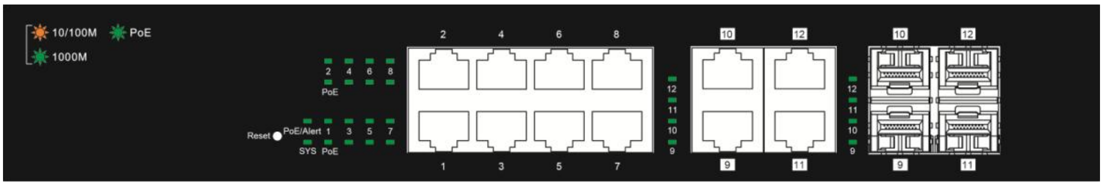


Figure 5 - Bracket Installation

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

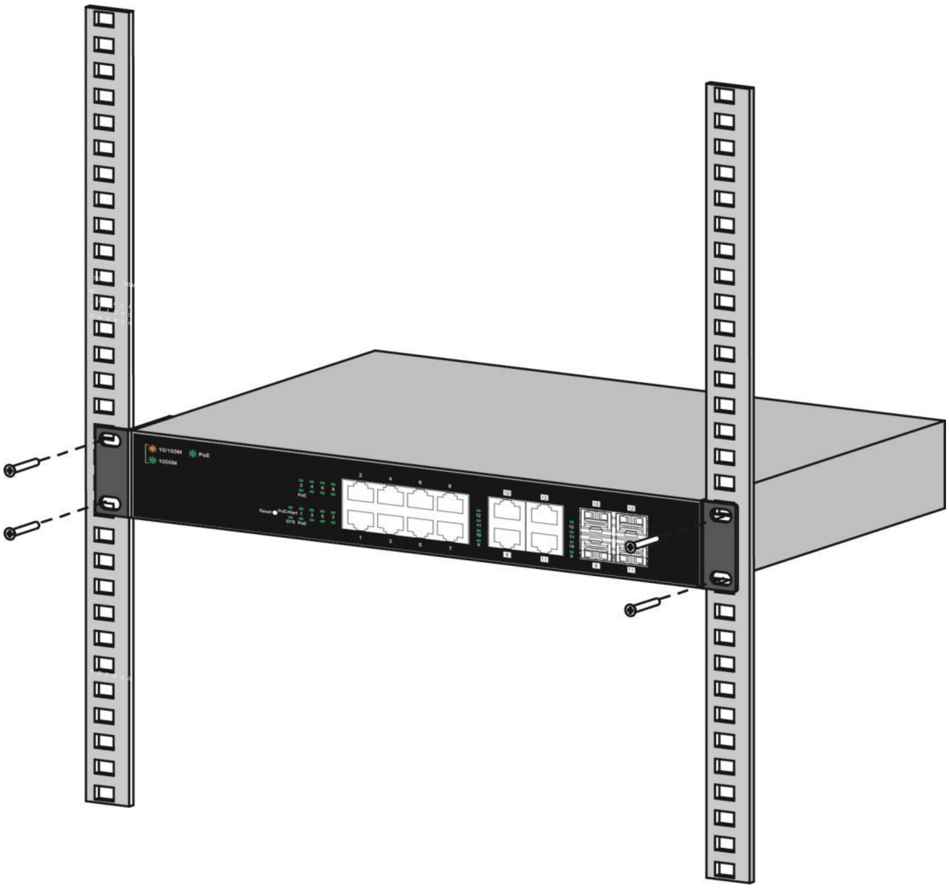


Figure 6 - Rack Installation

3. 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

3.1. Power

3.1.1. 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.

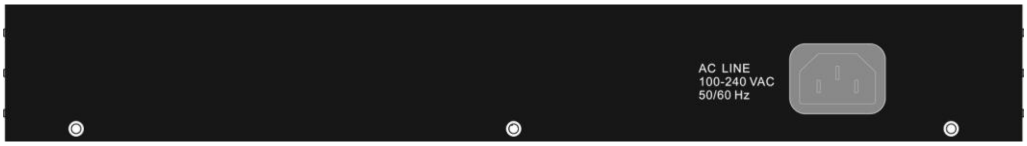


Figure 7 - Rear View AC Power Socket

3.1.2. Connecting to the 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.

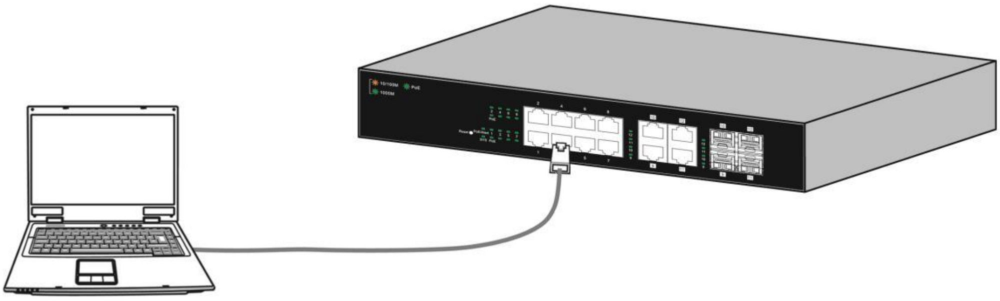


Figure 8 - PC Connect

3.1.3. 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 Ports	PoE Standard Supported
DG-GS1512HP	140W	1 to 8	IEEE802.3at/af

Ports 1-8 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.

3.1.4. 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 192.168.1.10) 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: 192.168.1.x (whereas x is a number from 2 to 254).

After a successful connection, the login window displays.

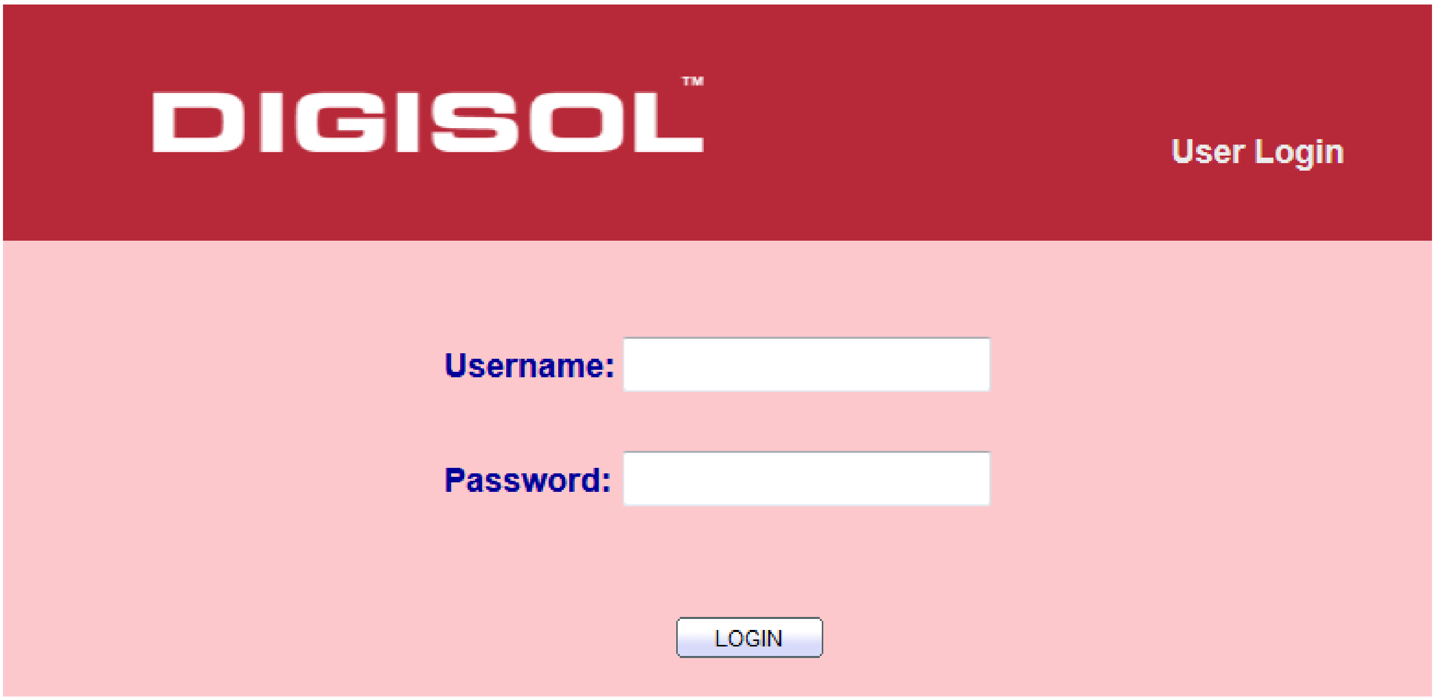


Figure 9 - Login Window

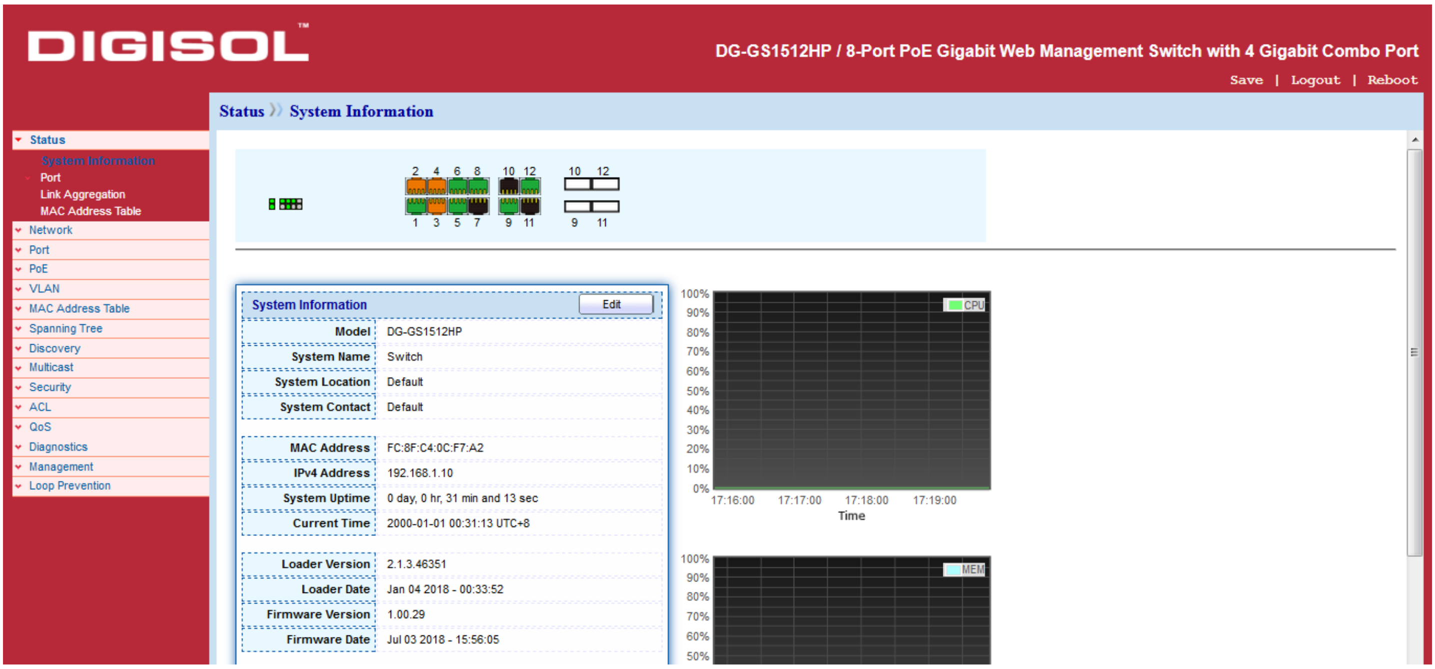
3.1.5. Logging In

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.

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



DG-GS1512HP / 8-Port PoE Gigabit Web Management Switch with 4 Gigabit Combo Port

Status » System Information

System Information

Model	DG-GS1512HP
System Name	Switch
System Location	Default
System Contact	Default
MAC Address	FC:8F:C4:0C:F7:A2
IPv4 Address	192.168.1.10
System Uptime	0 day, 0 hr, 31 min and 13 sec
Current Time	2000-01-01 00:31:13 UTC+8
Loader Version	2.1.3.46351
Loader Date	Jan 04 2018 - 00:33:52
Firmware Version	1.00.29
Firmware Date	Jul 03 2018 - 15:56:05

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.

Logging Out

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

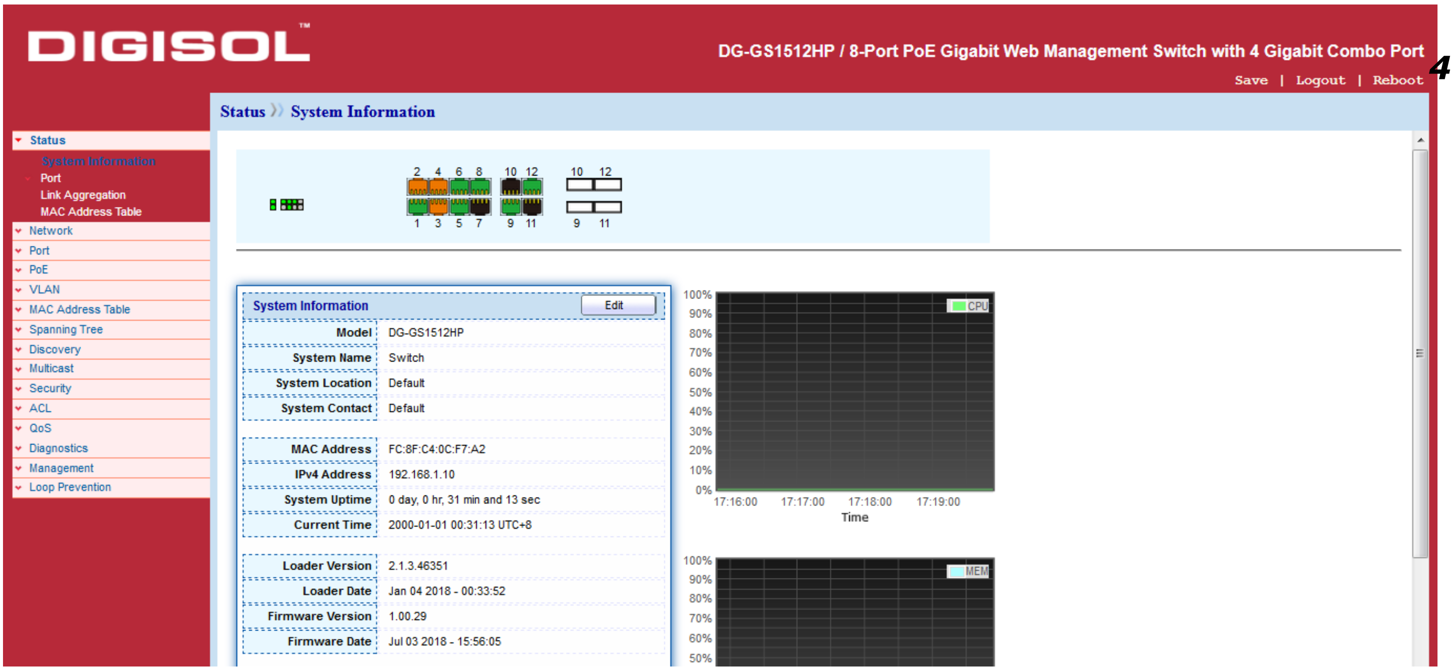
To logout, click Logout in the top right corner of any page. The system logs out of the device.

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.

4. 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:



Status » System Information

System Information

Model	DG-GS1512HP
System Name	Switch
System Location	Default
System Contact	Default
MAC Address	FC:8F:C4:0C:F7:A2
IPv4 Address	192.168.1.10
System Uptime	0 day, 0 hr, 31 min and 13 sec
Current Time	2000-01-01 00:31:13 UTC+8
Loader Version	2.1.3.46351
Loader Date	Jan 04 2018 - 00:33:52
Firmware Version	1.00.29
Firmware Date	Jul 03 2018 - 15:56:05

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.

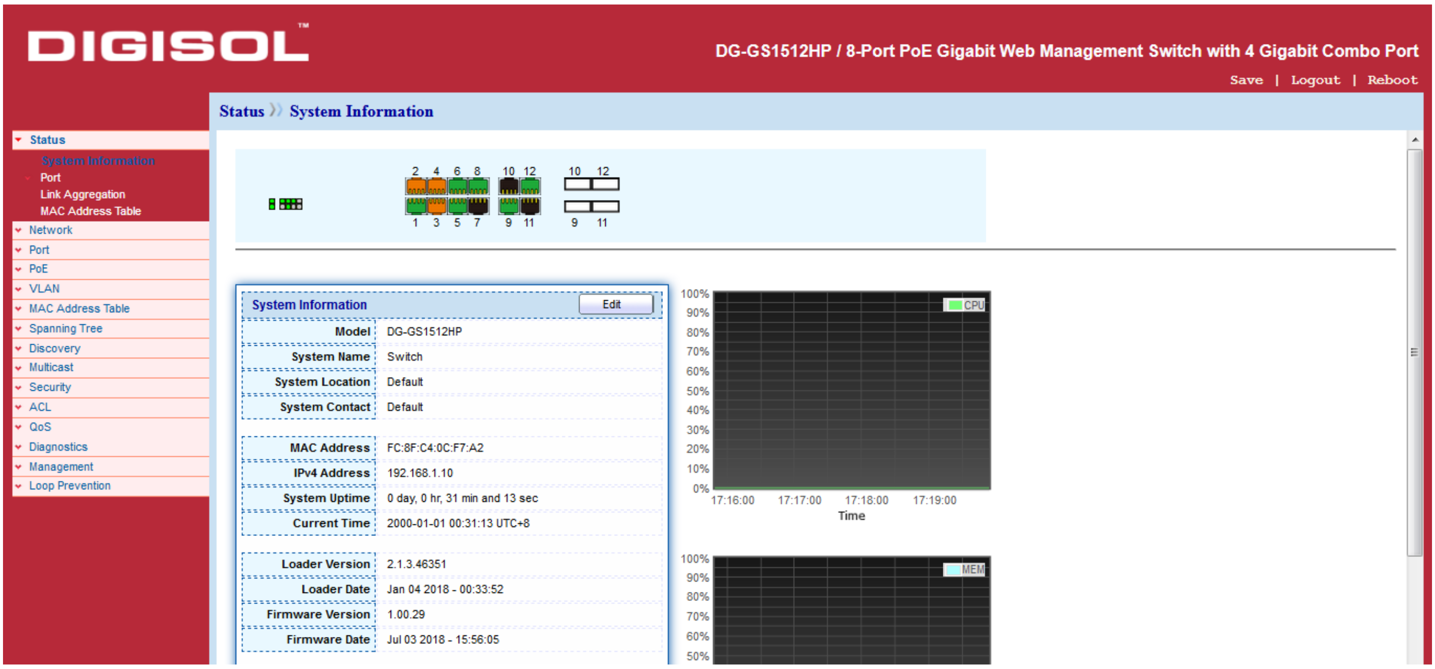
4.1. Status

Use the Status pages to view system information and status.

4.1.1. 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**.



Status » System Information

System Information

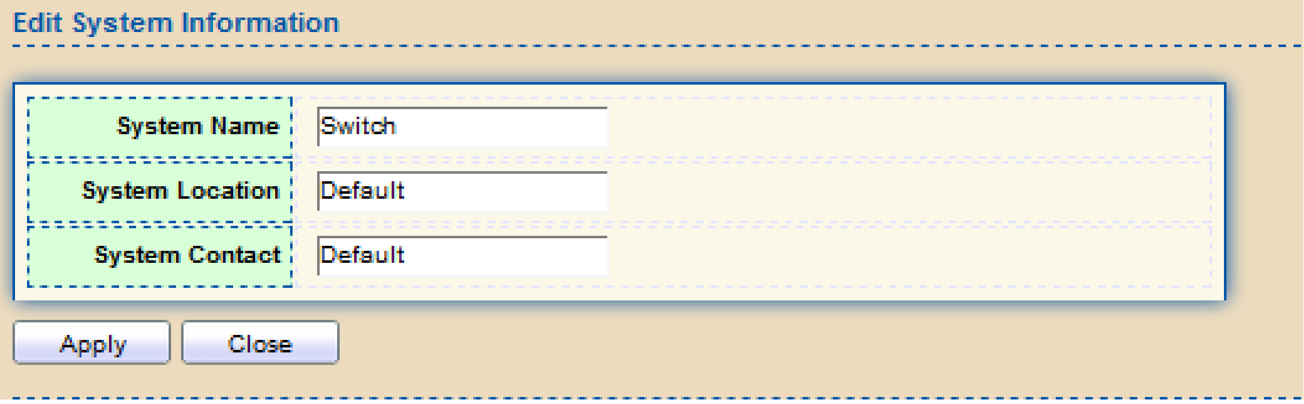
Model	DG-GS1512HP
System Name	Switch
System Location	Default
System Contact	Default
MAC Address	FC:8F:C4:0C:F7:A2
IPv4 Address	192.168.1.10
System Uptime	0 day, 0 hr, 31 min and 13 sec
Current Time	2000-01-01 00:31:13 UTC+8
Loader Version	2.1.3.46351
Loader Date	Jan 04 2018 - 00:33:52
Firmware Version	1.00.29
Firmware Date	Jul 03 2018 - 15:56:05

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.
IPv6 Address	Current system IPv6 address.
System OID	SNMP system object ID.
System Uptime	Total elapsed time from booting.
Current Time	Current system time.
Loader Version	Boot loader image version.
Loader Date	Boot loader image build date.
Firmware Version	Current running firmware image version.
Firmware Date	Current running firmware image build date.
Telnet	Current Telnet service enable/disable state.
SSH	Current SSH service enable/disable state.
HTTP	Current HTTP service enable/disable state.
HTTPS	Current HTTPS service enable/disable state.
SNMP	Current SNMP service enable/disable state.

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



Edit System Information

System Name	Switch
System Location	Default
System Contact	Default

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.

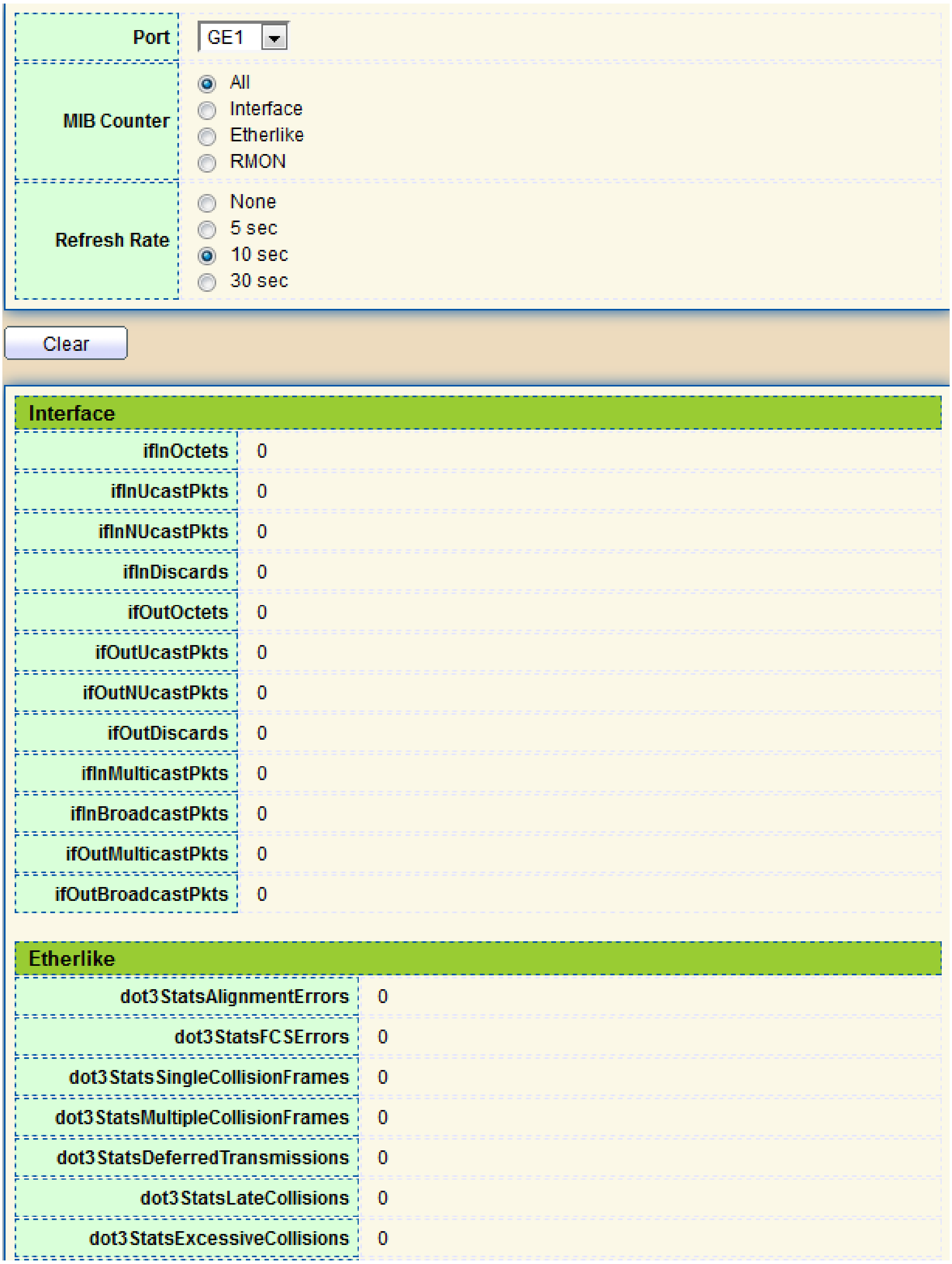
4.1.2. Port

The Port configuration page displays port summary and status information.

4.1.2.1. 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**.



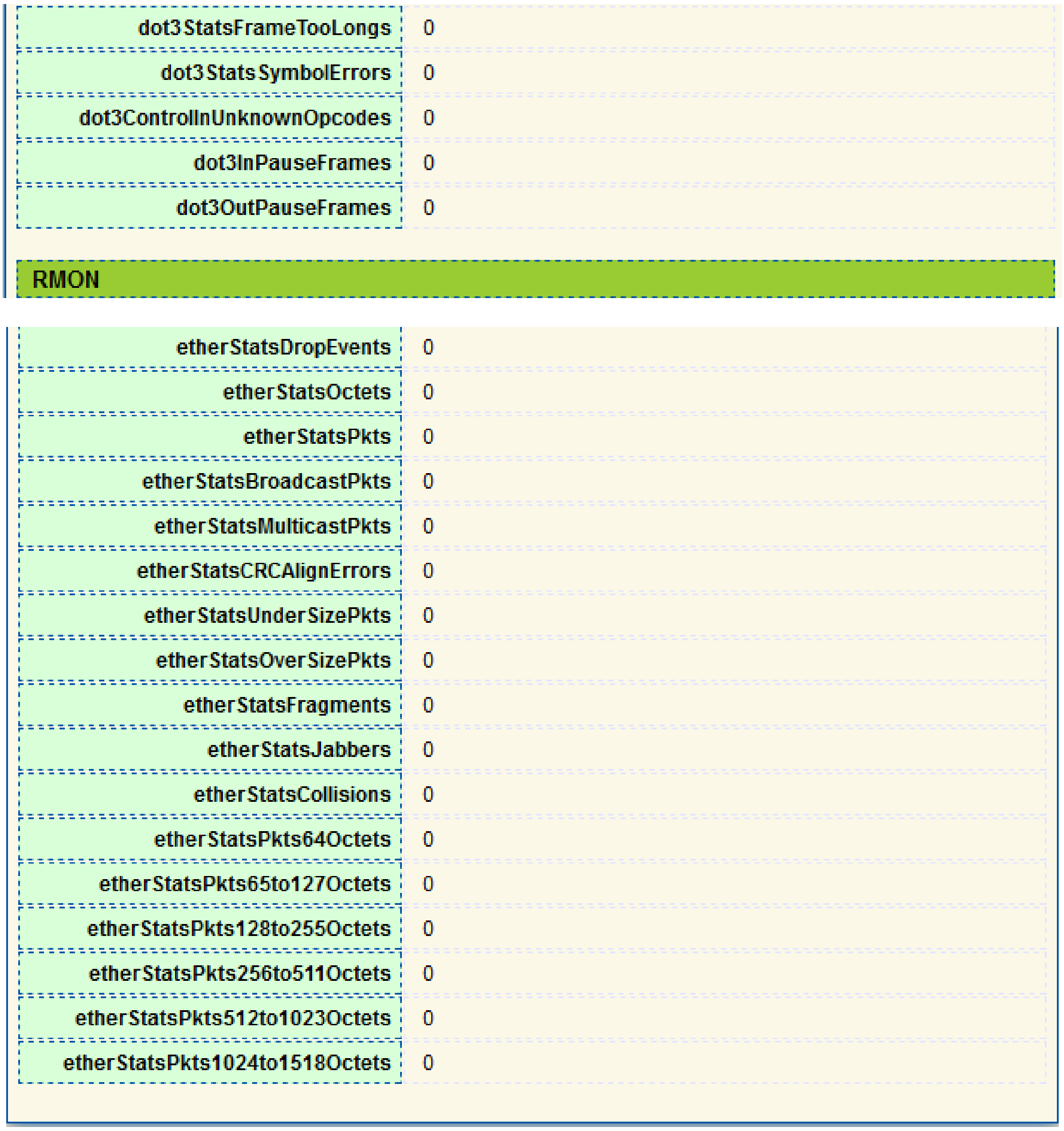
Port	GE1
MIB Counter	● All ○ Interface ○ Etherlike ○ RMON
Refresh Rate	○ None ○ 5 sec ● 10 sec ○ 30 sec

Interface

ifInOctets	0
ifInUcastPkts	0
ifInNUcastPkts	0
ifInDiscards	0
ifOutOctets	0
ifOutUcastPkts	0
ifOutNUcastPkts	0
ifOutDiscards	0
ifInMulticastPkts	0
ifInBroadcastPkts	0
ifOutMulticastPkts	0
ifOutBroadcastPkts	0

Etherlike

dot3StatsAlignmentErrors	0
dot3StatsFCSErrors	0
dot3StatsSingleCollisionFrames	0
dot3StatsMultipleCollisionFrames	0
dot3StatsDeferredTransmissions	0
dot3StatsLateCollisions	0
dot3StatsExcessiveCollisions	0



dot3StatsFrameTooLongs	0
dot3StatsSymbolErrors	0
dot3ControlInUnknownOpcodes	0
dot3InPauseFrames	0
dot3OutPauseFrames	0

RMON

etherStatsDropEvents	0
etherStatsOctets	0
etherStatsPkts	0
etherStatsBroadcastPkts	0
etherStatsMulticastPkts	0
etherStatsCRCAlignErrors	0
etherStatsUnderSizePkts	0
etherStatsOverSizePkts	0
etherStatsFragments	0
etherStatsJabbers	0
etherStatsCollisions	0
etherStatsPkts64Octets	0
etherStatsPkts65to127Octets	0
etherStatsPkts128to255Octets	0
etherStatsPkts256to511Octets	0
etherStatsPkts512to1023Octets	0
etherStatsPkts1024to1518Octets	0

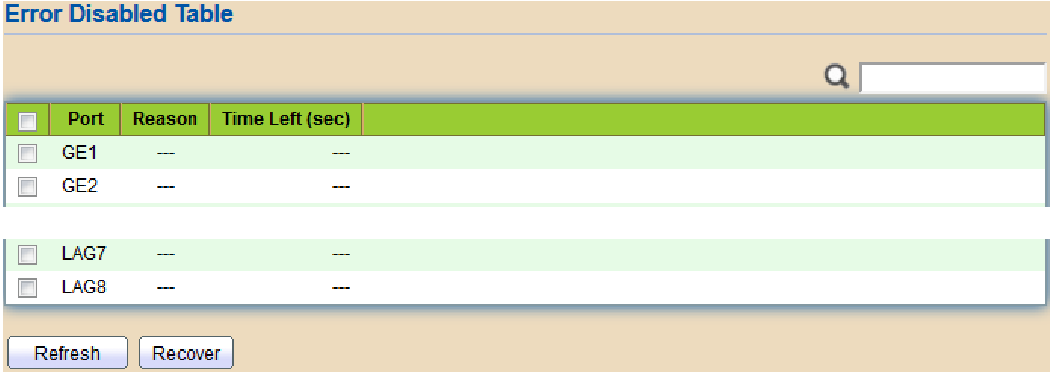
Figure 15 - Status > Port > Statistics

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.

4.1.2.2. Error Disabled

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


Error Disabled Table

□	Port	Reason	Time Left (sec)
□	GE1	---	---
□	GE2	---	---
□	LAG7	---	---
□	LAG8	---	---

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.

4.1.2.3. 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.**

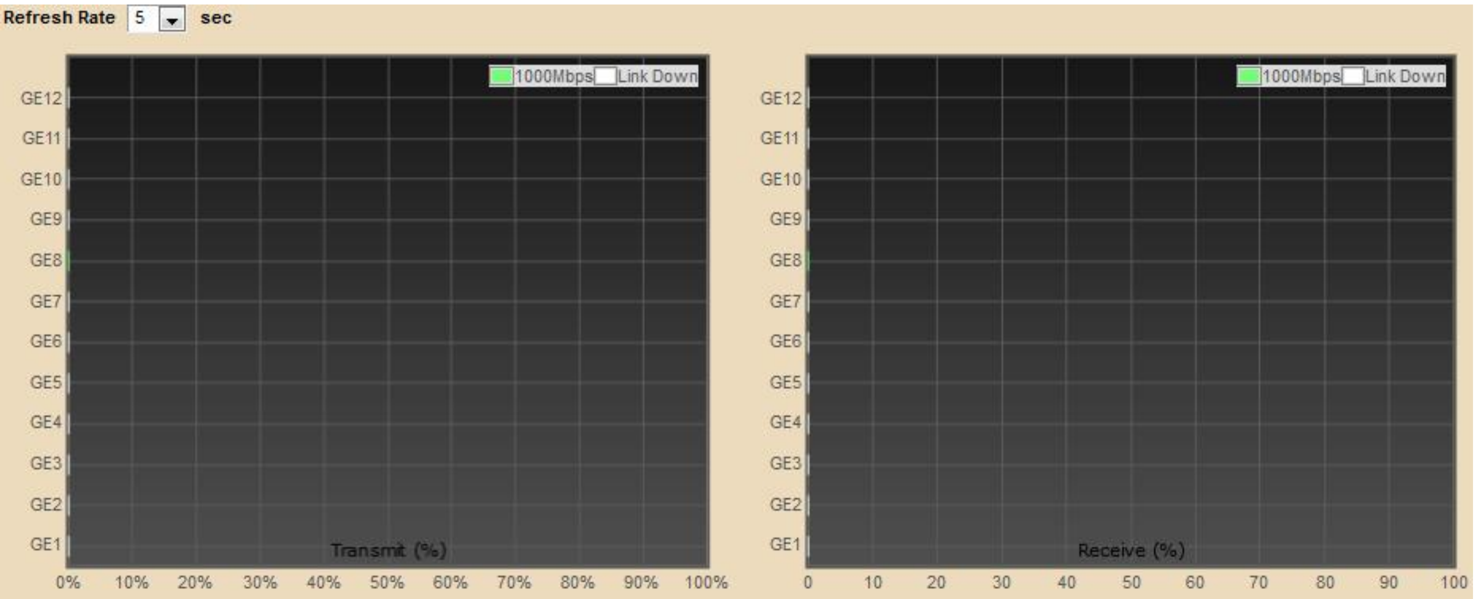
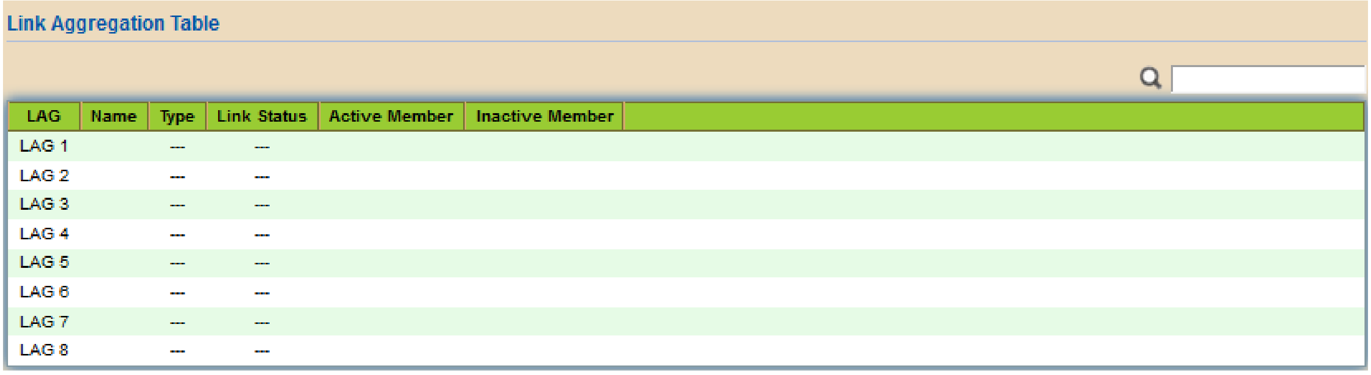

Refresh Rate 5 sec

Figure 17 - Status > Port > Bandwidth Utilization

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

4.1.3. Link Aggregation

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



Link Aggregation Table

LAG	Name	Type	Link Status	Active Member	Inactive Member
LAG 1		---	---		
LAG 2		---	---		
LAG 3		---	---		
LAG 4		---	---		
LAG 5		---	---		
LAG 6		---	---		
LAG 7		---	---		
LAG 8		---	---		

Figure 18 - Status > Link Aggregation

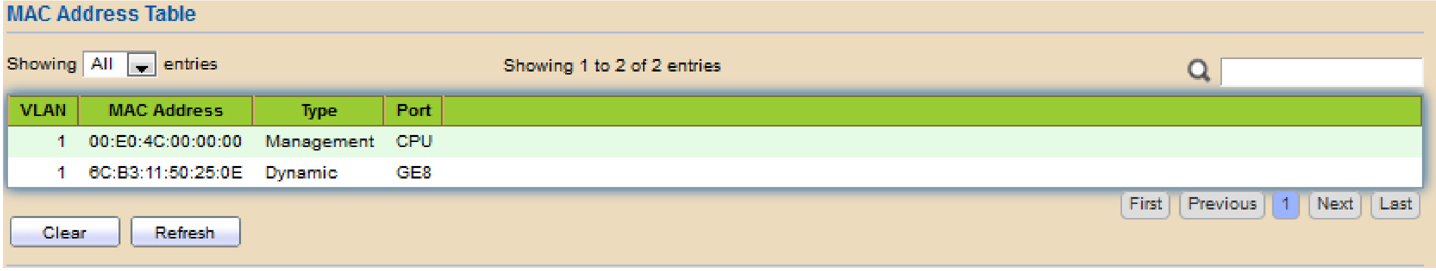
Item	Description
LAG	LAG Name.
Name	LAG port description.
Type	• The type of the LAG. • Static: The group of ports assigned to a static LAG are always active members. • LACP: The group of ports assigned to dynamic LAG are candidate ports. LACP determines which candidate ports are active member ports.

Link Status	LAG port link status.
Active Member	Active member ports of the LAG.
Inactive Member	Inactive member ports of the LAG.

4.1.4. 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**.



MAC Address Table

Showing All entries

Showing 1 to 2 of 2 entries

VLAN	MAC Address	Type	Port
1	00:E0:4C:00:00:00	Management	CPU
1	6C:B3:11:50:25:0E	Dynamic	GE8

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.

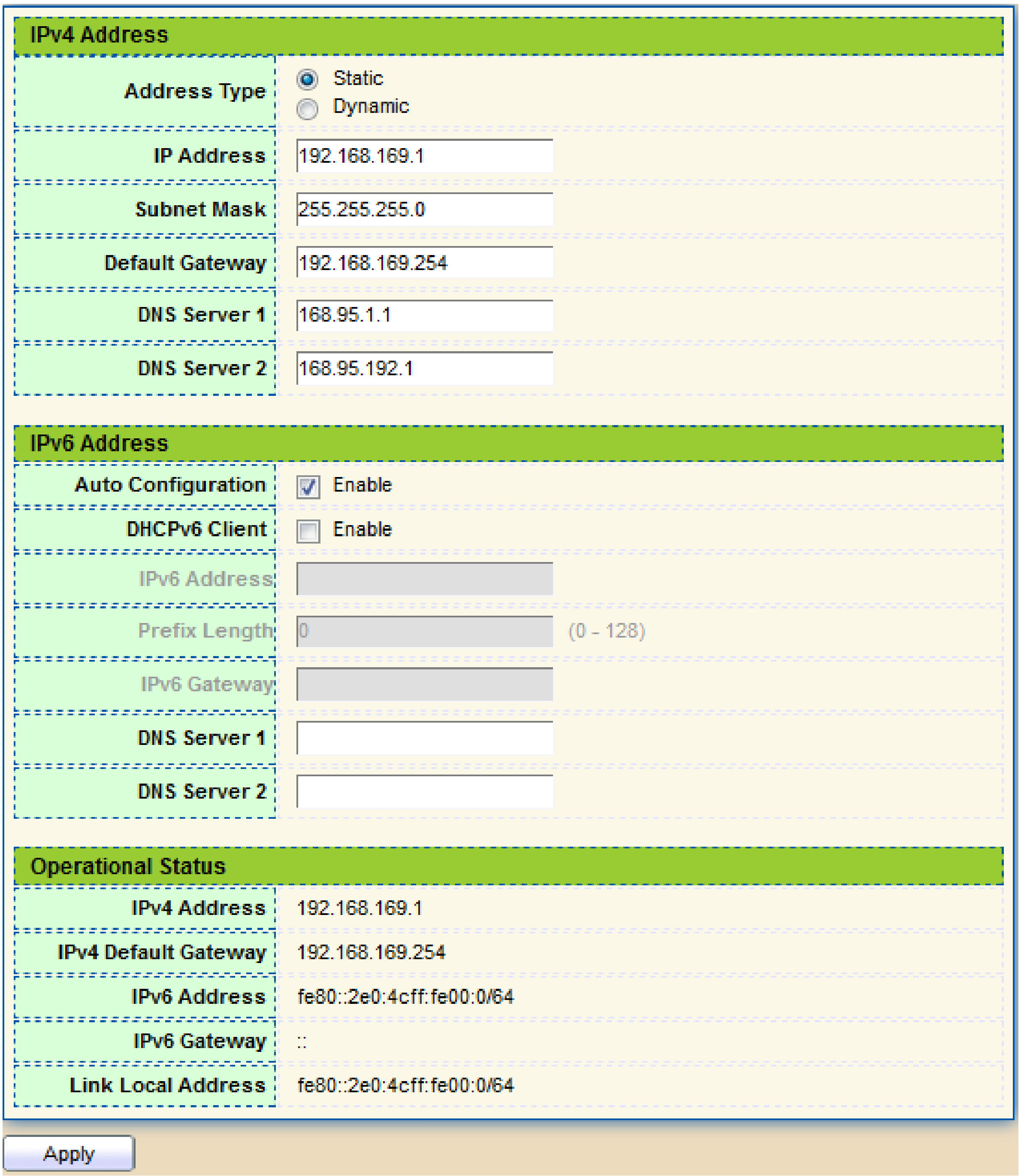
4.2. Network

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

4.2.1. 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**.



IPv4 Address

Address Type	● Static ○ Dynamic
IP Address	192.168.169.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.169.254
DNS Server 1	168.95.1.1
DNS Server 2	168.95.192.1

IPv6 Address

Auto Configuration	☑ Enable
DHCPv6 Client	□ Enable
IPv6 Address	
Prefix Length	0 (0 - 128)
IPv6 Gateway	
DNS Server 1	
DNS Server 2	

Operational Status

IPv4 Address	192.168.169.1
IPv4 Default Gateway	192.168.169.254
IPv6 Address	fe80::2e0:4cff:fe00:0/64
IPv6 Gateway	::
Link Local Address	fe80::2e0:4cff:fe00:0/64

Figure 20 - Network > IP Address

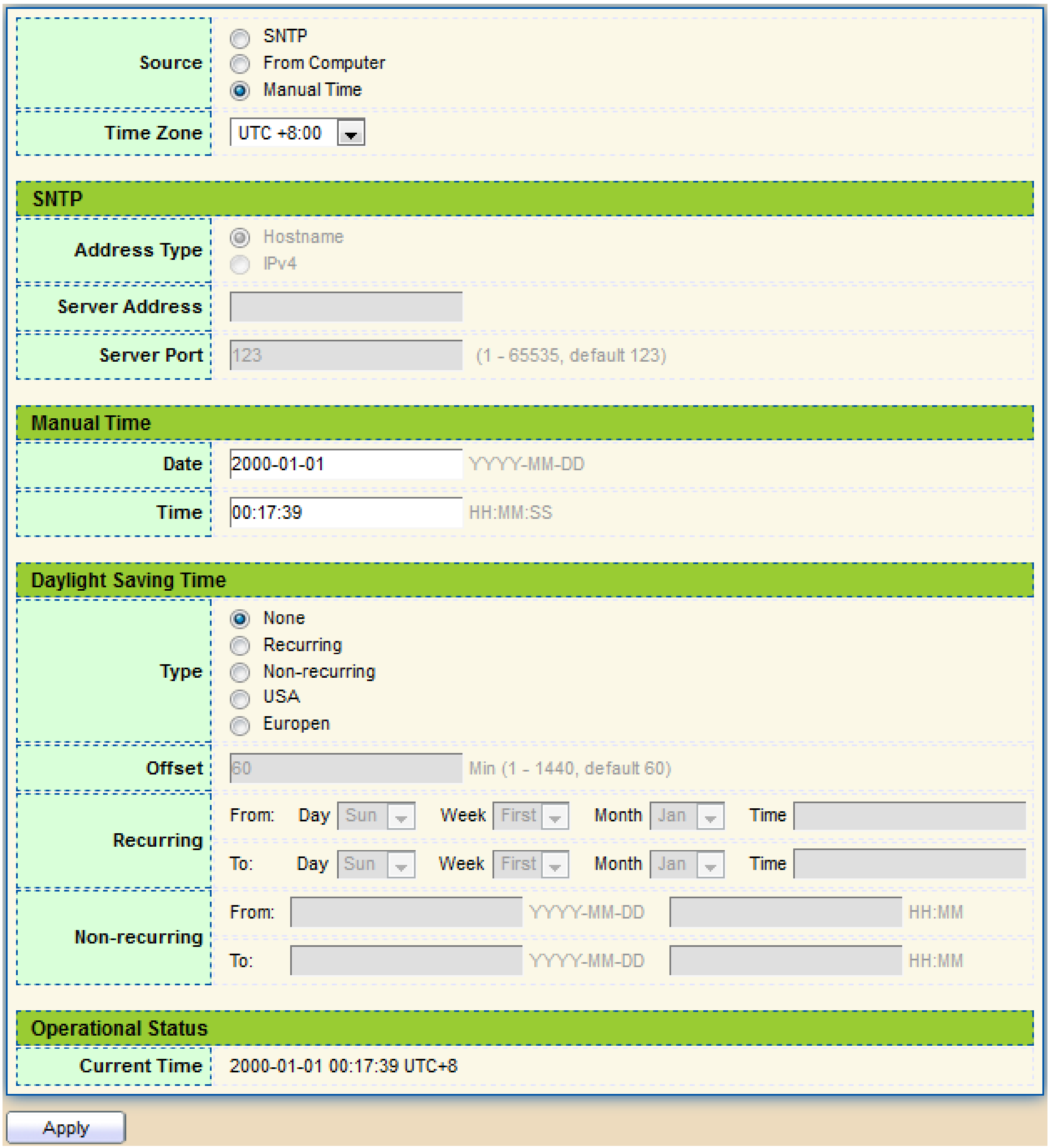
Item	Description
Address Type	The address type of switch IP configuration including • **Static**: Static IP configured by users will be used. • **Dynamic**: Enable the DHCP to obtain the IP address from a DHCP server.
IP Address	Specify the switch static IP address on the static configuration.
Subnet 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 Default 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.

4.2.2. 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**



Source	○ SNTP ○ From Computer ● Manual Time
Time Zone	UTC +8:00

SNTP

Address Type	● Hostname ○ IPv4
Server Address	
Server Port	123 (1 - 65535, default 123)

Manual Time

Date	2000-01-01 YYYY-MM-DD
Time	00:17:39 HH:MM:SS

Daylight Saving Time

Type	● None ○ Recurring ○ Non-recurring ○ USA ○ Europen
Offset	60 Min (1 - 1440, default 60)
Recurring	From: Day Sun Week First Month Jan Time To: Day Sun Week First Month Jan Time
Non-recurring	From: YYYY-MM-DD HH:MM To: YYYY-MM-DD HH:MM

Operational Status

Current Time	2000-01-01 00:17:39 UTC+8

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.

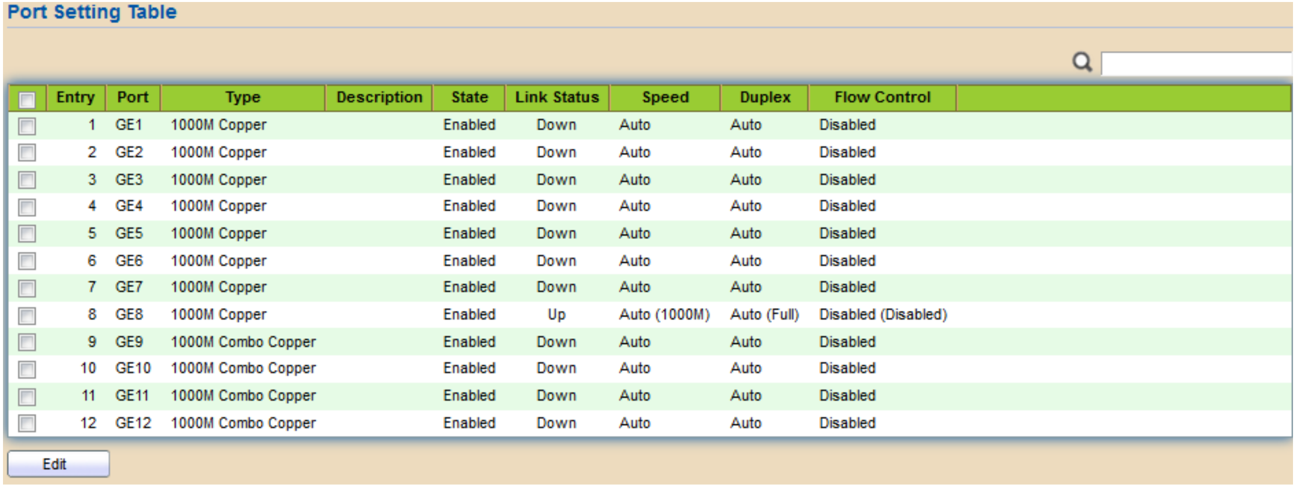
4.3. Port

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

4.3.1. Port Setting

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

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



Port Setting Table

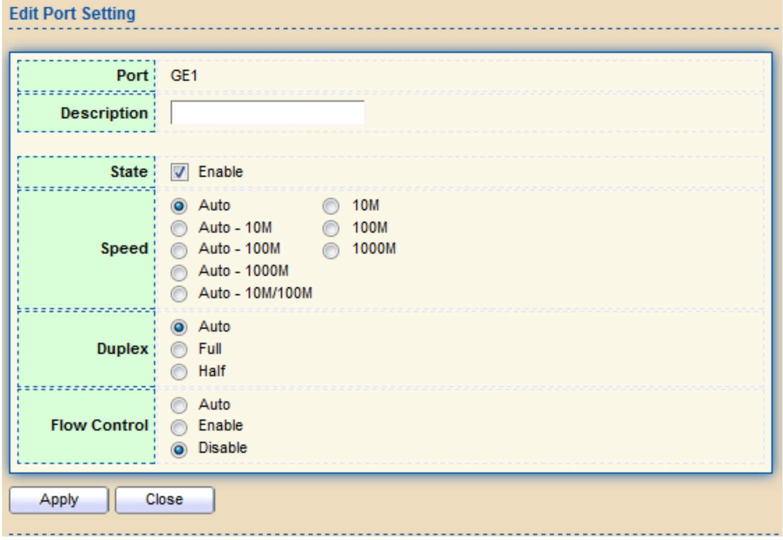
☐	Entry	Port	Type	Description	State	Link Status	Speed	Duplex	Flow Control
☐	1	GE1	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	2	GE2	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	3	GE3	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	4	GE4	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	5	GE5	1000M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

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,



Edit Port Setting

Port	GE1
Description	
State	☑ Enable
Speed	● Auto ○ Auto - 10M ○ Auto - 100M ○ Auto - 1000M ○ Auto - 10M/100M ○ 10M ○ 100M ○ 1000M
Duplex	● Auto ○ Full ○ Half
Flow Control	○ Auto ○ Enable ● Disable

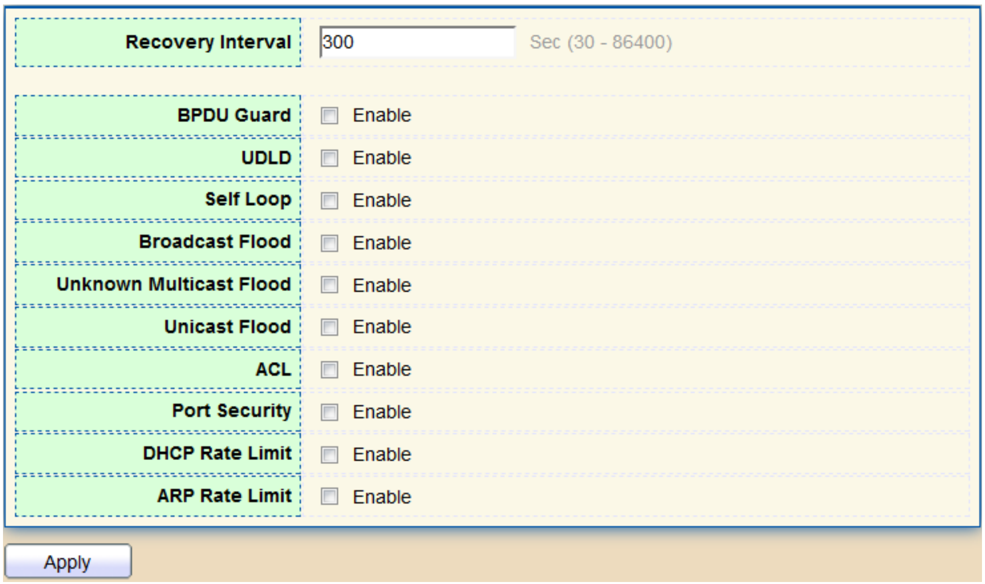
Figure 23 - Port > Port Setting > Port Setting

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.

4.3.2. Error Disable

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



Recovery Interval	300 Sec (30 - 86400)
BPDU Guard	□ Enable
UDLD	□ Enable
Self Loop	□ Enable
Broadcast Flood	□ Enable
Unknown Multicast Flood	□ Enable
Unicast Flood	□ Enable
ACL	□ Enable
Port Security	□ Enable
DHCP Rate Limit	□ Enable
ARP Rate Limit	□ Enable

Figure 24 - Port > Error disable

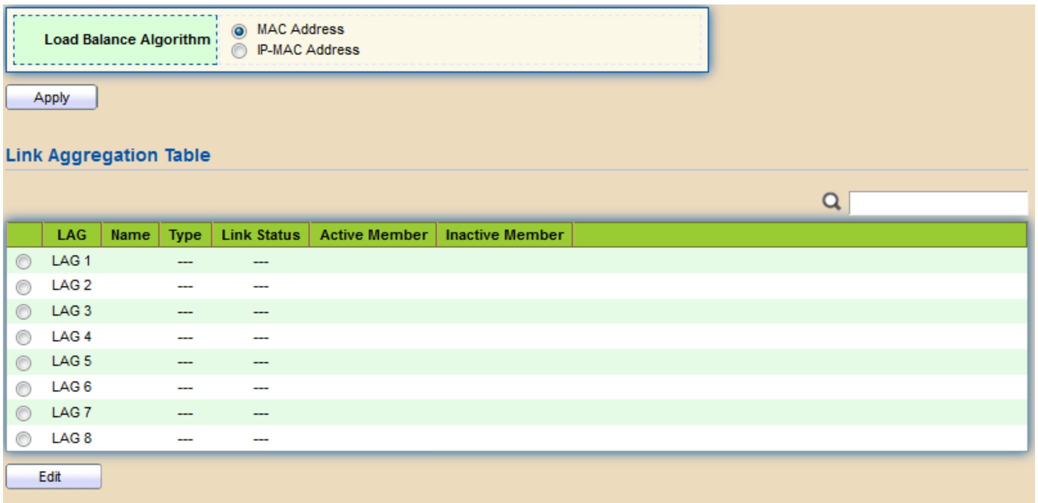
Item	Description
Recover Interval	Auto recovery after this interval for error disabled port.
BPDU Guard	Enabled to auto shutdown port when BPDU Guard reason occur. This reason caused by STP BPDU Guard mechanism.
UDLD	Enabled to auto shutdown port when UDLD violation occur.
Self Loop	Enabled to auto shutdown 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.

4.3.3. Link Aggregation

4.3.3.1. 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**.



Load Balance Algorithm ● MAC Address ○ IP-MAC Address

Link Aggregation Table

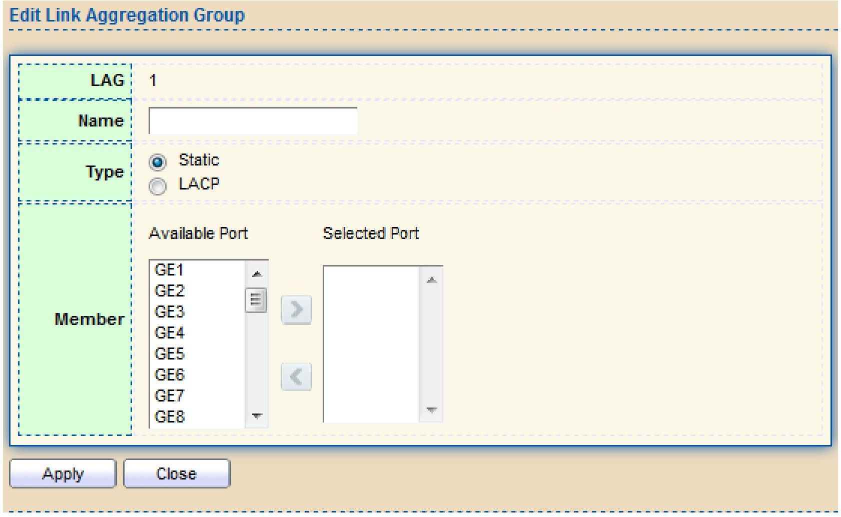
	LAG	Name	Type	Link Status	Active Member	Inactive Member
○	LAG 1		---	---		
○	LAG 2		---	---		
○	LAG 3		---	---		
○	LAG 4		---	---		
○	LAG 5		---	---		
○	LAG 6		---	---		
○	LAG 7		---	---		
○	LAG 8		---	---		

Figure 25 - 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.



Edit Link Aggregation Group

LAG	1
Name	
Type	● Static ○ LACP
Member	Available Port: GE1, GE2, GE3, GE4, GE5, GE6, GE7, GE8 Selected Port:

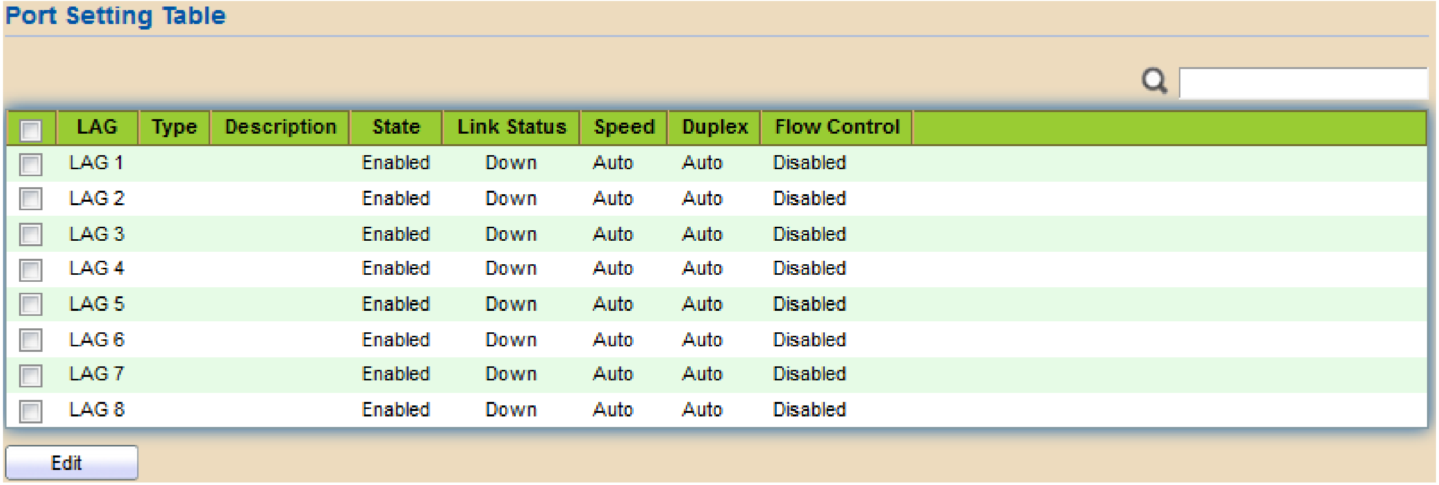
Figure 26 - Port > Link Aggregation > Group > Edit Link Aggregation Group

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.

4.3.3.2. Port Setting

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

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



Port Setting Table

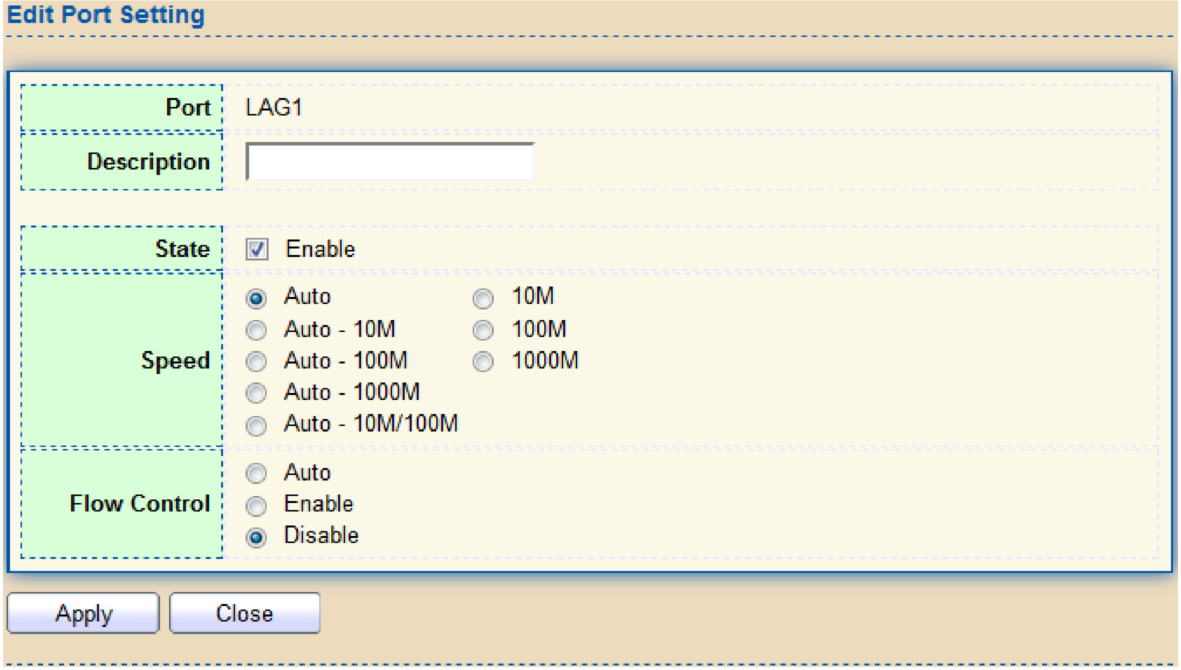
□	LAG	Type	Description	State	Link Status	Speed	Duplex	Flow Control
□	LAG 1			Enabled	Down	Auto	Auto	Disabled
□	LAG 2			Enabled	Down	Auto	Auto	Disabled
□	LAG 3			Enabled	Down	Auto	Auto	Disabled
□	LAG 4			Enabled	Down	Auto	Auto	Disabled
□	LAG 5			Enabled	Down	Auto	Auto	Disabled
□	LAG 6			Enabled	Down	Auto	Auto	Disabled
□	LAG 7			Enabled	Down	Auto	Auto	Disabled
□	LAG 8			Enabled	Down	Auto	Auto	Disabled

Figure 27 - 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.



Edit Port Setting

Port	LAG1
Description	
State	☑ Enable
Speed	● Auto ○ 10M ○ Auto - 10M ○ 100M ○ Auto - 100M ○ 1000M ○ Auto - 1000M ○ Auto - 10M/100M
Flow Control	○ Auto ○ Enable ● Disable

Figure 28 - Port > Link Aggregation > Port Setting > Edit Port Setting

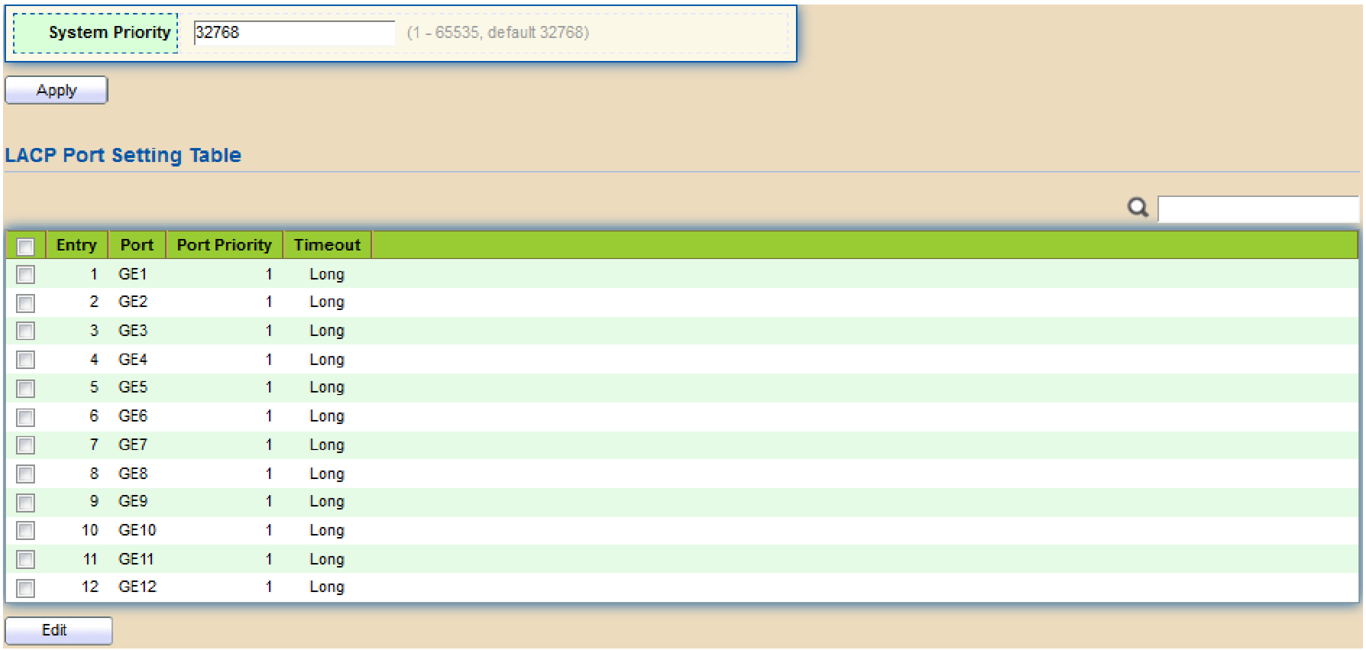
Item	Description
Port	Selected Port list.
Description	Port description.
State	Port admin state

	• 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.

4.3.3.3. 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**.



System Priority: 32768 (1 - 65535, default 32768)

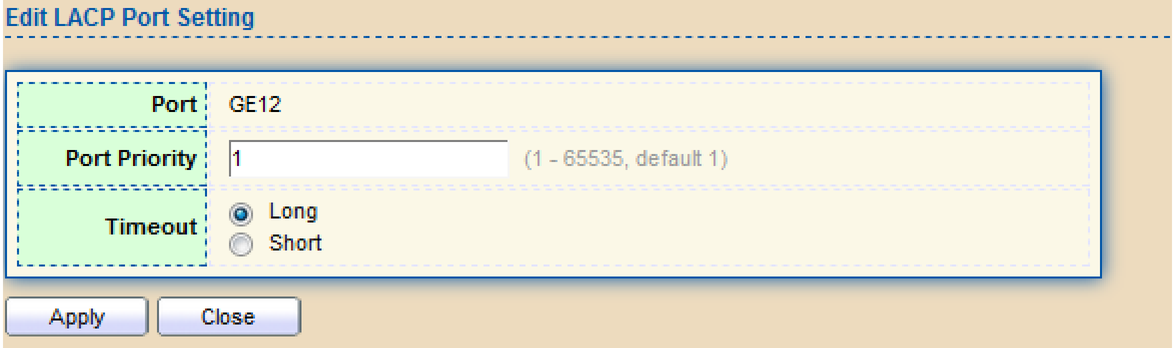
LACP Port Setting Table

□	Entry	Port	Port Priority	Timeout
□	1	GE1	1	Long
□	2	GE2	1	Long
□	3	GE3	1	Long
□	4	GE4	1	Long
□	5	GE5	1	Long
□	6	GE6	1	Long
□	7	GE7	1	Long
□	8	GE8	1	Long
□	9	GE9	1	Long
□	10	GE10	1	Long
□	11	GE11	1	Long
□	12	GE12	1	Long

Figure 29 - 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.



Edit LACP Port Setting

Port	GE12
Port Priority	1 (1 - 65535, default 1)
Timeout	● Long ○ Short

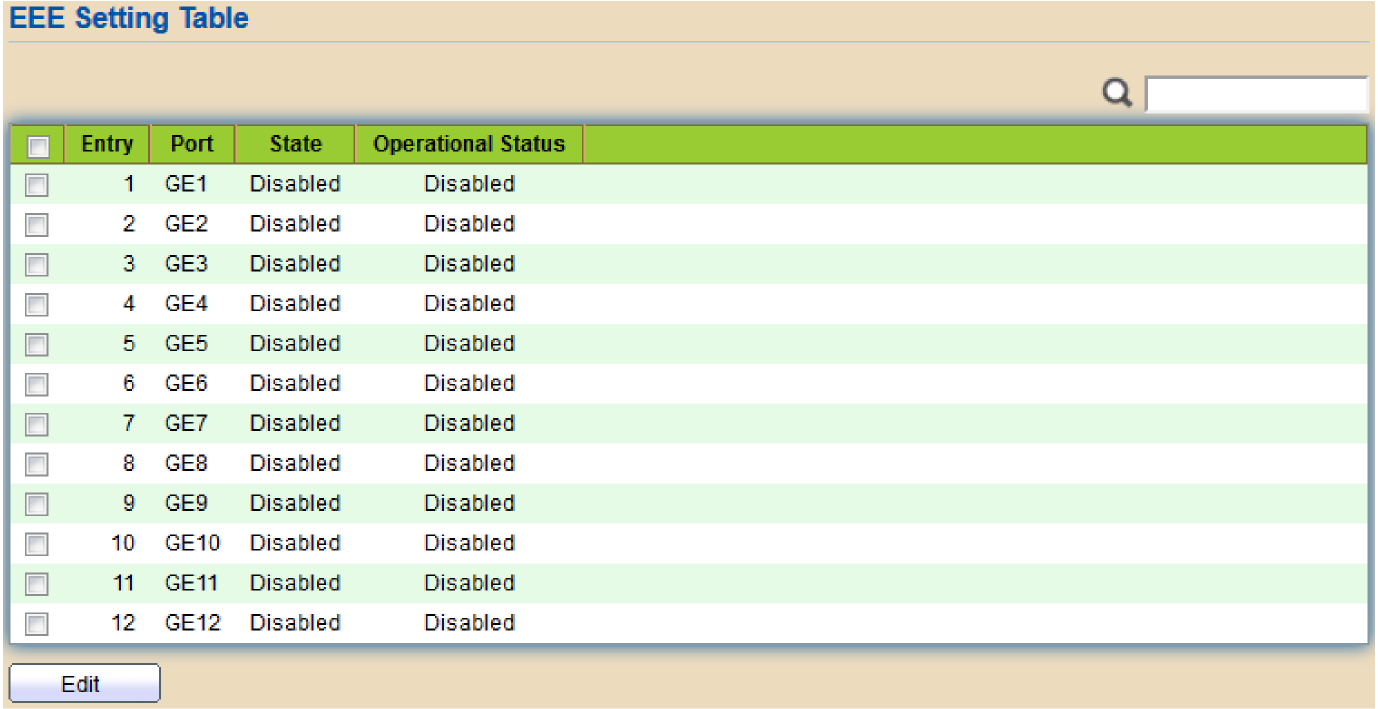
Figure 30 - Port > Link Aggregation > LACP > Edit LACP Port Setting

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).

4.3.4. EEE

This page allow user to configure Energy Efficient Ethernet settings.

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



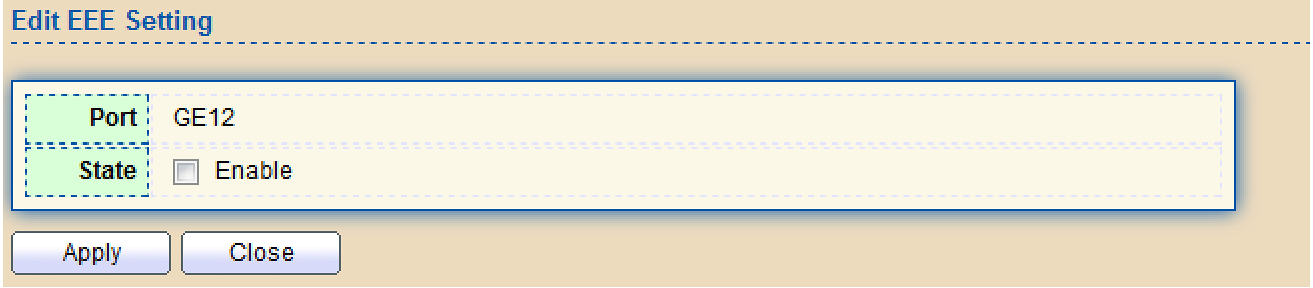
EEE Setting Table

□	Entry	Port	State	Operational Status
□	1	GE1	Disabled	Disabled
□	2	GE2	Disabled	Disabled
□	3	GE3	Disabled	Disabled
□	4	GE4	Disabled	Disabled
□	5	GE5	Disabled	Disabled
□	6	GE6	Disabled	Disabled
□	7	GE7	Disabled	Disabled
□	8	GE8	Disabled	Disabled
□	9	GE9	Disabled	Disabled
□	10	GE10	Disabled	Disabled
□	11	GE11	Disabled	Disabled
□	12	GE12	Disabled	Disabled

Figure 31 - 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.



Edit EEE Setting

Port	GE12
State	□ Enable

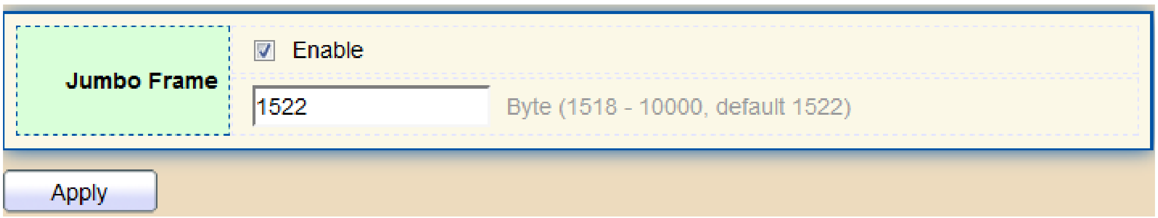
Figure 32 - Port > EEE > Edit EEE Setting

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

4.3.5. Jumbo Frame

This page allow user to configure switch jumbo frame size.

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



Jumbo Frame	☑ Enable 1522 Byte (1518 - 10000, default 1522)

Figure 33 - 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

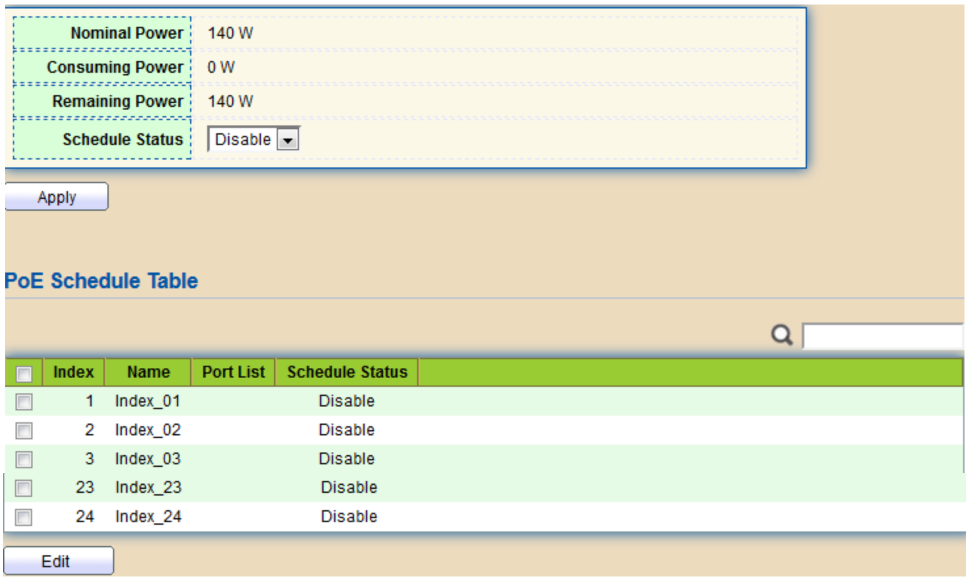
	jumbo frame is disabled, default frame size 1522 will be used.

4.4. PoE

PoE lets Ethernet cables supply power to network devices over the existing data connection.

4.4.1. Global Setting

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



Nominal Power	140 W
Consuming Power	0 W
Remaining Power	140 W
Schedule Status	Disable

PoE Schedule Table

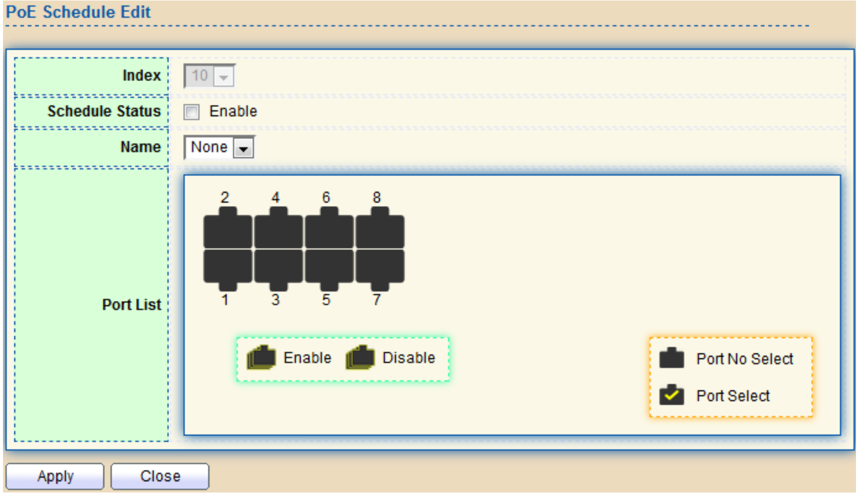
□	Index	Name	Port List	Schedule Status
□	1	Index_01		Disable
□	2	Index_02		Disable
□	3	Index_03		Disable
□	23	Index_23		Disable
□	24	Index_24		Disable

Figure 34 - 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.



PoE Schedule Edit

Index: 10

Schedule Status: □ Enable

Name: None

Port List

Figure 35 - 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.

4.4.2. 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**.

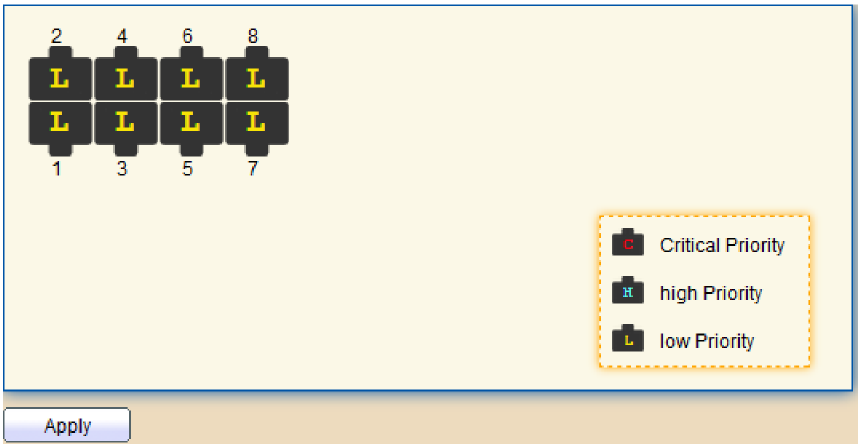
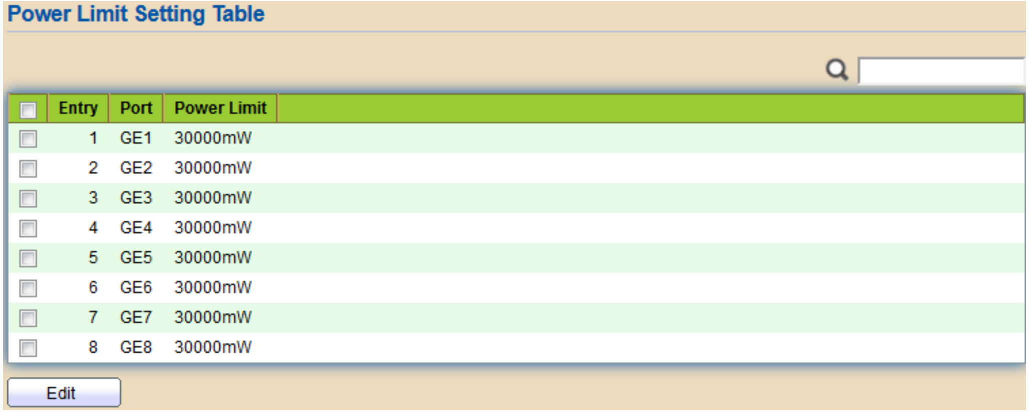


Figure 36 - PoE > Priority Setting

Item	Description
"L" is lower priority, "H" is high priority and "C" is Critical priority. Click the port to change its priority status.	

4.4.3. Power Limit

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

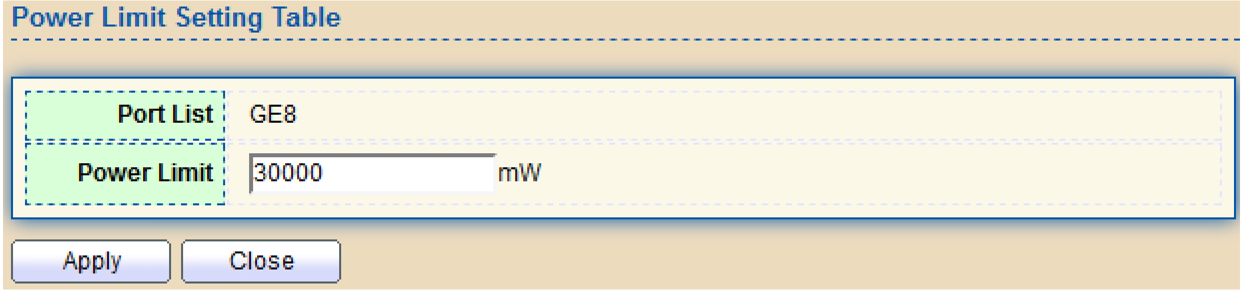

Power Limit Setting Table

□	Entry	Port	Power Limit
□	1	GE1	30000mW
□	2	GE2	30000mW
□	3	GE3	30000mW
□	4	GE4	30000mW
□	5	GE5	30000mW
□	6	GE6	30000mW
□	7	GE7	30000mW
□	8	GE8	30000mW

Figure 37 - 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.



Power Limit Setting Table

Port List	GE8
Power Limit	30000 mW

Figure 38 - 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.

4.4.4. Power show

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

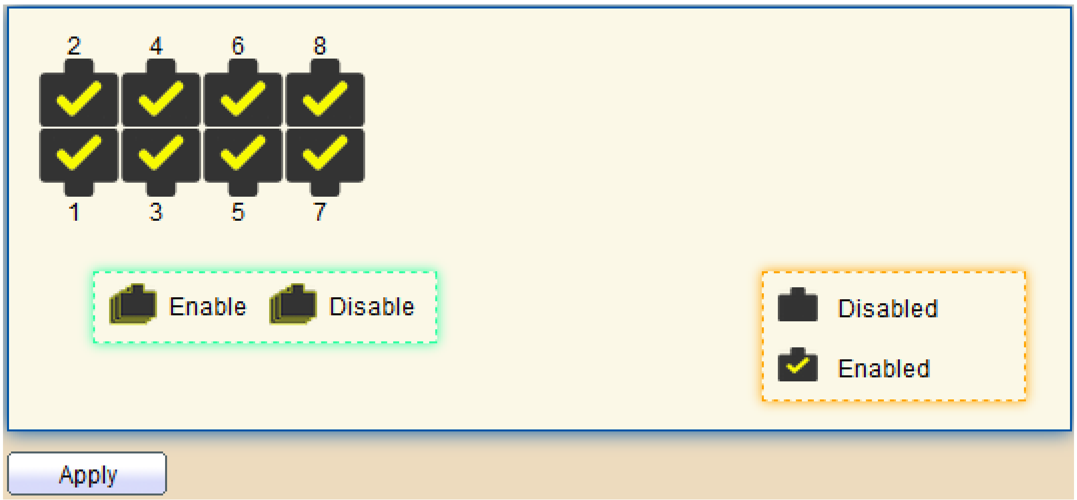


Figure 39 - PoE > Power Show

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

4.5. VLAN

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

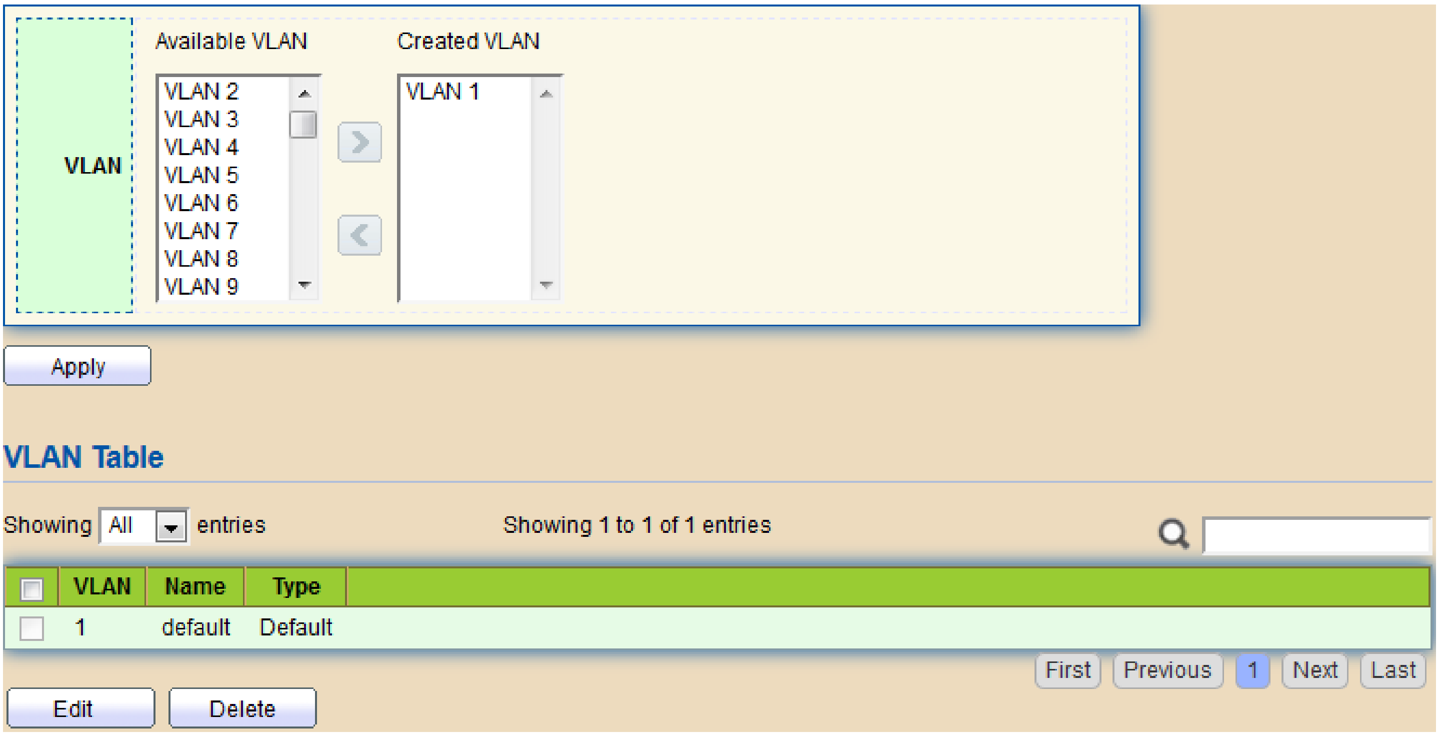
4.5.1. VLAN

Use the VLAN pages to configure settings of VLAN.

4.5.1.1. 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**



VLAN

Available VLAN: VLAN 2, VLAN 3, VLAN 4, VLAN 5, VLAN 6, VLAN 7, VLAN 8, VLAN 9

Created VLAN: VLAN 1

VLAN Table

Showing All entries

Showing 1 to 1 of 1 entries

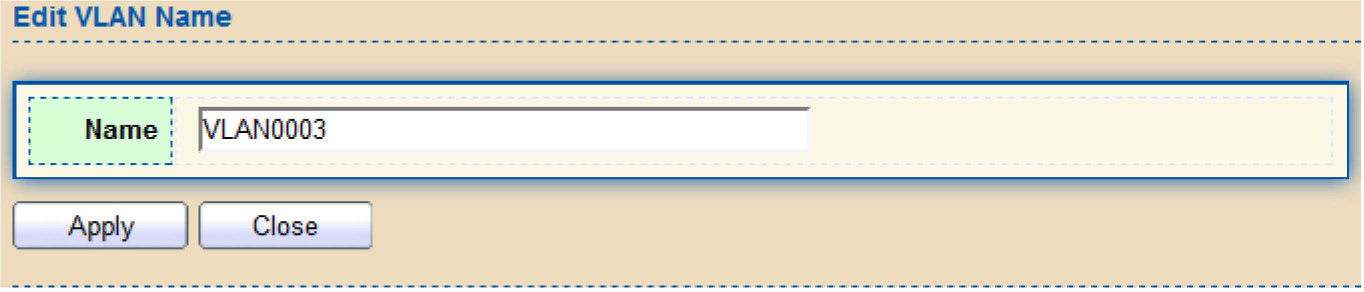
□	VLAN	Name	Type
□	1	default	Default

Figure 40 - 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.



Edit VLAN Name

Name: VLAN0003

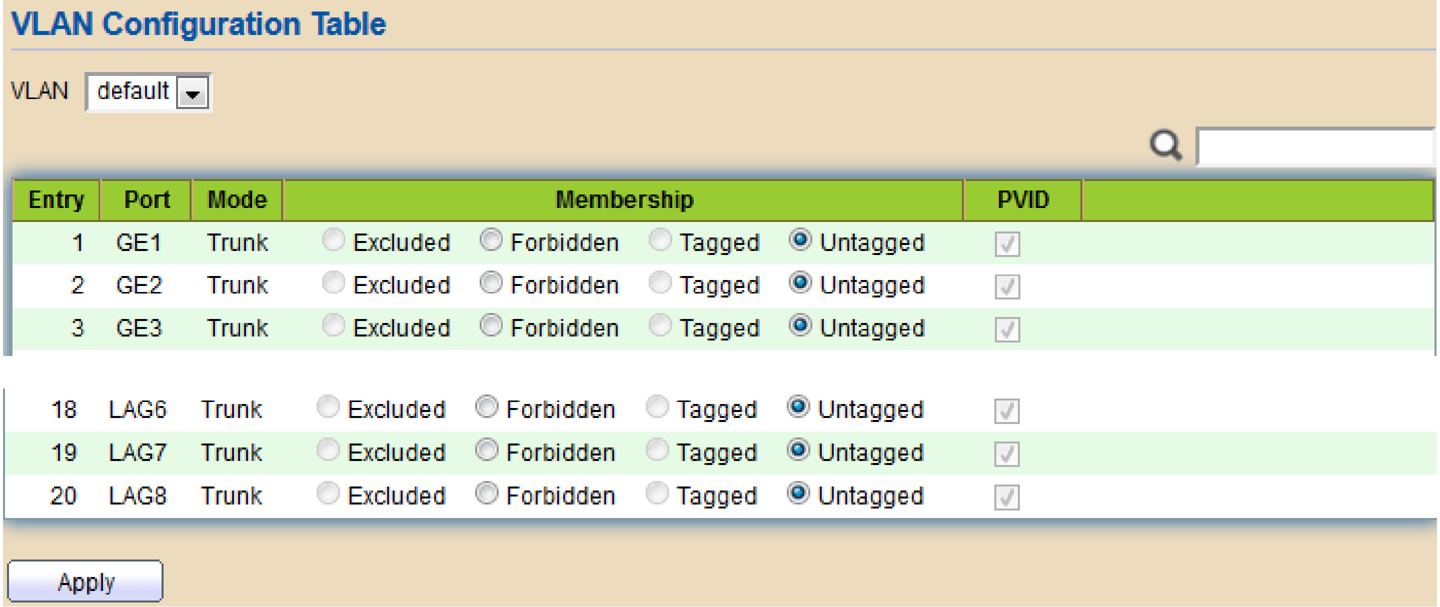
Figure 41 - VLAN > VLAN > Create VLAN > Edit VLAN Name

Item	Description
Name	Input VLAN name.

4.5.1.2. 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.**



VLAN Configuration Table

VLAN default ▾

Entry	Port	Mode	Membership				PVID
1	GE1	Trunk	○ Excluded	○ Forbidden	○ Tagged	● Untagged	☑
2	GE2	Trunk	○ Excluded	○ Forbidden	○ Tagged	● Untagged	☑
3	GE3	Trunk	○ Excluded	○ Forbidden	○ Tagged	● Untagged	☑
18	LAG6	Trunk	○ Excluded	○ Forbidden	○ Tagged	● Untagged	☑
19	LAG7	Trunk	○ Excluded	○ Forbidden	○ Tagged	● Untagged	☑
20	LAG8	Trunk	○ Excluded	○ Forbidden	○ Tagged	● Untagged	☑

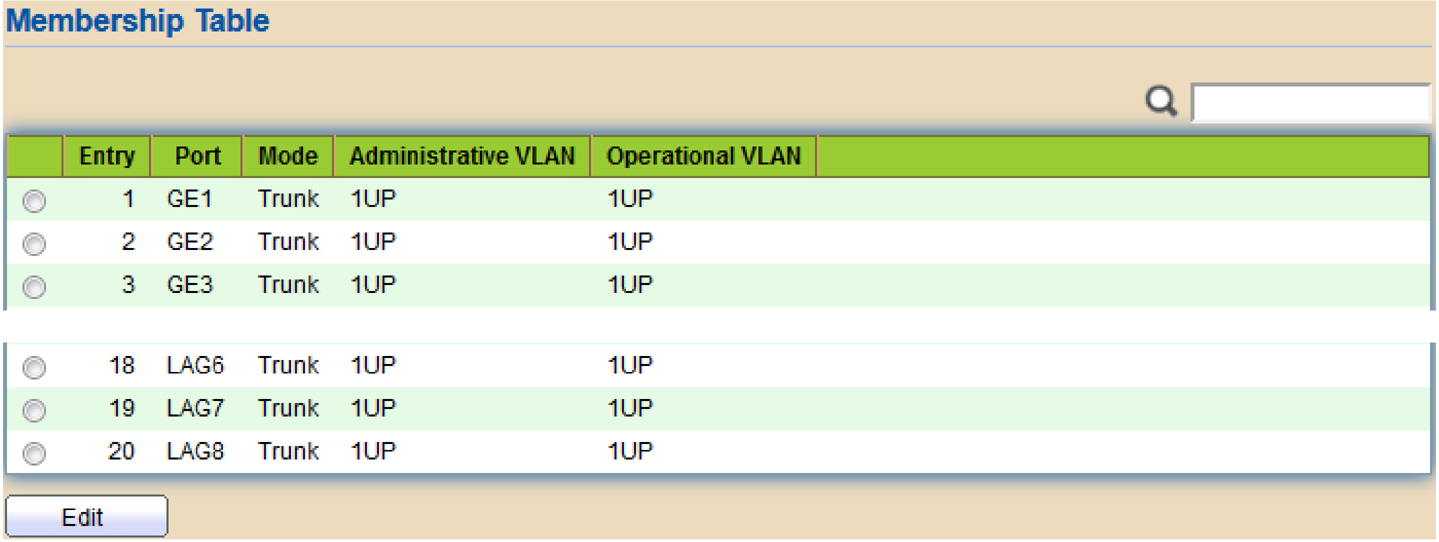
Figure 42 - VLAN > VLAN > VLAN Configuration

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.

4.5.1.3. 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**



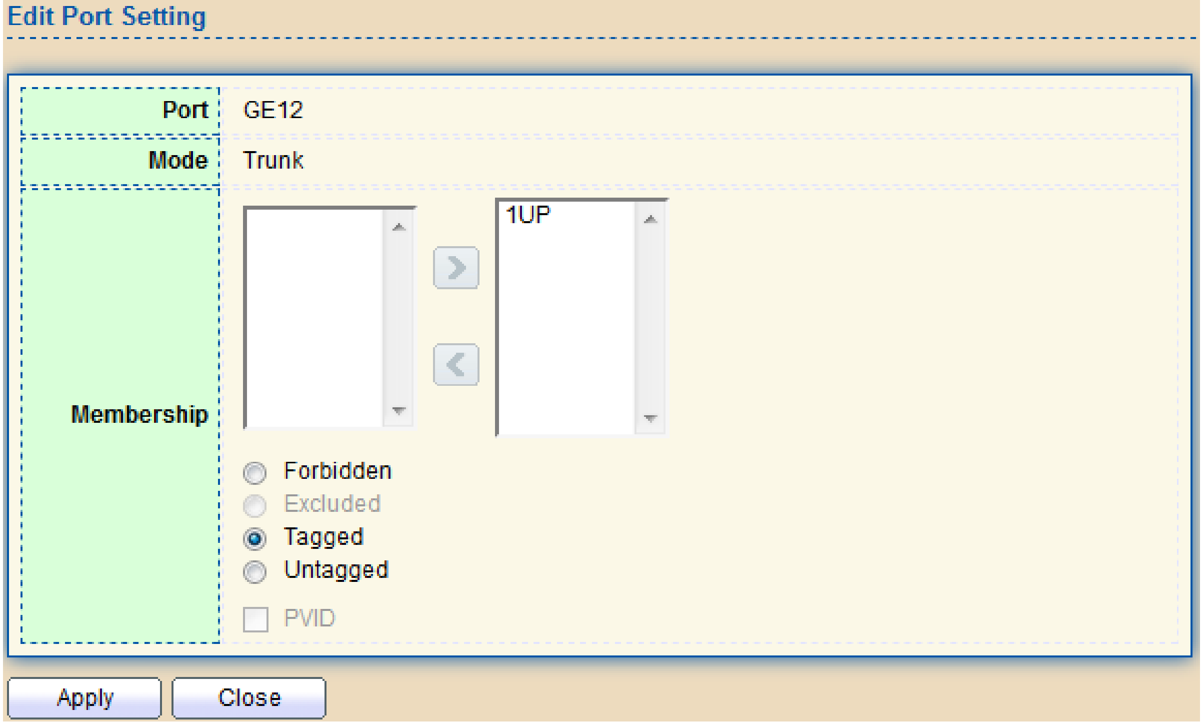
Membership Table

	Entry	Port	Mode	Administrative VLAN	Operational VLAN
○	1	GE1	Trunk	1UP	1UP
○	2	GE2	Trunk	1UP	1UP
○	3	GE3	Trunk	1UP	1UP
○	18	LAG6	Trunk	1UP	1UP
○	19	LAG7	Trunk	1UP	1UP
○	20	LAG8	Trunk	1UP	1UP

Figure 43 - 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



Edit Port Setting

Port	GE12
Mode	Trunk
Membership	1UP ○ Forbidden ○ Excluded ● Tagged ○ Untagged □ PVID

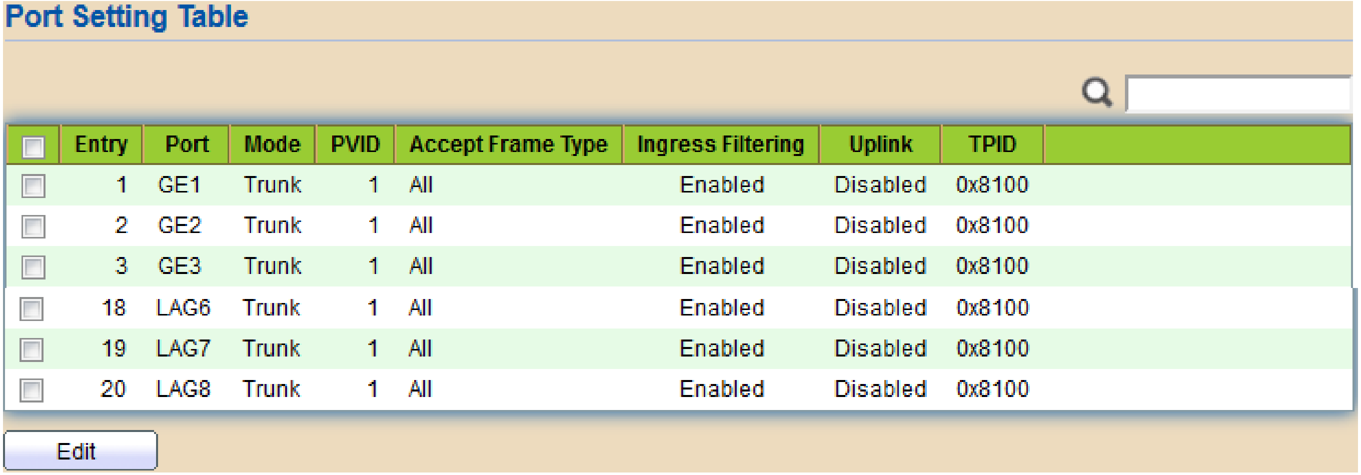
Figure 44 - VLAN > VLAN > Membership > Edit Port Setting

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.

4.5.1.4. 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**



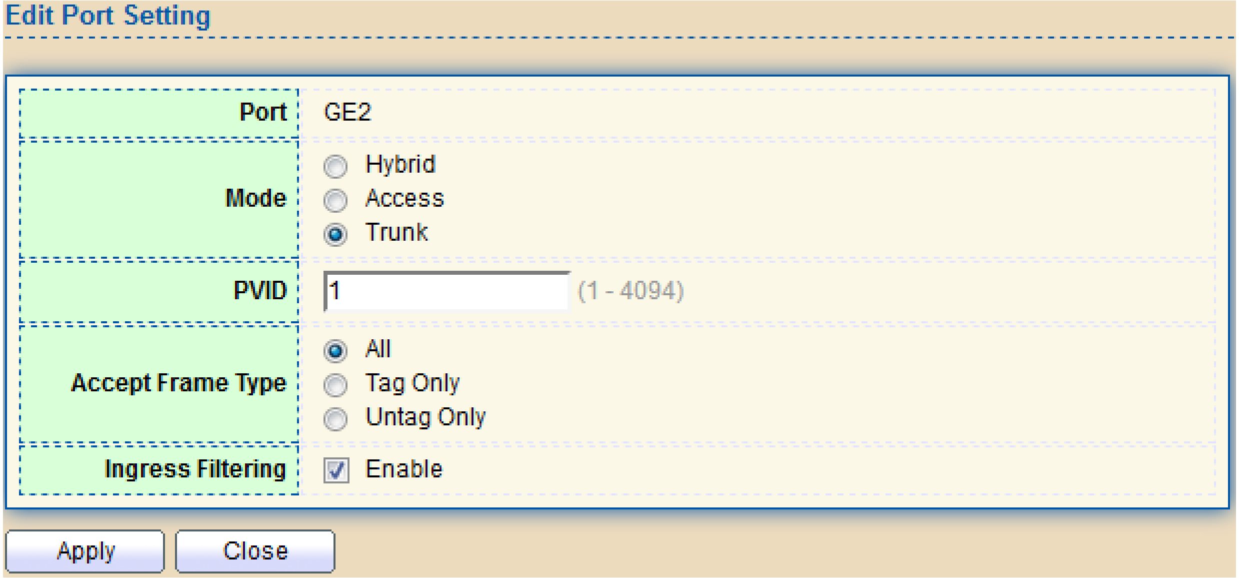
Port Setting Table

□	Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
□	1	GE1	Trunk	1	All	Enabled	Disabled	0x8100
□	2	GE2	Trunk	1	All	Enabled	Disabled	0x8100
□	3	GE3	Trunk	1	All	Enabled	Disabled	0x8100
□	18	LAG6	Trunk	1	All	Enabled	Disabled	0x8100
□	19	LAG7	Trunk	1	All	Enabled	Disabled	0x8100
□	20	LAG8	Trunk	1	All	Enabled	Disabled	0x8100

Figure 45 - 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.



Edit Port Setting

Port	GE2
Mode	○ Hybrid ○ Access ● Trunk
PVID	1 (1 - 4094)
Accept Frame Type	● All ○ Tag Only ○ Untag Only
Ingress Filtering	☑ Enable

Figure 46 - 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.

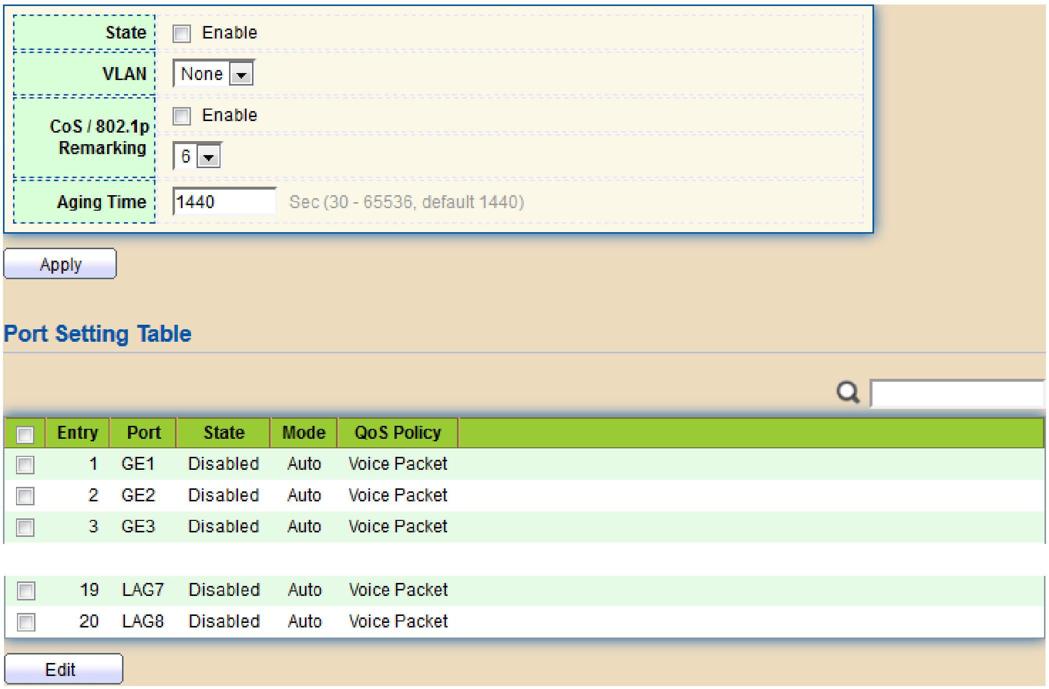
4.5.2. Voice VLAN

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

4.5.2.1. 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**



State	□ Enable
VLAN	None ▾
CoS / 802.1p Remarking	□ Enable 6 ▾
Aging Time	1440 Sec (30 - 65536, default 1440)

Port Setting Table

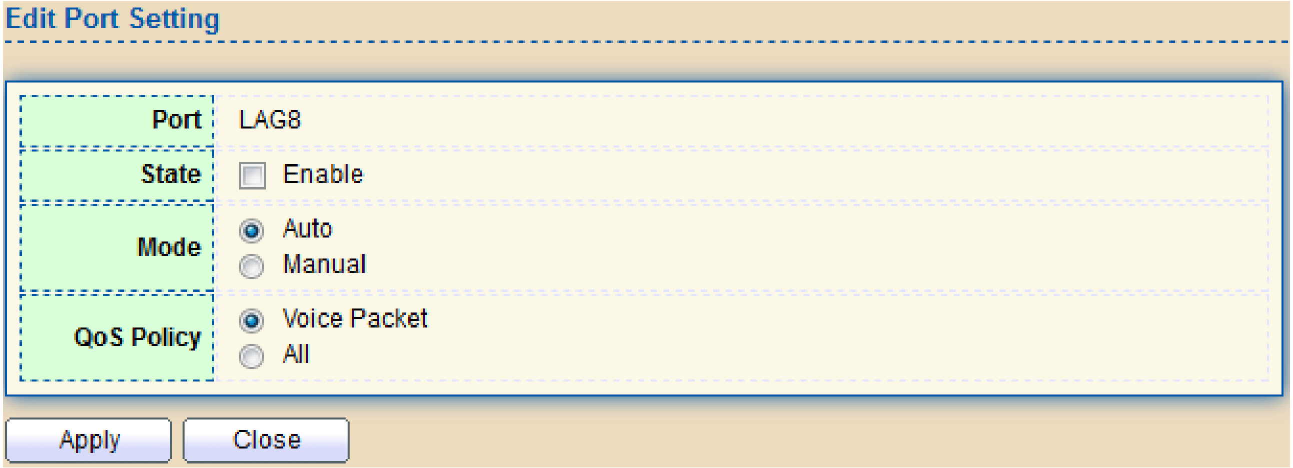
□	Entry	Port	State	Mode	QoS Policy
□	1	GE1	Disabled	Auto	Voice Packet
□	2	GE2	Disabled	Auto	Voice Packet
□	3	GE3	Disabled	Auto	Voice Packet
□	19	LAG7	Disabled	Auto	Voice Packet
□	20	LAG8	Disabled	Auto	Voice Packet

Figure 47 - 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.



Edit Port Setting

Port: LAG8

State: □ Enable

Mode: ● Auto ○ Manual

QoS Policy: ● Voice Packet ○ All

Figure 48 - VLAN > Voice VLAN > Property > Edit Port Setting

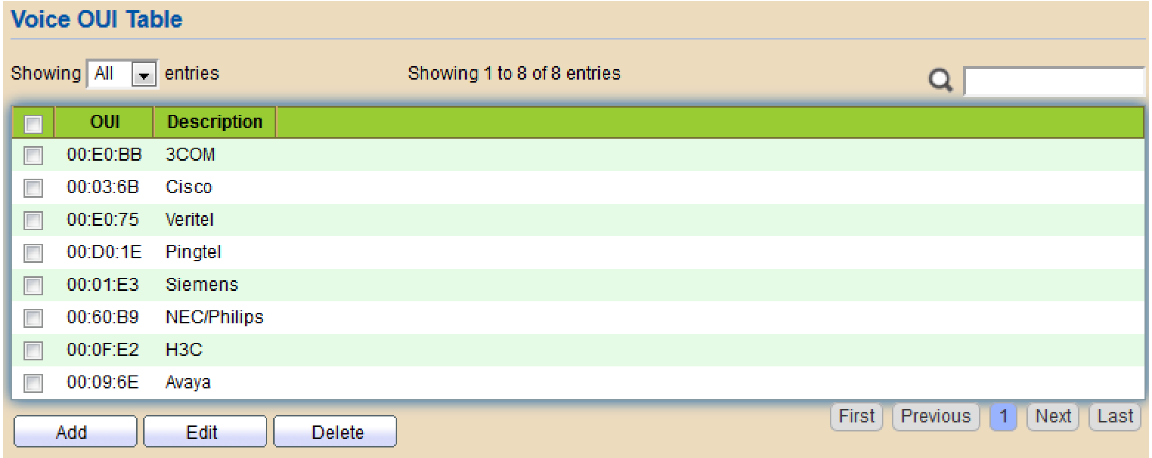
Item	Description
Port	Display selected port to be edited.
State	Set checkbox to enable/disabled voice VLAN function of

	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 the Voice VLAN.

4.5.2.2. 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**.



Voice OUI Table

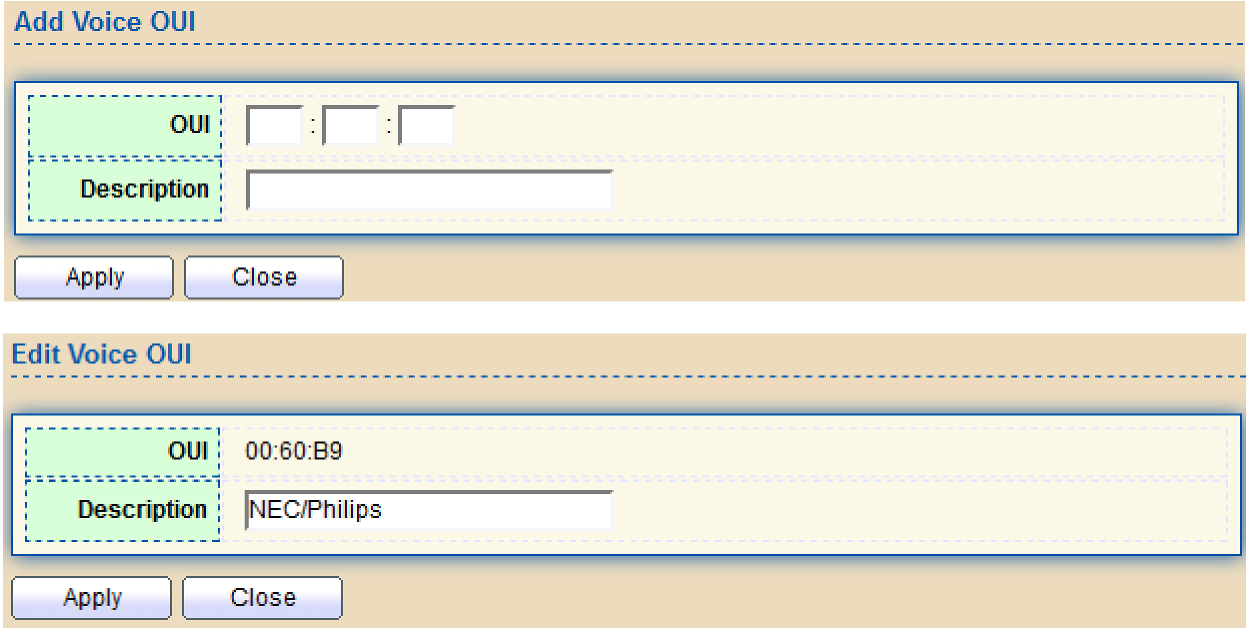
Showing All entries   Showing 1 to 8 of 8 entries

□	OUI	Description
□	00:E0:BB	3COM
□	00:03:6B	Cisco
□	00:E0:75	Veritel
□	00:D0:1E	Pingtel
□	00:01:E3	Siemens
□	00:60:B9	NEC/Philips
□	00:0F:E2	H3C
□	00:09:6E	Avaya

Figure 49 - 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.



Add Voice OUI

OUI: [ ] : [ ] : [ ]

Description: [ ]

Edit Voice OUI

OUI: 00:60:B9

Description: NEC/Philips

Figure 50 - 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.

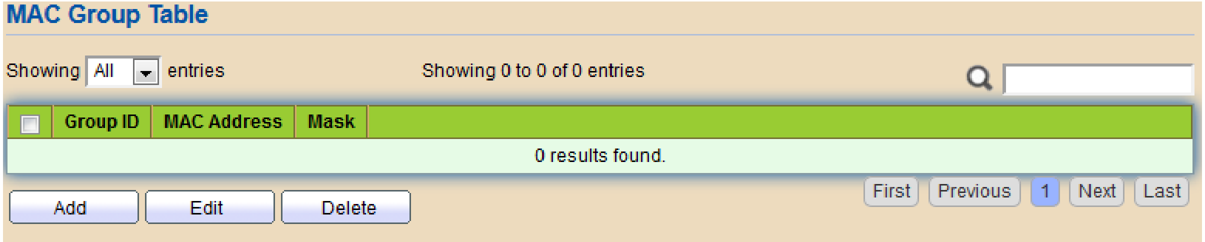
4.5.4. MAC VLAN

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

4.5.4.1. 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**.



MAC Group Table

Showing All entries

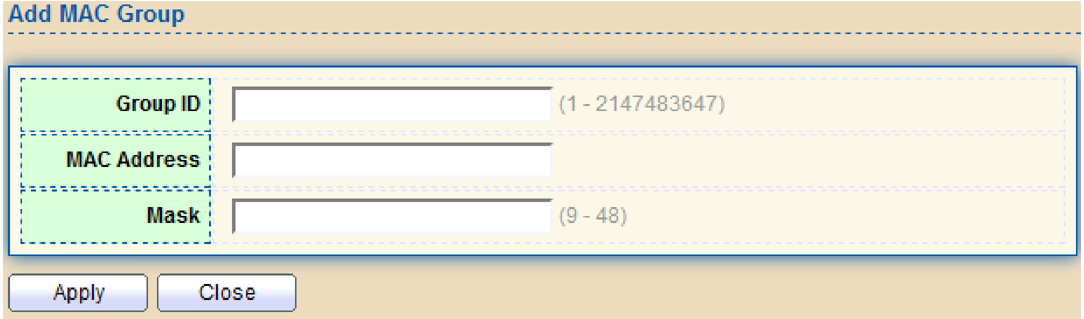
Showing 0 to 0 of 0 entries

□	Group ID	MAC Address	Mask
0 results found.			

Figure 51 - VLAN > MAC VLAN > MAC Group

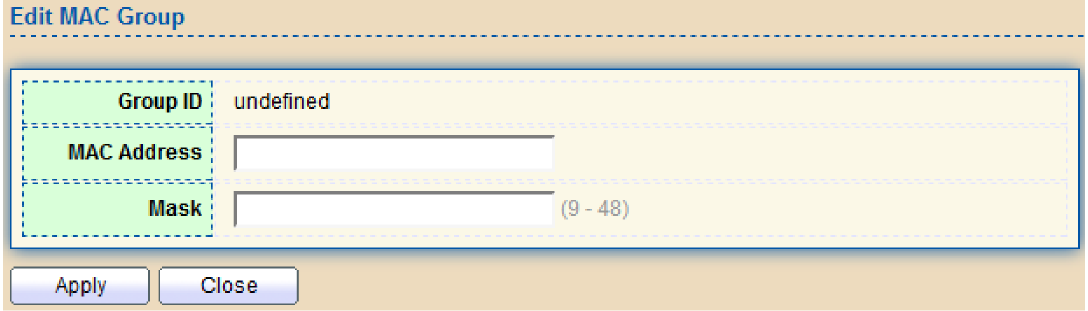
Item	Description
Group ID	Display group ID of entry.
MAC Address	Display mac address of entry.
Mask	Display mask of mac address for classified packet.

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



Add MAC Group

Group ID		(1 - 2147483647)
MAC Address		
Mask		(9 - 48)


Edit MAC Group

Group ID	undefined
MAC Address	
Mask	(9 - 48)

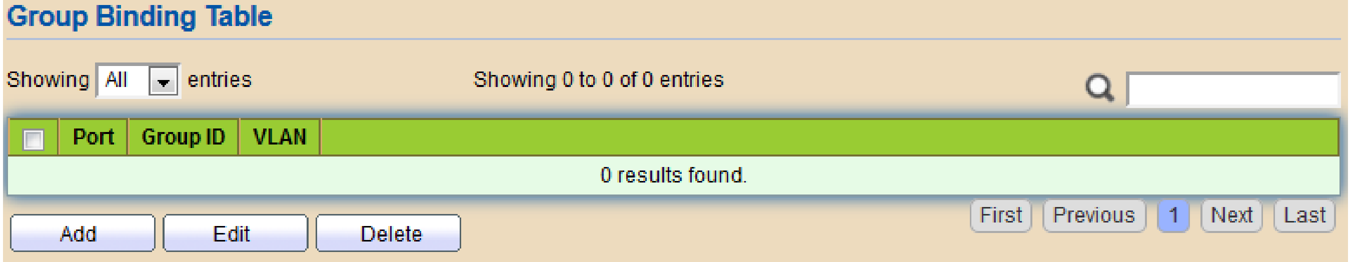
Figure 52 - VLAN > MAC VLAN > MAC Group > Add/Edit MAC

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.

4.5.4.2. 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**


Group Binding Table

Showing All entries   Showing 0 to 0 of 0 entries

□	Port	Group ID	VLAN
0 results found.			

Figure 53 - 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” button to view the Add Group Binding menu.

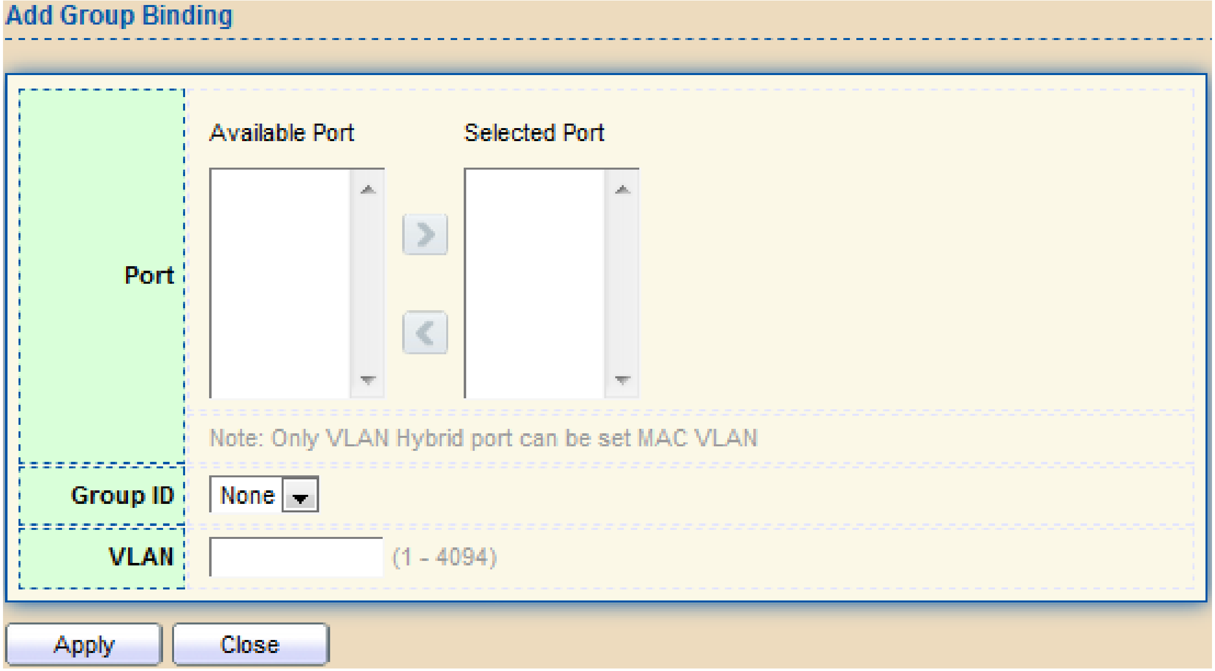


Figure 54 - VLAN > MAC VLAN > Group Binding

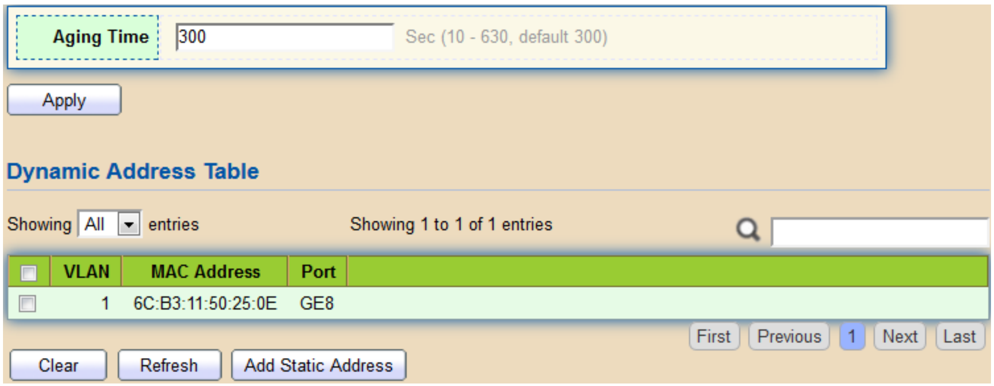
Item	Description
Port	Select ports in left box then move to right to binding with MAC group. Or select ports in right box then move to left to unbind with MAC group. Only interface has hybrid VLAN mode can be selected and bound with protocol group. Only available on Add dialog.
Group ID	Select a Group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

4.6. MAC Address Table

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

4.6.1. Dynamic Address

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



Aging Time: 300 Sec (10 - 630, default 300)

Dynamic Address Table

Showing All entries — Showing 1 to 1 of 1 entries

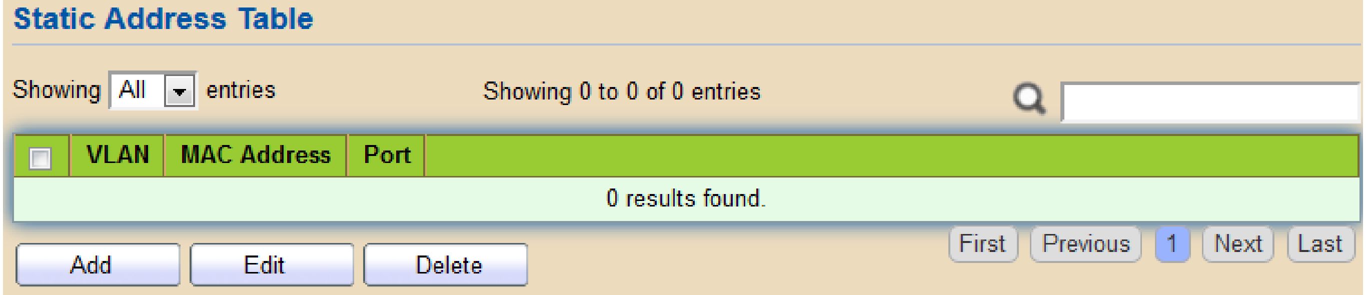
□	VLAN	MAC Address	Port
□	1	6C:B3:11:50:25:0E	GE8

Figure 55 - 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.

4.6.2. Static Address

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



Static Address Table

Showing All entries Showing 0 to 0 of 0 entries

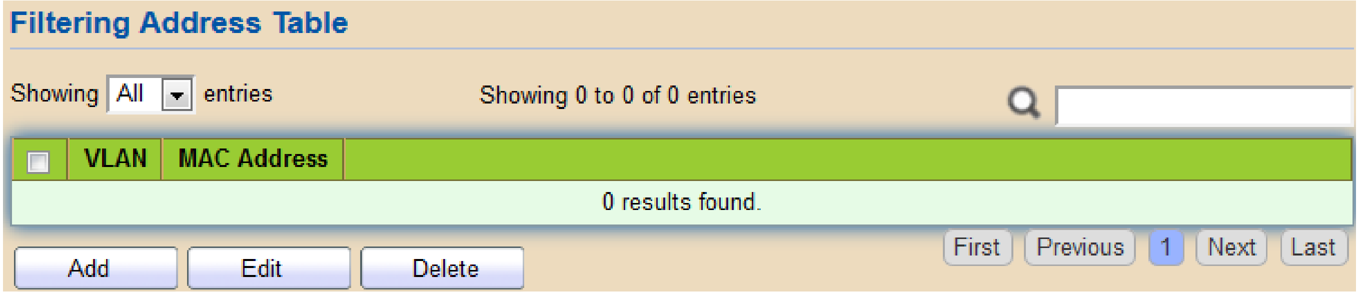
□	VLAN	MAC Address	Port
0 results found.			

Figure 56 - 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.

4.6.3. Filtering Address

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



Filtering Address Table

Showing All entries Showing 0 to 0 of 0 entries

□	VLAN	MAC Address
0 results found.		

Figure 57 - MAC Address Table > Filtering Address.

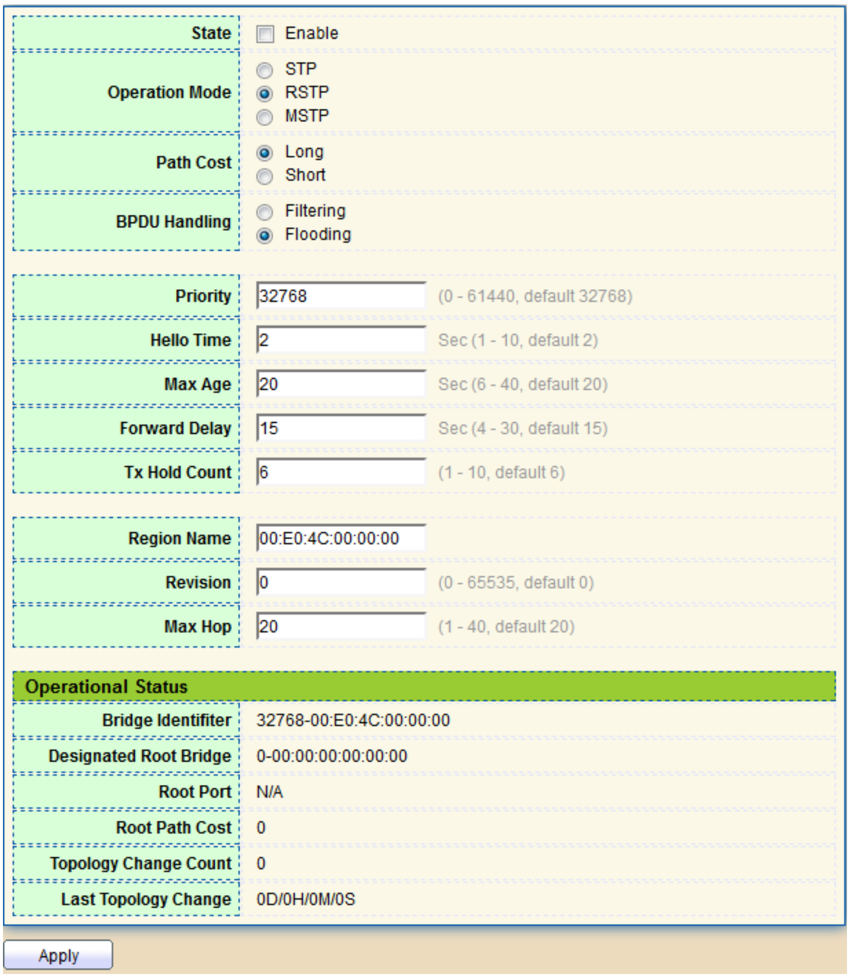
Item	Description
MAC Address	Specify unicast MAC address in the packets to be dropped.
VLAN	Specify the VLAN to show or clear MAC entries.

4.7. Spanning Tree

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

4.7.1. Property

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



State	□ Enable	
Operation Mode	○ STP ● RSTP ○ MSTP	
Path Cost	● Long ○ Short	
BPDU Handling	○ Filtering ● Flooding	
Priority	32768	(0 - 61440, default 32768)
Hello Time	2	Sec (1 - 10, default 2)
Max Age	20	Sec (6 - 40, default 20)
Forward Delay	15	Sec (4 - 30, default 15)
Tx Hold Count	6	(1 - 10, default 6)
Region Name	00:E0:4C:00:00:00	
Revision	0	(0 - 65535, default 0)
Max Hop	20	(1 - 40, default 20)

Operational Status

Bridge Identifiter	32768-00:E0:4C:00:00:00
Designated Root Bridge	0-00:00:00:00:00:00
Root Port	N/A
Root Path Cost	0
Topology Change Count	0
Last Topology Change	0D/0H/0M/0S

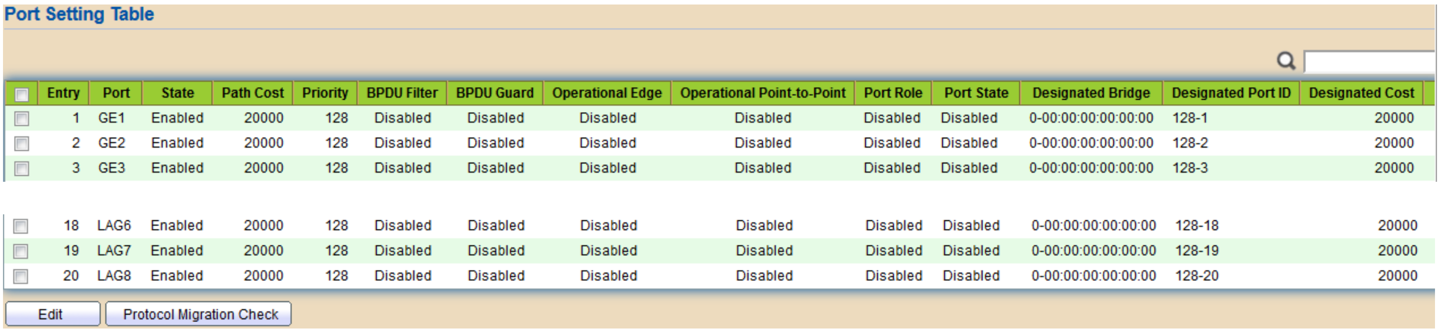
Figure 58 - Spanning Tree > Property

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.

4.7.2. Port Setting

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



Port Setting Table

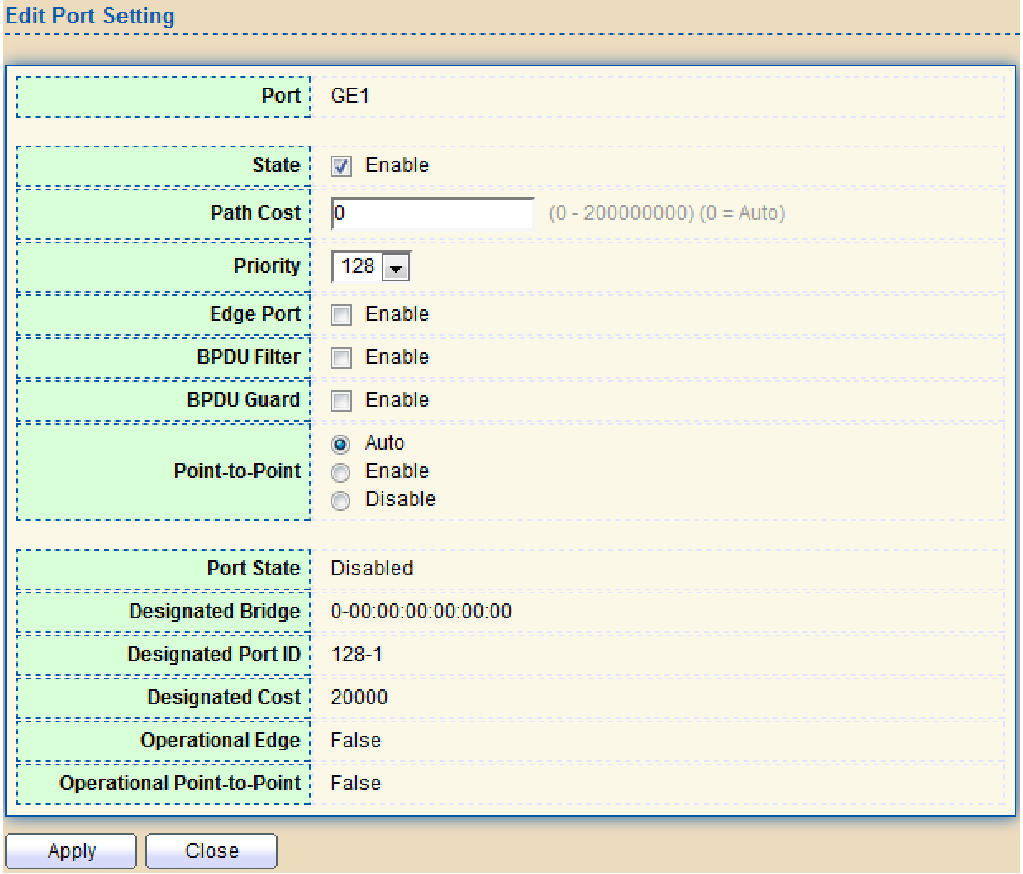
□	Entry	Port	State	Path Cost	Priority	BPDU Filter	BPDU Guard	Operational Edge	Operational Point-to-Point	Port Role	Port State	Designated Bridge	Designated Port ID	Designated Cost
□	1	GE1	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-1	20000
□	2	GE2	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-2	20000
□	3	GE3	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-3	20000
□	18	LAG6	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-18	20000
□	19	LAG7	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-19	20000
□	20	LAG8	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-20	20000

Figure 59 - 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.



Edit Port Setting

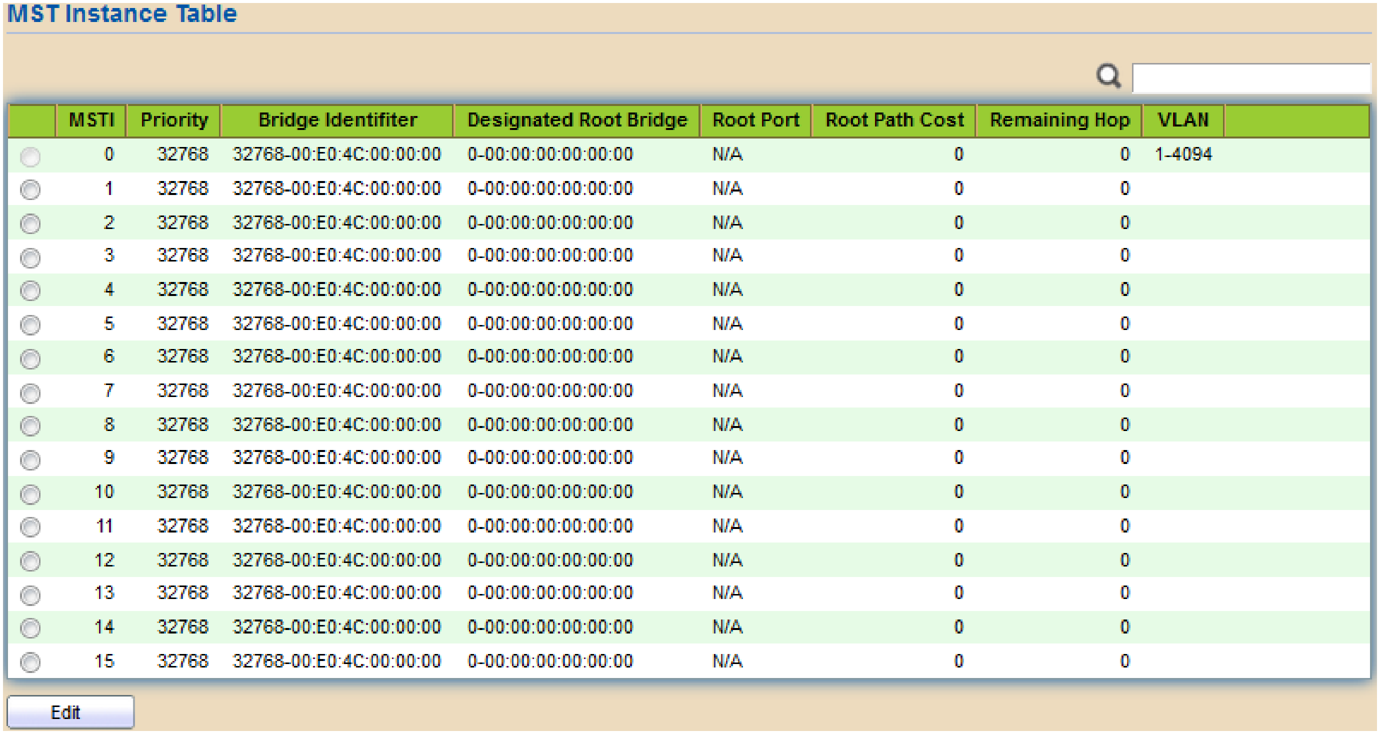
Port	GE1
State	☑ Enable
Path Cost	0 (0 - 200000000) (0 = Auto)
Priority	128
Edge Port	□ Enable
BPDU Filter	□ Enable
BPDU Guard	□ Enable
Point-to-Point	● Auto ○ Enable ○ Disable
Port State	Disabled
Designated Bridge	0-00:00:00:00:00:00
Designated Port ID	128-1
Designated Cost	20000
Operational Edge	False
Operational Point-to-Point	False

Figure 60 - 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

4.7.3. MST Instance

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



MST Instance Table

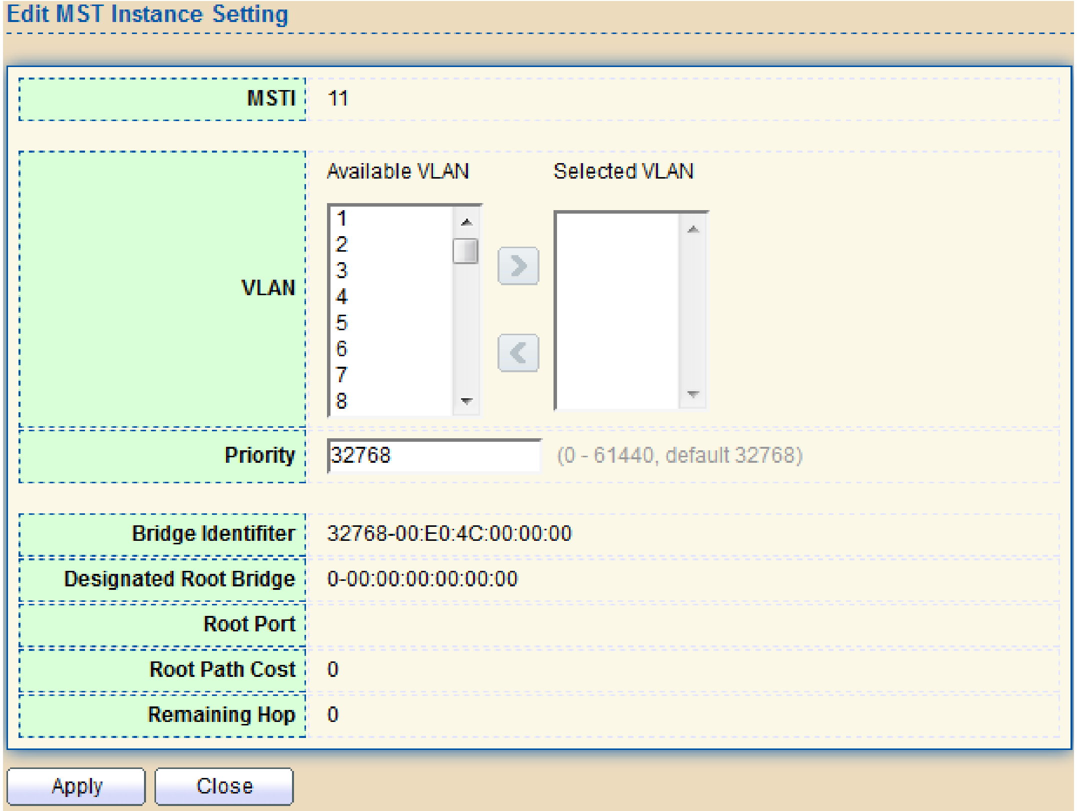
	MSTI	Priority	Bridge Identifiter	Designated Root Bridge	Root Port	Root Path Cost	Remaining Hop	VLAN
○	0	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	1-4094
○	1	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	2	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	3	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	4	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	5	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	6	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	7	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	8	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	9	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	10	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	11	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	12	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	13	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	14	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
○	15	32768	32768-00:E0:4C:00:00:00	0-00:00:00:00:00:00	N/A	0	0	

Figure 61 - 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.



Edit MST Instance Setting

MSTI: 11

VLAN: Available VLAN: 1, 2, 3, 4, 5, 6, 7, 8; Selected VLAN: (empty)

Priority: 32768 (0 - 61440, default 32768)

Bridge Identifiter: 32768-00:E0:4C:00:00:00

Designated Root Bridge: 0-00:00:00:00:00:00

Root Port:

Root Path Cost: 0

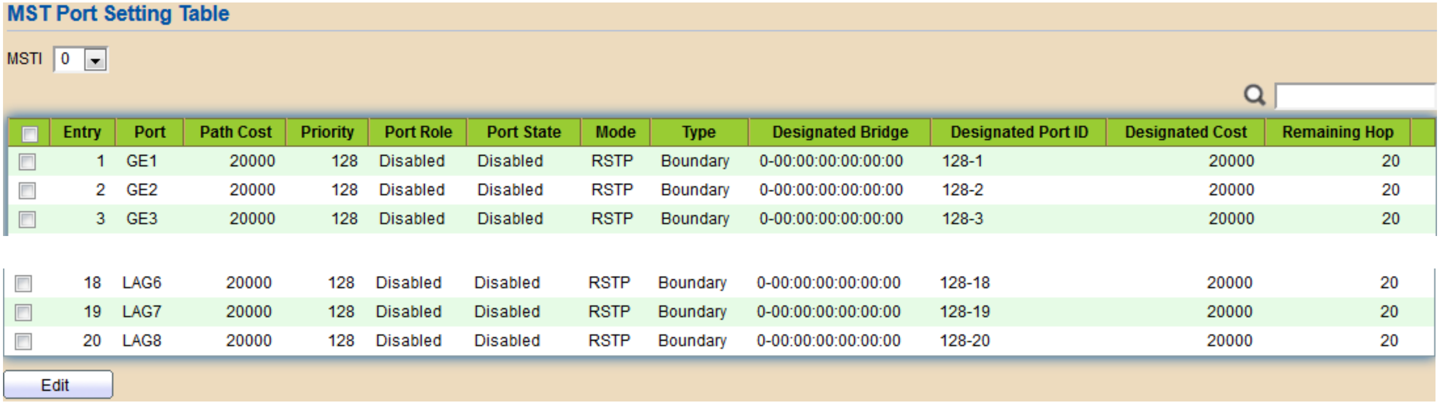
Remaining Hop: 0

Figure 62 - 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.

4.7.4. MST Port Setting

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



MST Port Setting Table

MSTI 0

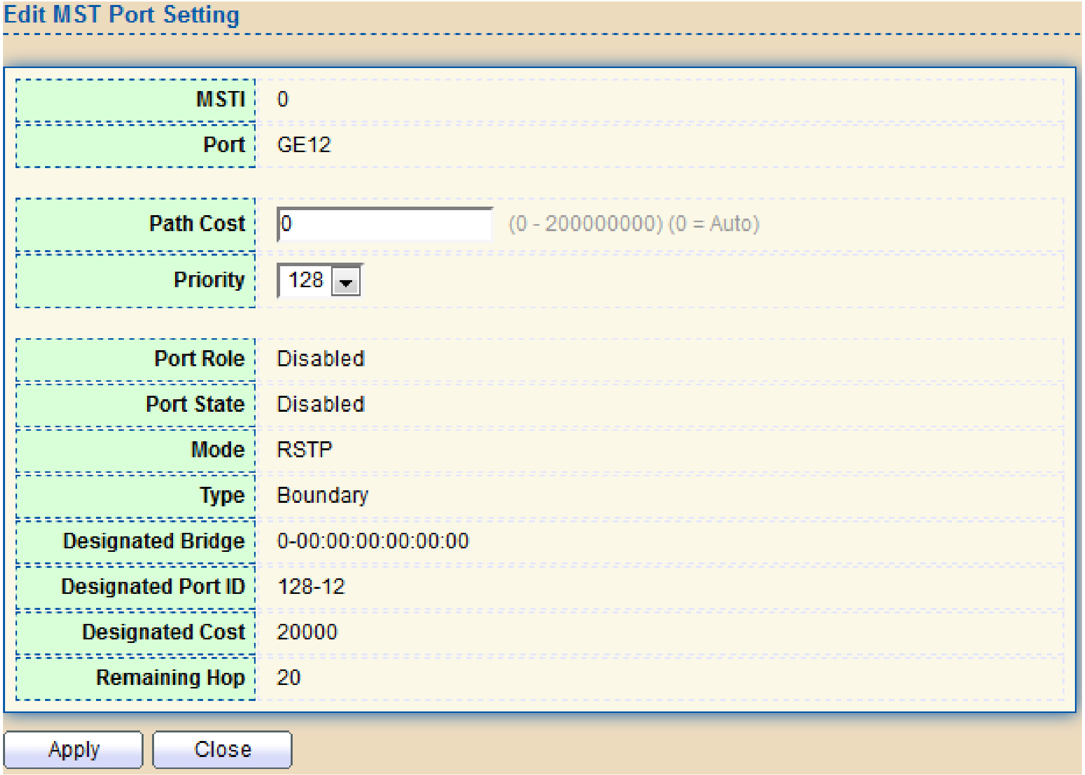
□	Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Type	Designated Bridge	Designated Port ID	Designated Cost	Remaining Hop
□	1	GE1	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-1	20000	20
□	2	GE2	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-2	20000	20
□	3	GE3	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-3	20000	20
□	18	LAG6	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-18	20000	20
□	19	LAG7	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-19	20000	20
□	20	LAG8	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-20	20000	20

Figure 63 - Spanning Tree > MST Port Setting

Item	Descriptio n
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.


Edit MST Port Setting

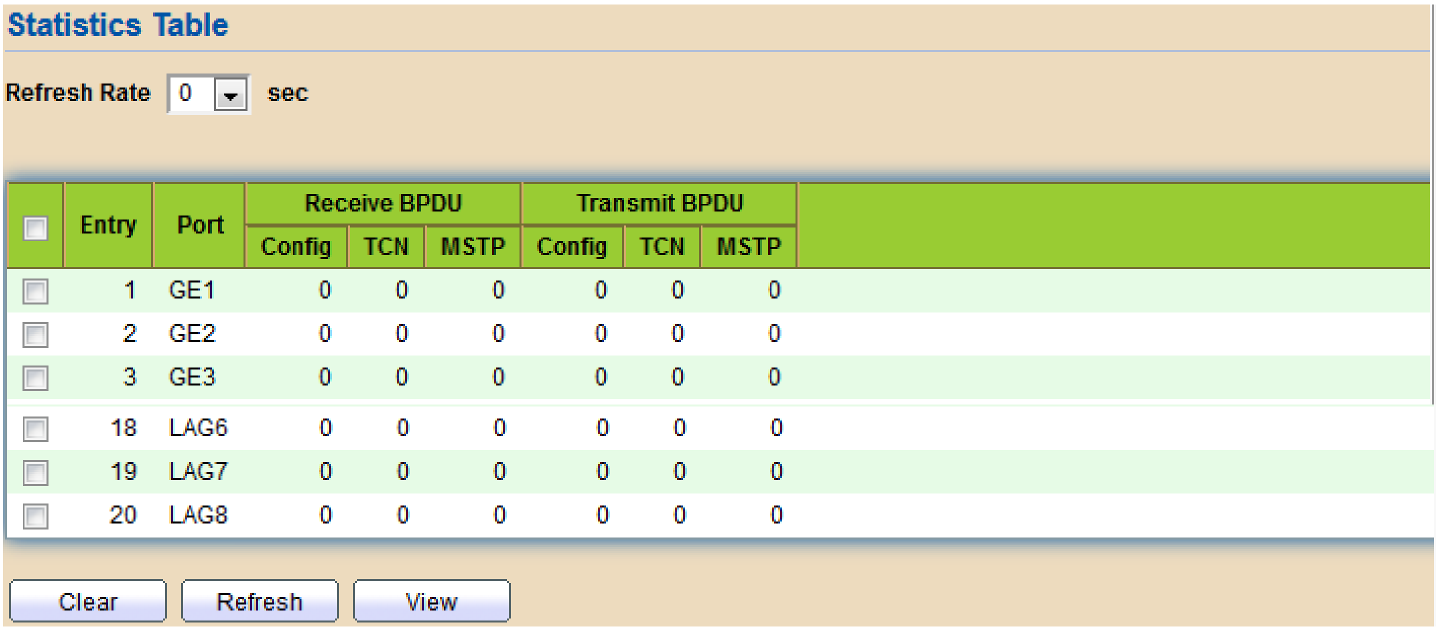
MSTI	0
Port	GE12
Path Cost	0 (0 - 200000000) (0 = Auto)
Priority	128
Port Role	Disabled
Port State	Disabled
Mode	RSTP
Type	Boundary
Designated Bridge	0-00:00:00:00:00:00
Designated Port ID	128-12
Designated Cost	20000
Remaining Hop	20

Figure 64 - 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.

4.7.5. Statistics

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



Statistics Table

Refresh Rate 0 sec

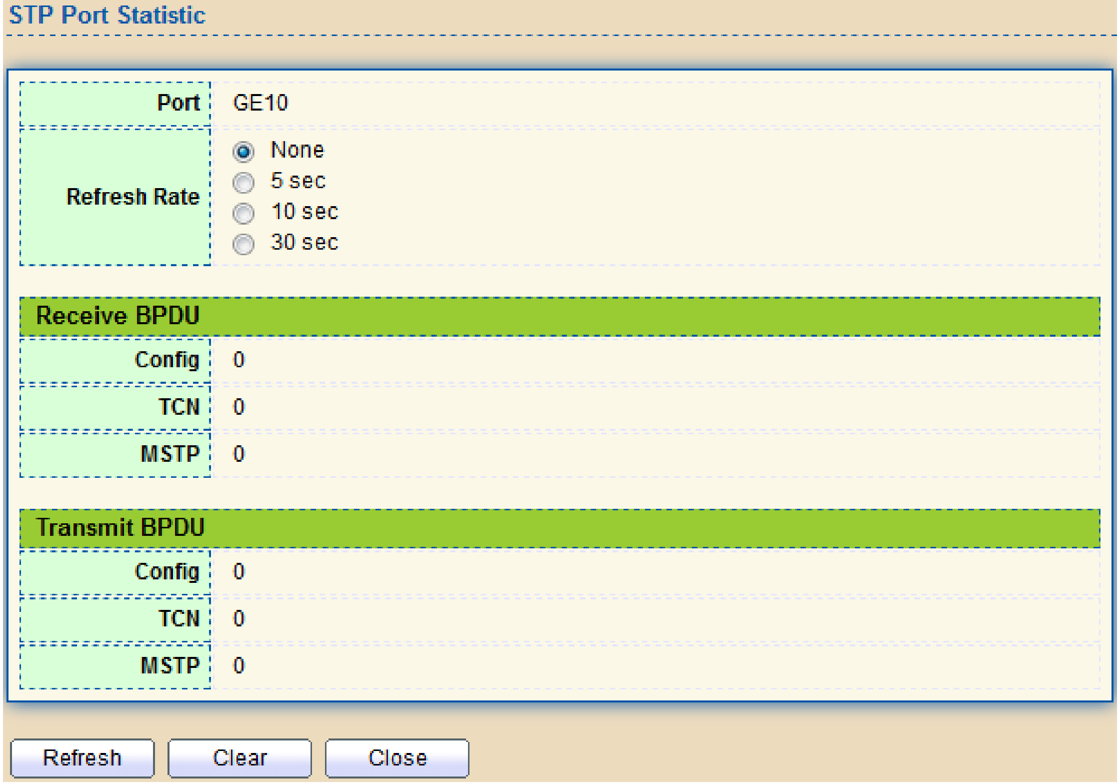
□	Entry	Port	Receive BPDU			Transmit BPDU		
			Config	TCN	MSTP	Config	TCN	MSTP
□	1	GE1	0	0	0	0	0	0
□	2	GE2	0	0	0	0	0	0
□	3	GE3	0	0	0	0	0	0
□	18	LAG6	0	0	0	0	0	0
□	19	LAG7	0	0	0	0	0	0
□	20	LAG8	0	0	0	0	0	0

Figure 65 - 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.



STP Port Statistic

Port	GE10
Refresh Rate	● None ○ 5 sec ○ 10 sec ○ 30 sec

Receive BPDU

Config	0
TCN	0
MSTP	0

Transmit BPDU

Config	0
TCN	0
MSTP	0

Figure 66 - 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.

4.8. Discovery

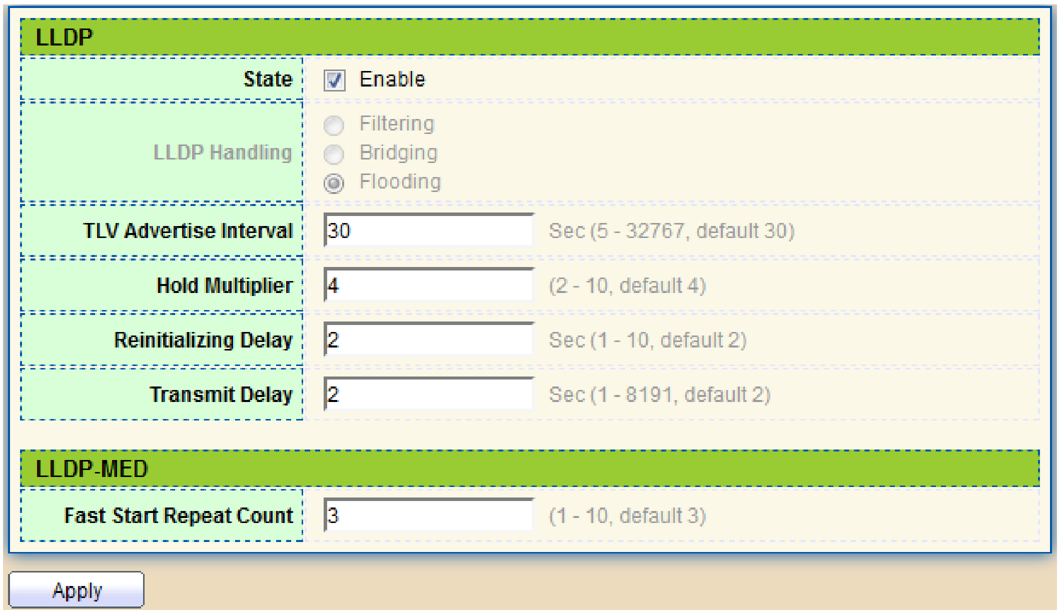
Use this section to configure LLDP.

4.8.1. LLDP

LLDP is a one-way protocol; there are no request/response sequences. Information 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.

4.8.1.1. Property

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



LLDP

State: ☑ Enable

LLDP Handling: ○ Filtering ○ Bridging ● Flooding

TLV Advertise Interval: 30 Sec (5 - 32767, default 30)

Hold Multiplier: 4 (2 - 10, default 4)

Reinitializing Delay: 2 Sec (1 - 10, default 2)

Transmit Delay: 2 Sec (1 - 8191, default 2)

LLDP-MED

Fast Start Repeat Count: 3 (1 - 10, default 3)

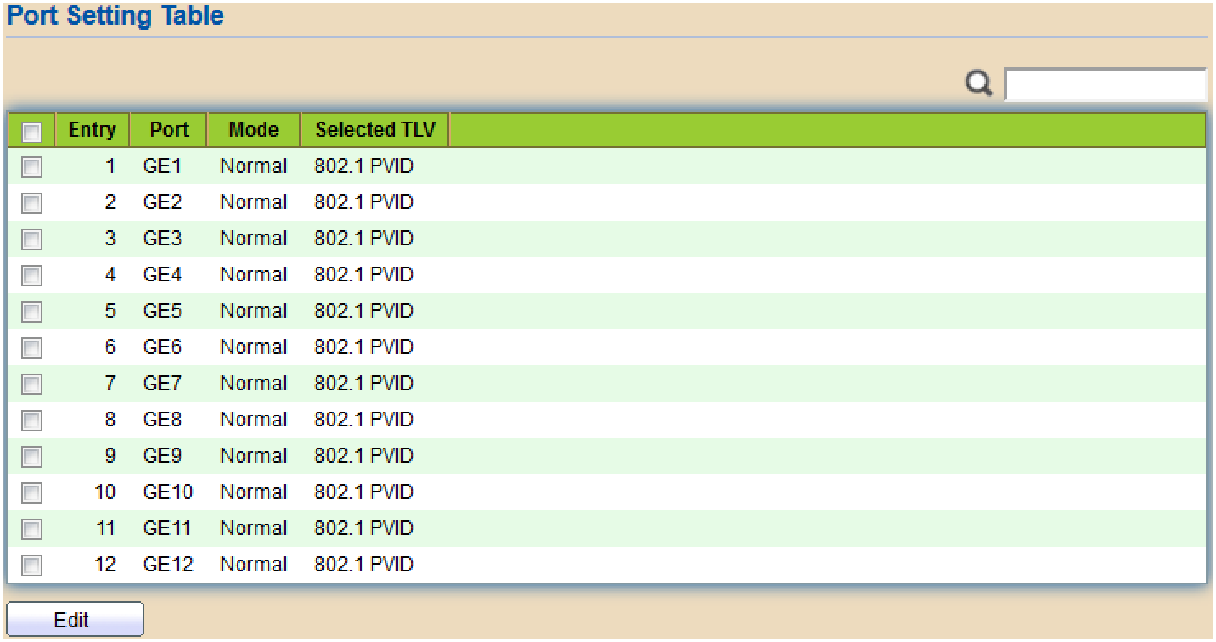
Figure 67 - Discovery > LLDP > Property

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 Interval	Select the interval at which frames are transmitted. The default is 30 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).

4.8.1.2. Port Setting

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



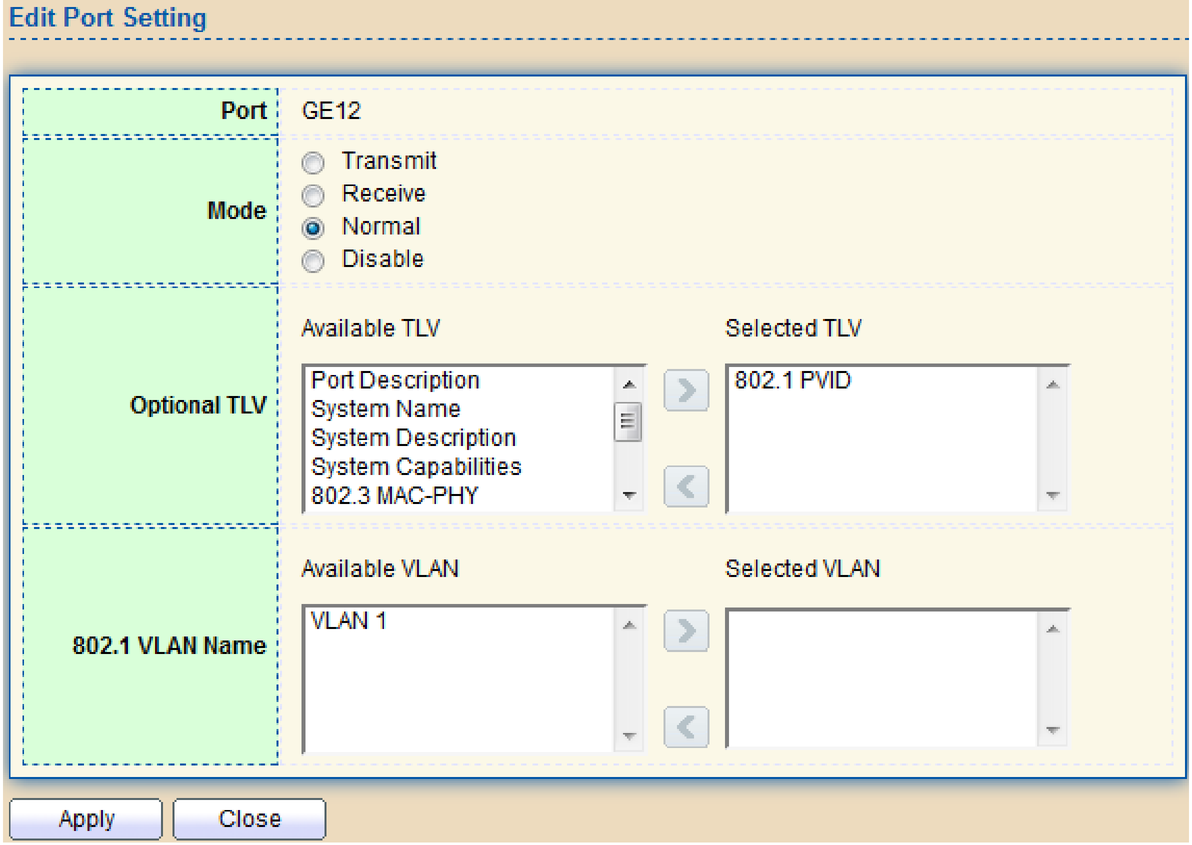
Port Setting Table

□	Entry	Port	Mode	Selected TLV
□	1	GE1	Normal	802.1 PVID
□	2	GE2	Normal	802.1 PVID
□	3	GE3	Normal	802.1 PVID
□	4	GE4	Normal	802.1 PVID
□	5	GE5	Normal	802.1 PVID
□	6	GE6	Normal	802.1 PVID
□	7	GE7	Normal	802.1 PVID
□	8	GE8	Normal	802.1 PVID
□	9	GE9	Normal	802.1 PVID
□	10	GE10	Normal	802.1 PVID
□	11	GE11	Normal	802.1 PVID
□	12	GE12	Normal	802.1 PVID

Figure 68 - Discovery > LLDP > Port Setting

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

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



Edit Port Setting

Port	GE12
Mode	○ Transmit ○ Receive ● Normal ○ Disable
Optional TLV	Available TLV: Port Description, System Name, System Description, System Capabilities, 802.3 MAC-PHY Selected TLV: 802.1 PVID
802.1 VLAN Name	Available VLAN: VLAN 1 Selected VLAN:

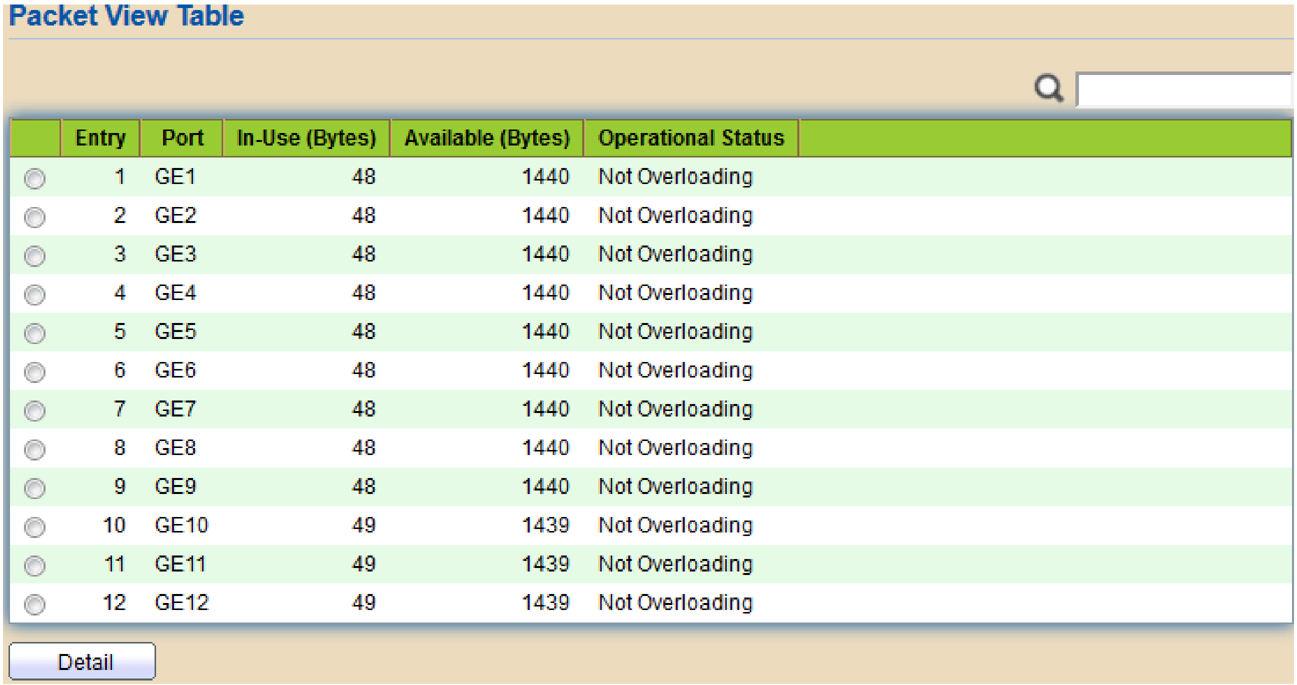
Figure 69 - Discovery > LLDP > Port Setting > Edit Port Setting

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).

4.8.1.3. Packet View

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



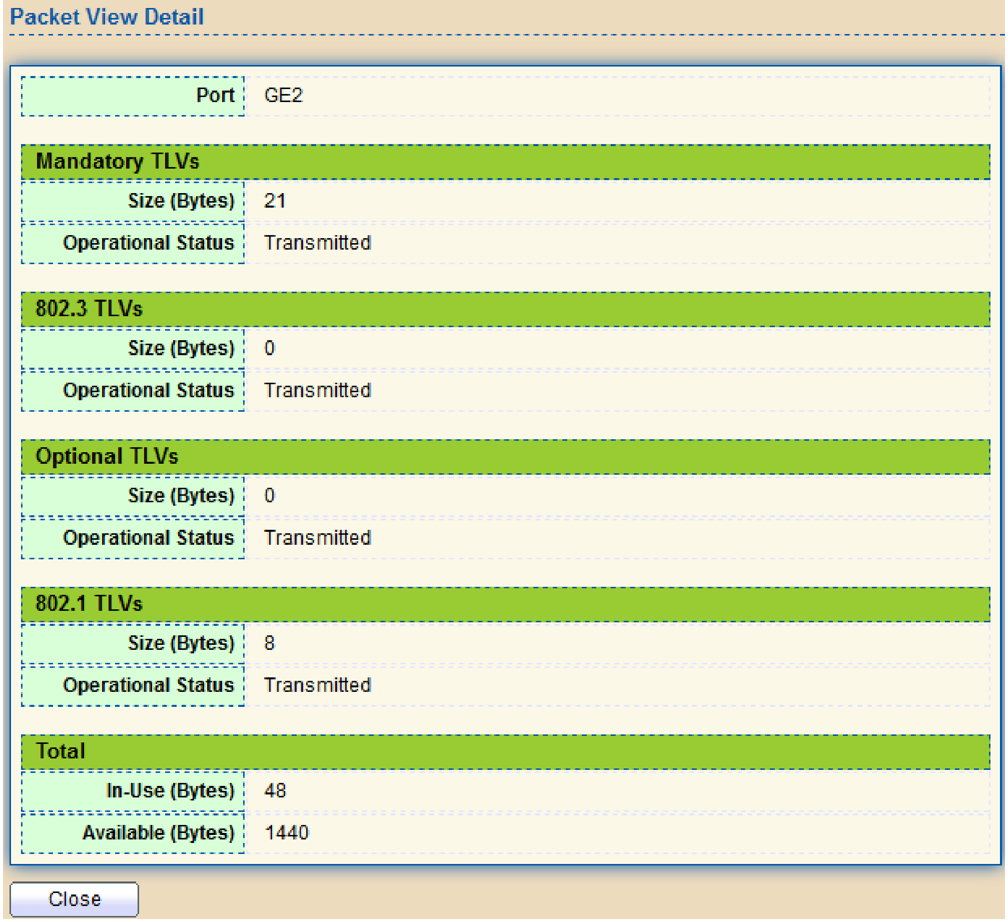
Packet View Table

	Entry	Port	In-Use (Bytes)	Available (Bytes)	Operational Status
○	1	GE1	48	1440	Not Overloading
○	2	GE2	48	1440	Not Overloading
○	3	GE3	48	1440	Not Overloading
○	4	GE4	48	1440	Not Overloading
○	5	GE5	48	1440	Not Overloading
○	6	GE6	48	1440	Not Overloading
○	7	GE7	48	1440	Not Overloading
○	8	GE8	48	1440	Not Overloading
○	9	GE9	48	1440	Not Overloading
○	10	GE10	49	1439	Not Overloading
○	11	GE11	49	1439	Not Overloading
○	12	GE12	49	1439	Not Overloading

Figure 70 - 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.



Packet View Detail

Port	GE2
Mandatory TLVs	
Size (Bytes)	21
Operational Status	Transmitted
802.3 TLVs	
Size (Bytes)	0
Operational Status	Transmitted
Optional TLVs	
Size (Bytes)	0
Operational Status	Transmitted
802.1 TLVs	
Size (Bytes)	8
Operational Status	Transmitted
Total	
In-Use (Bytes)	48
Available (Bytes)	1440

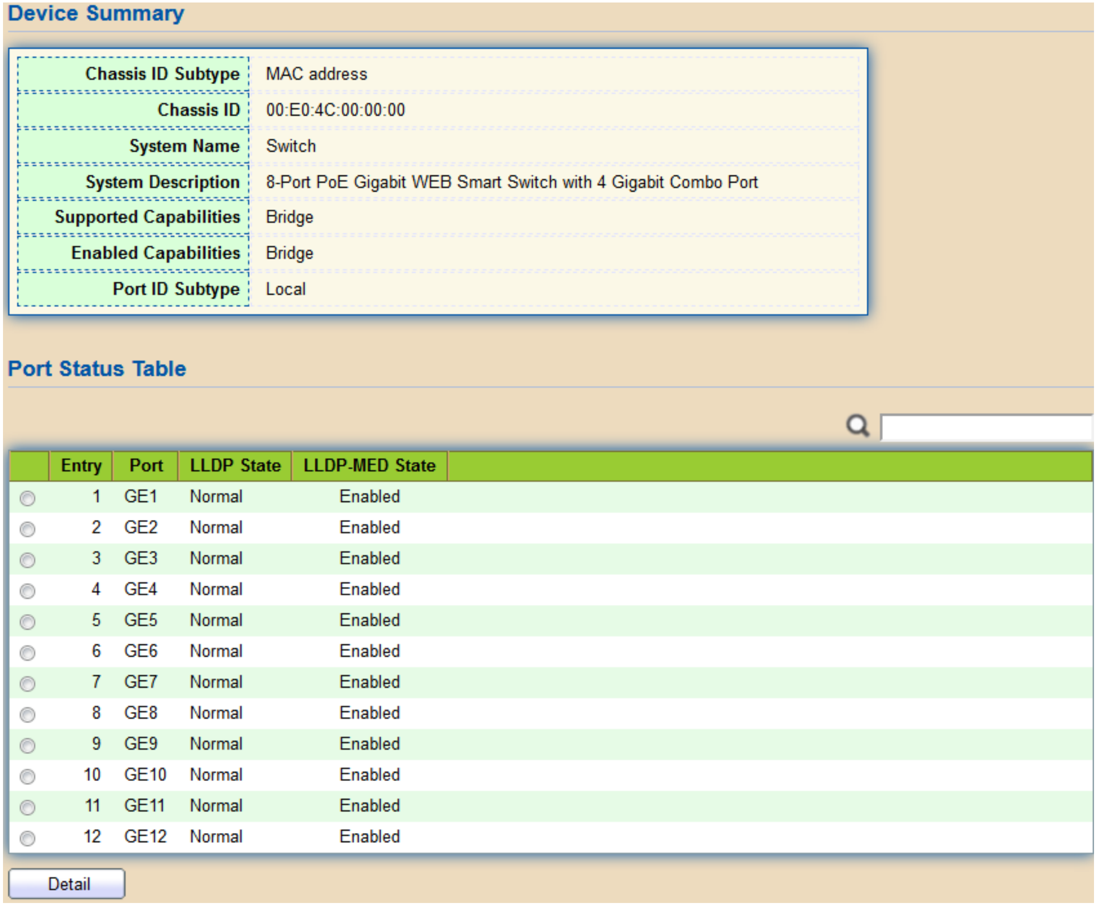
Figure 71 - Discovery > LLDP > Packet View > Packet View Detail

Item	Description
Port	Port Name.
Mandatory TLVs	Total mandatory TLV 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.

4.8.1.4. Local Information

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

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



Device Summary

Chassis ID Subtype	MAC address
Chassis ID	00:E0:4C:00:00:00
System Name	Switch
System Description	8-Port PoE Gigabit WEB Smart Switch with 4 Gigabit Combo Port
Supported Capabilities	Bridge
Enabled Capabilities	Bridge
Port ID Subtype	Local

Port Status Table

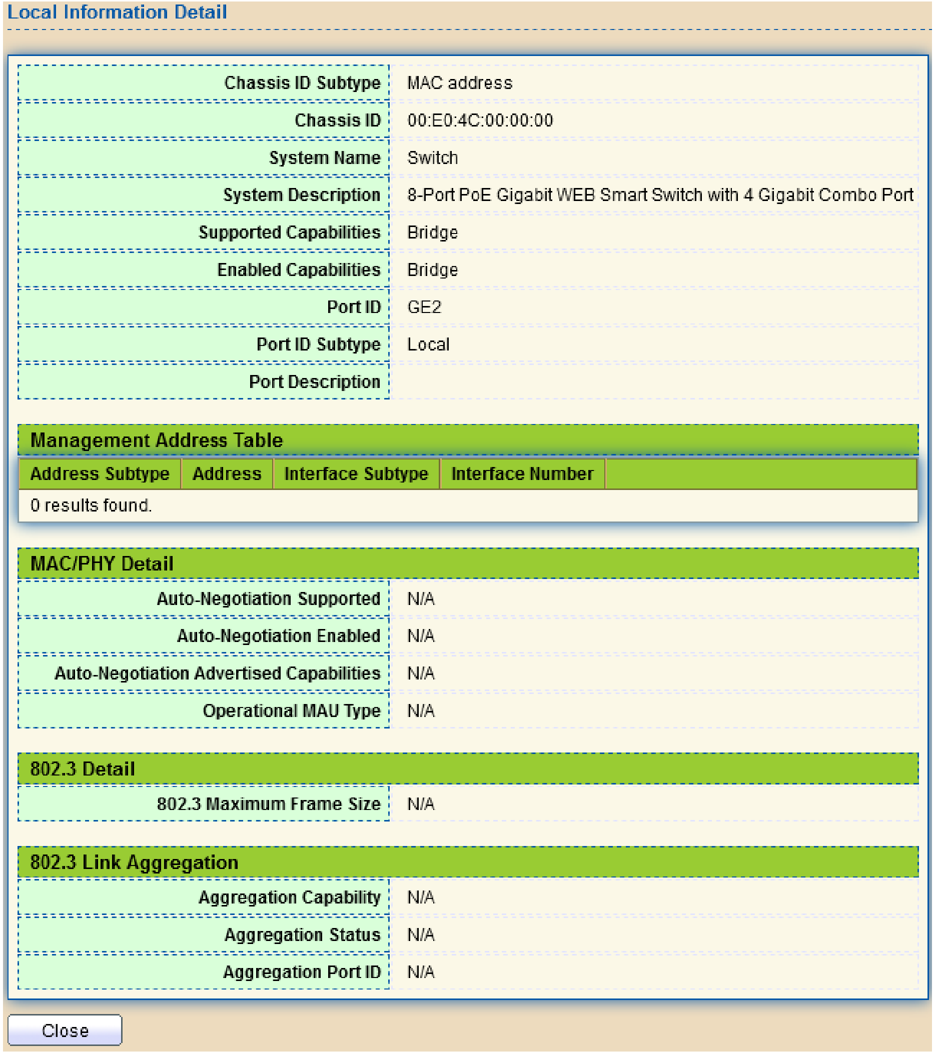
	Entry	Port	LLDP State	LLDP-MED State
○	1	GE1	Normal	Enabled
○	2	GE2	Normal	Enabled
○	3	GE3	Normal	Enabled
○	4	GE4	Normal	Enabled
○	5	GE5	Normal	Enabled
○	6	GE6	Normal	Enabled
○	7	GE7	Normal	Enabled
○	8	GE8	Normal	Enabled
○	9	GE9	Normal	Enabled
○	10	GE10	Normal	Enabled
○	11	GE11	Normal	Enabled
○	12	GE12	Normal	Enabled

Figure 72 - Discovery > LLDP > Local Information

Item	Descriptio n
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 Supported	Primary functions of the device, such as Bridge, WLAN AP, or Router.
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.



Local Information Detail

Chassis ID Subtype	MAC address
Chassis ID	00:E0:4C:00:00:00
System Name	Switch
System Description	8-Port PoE Gigabit WEB Smart Switch with 4 Gigabit Combo Port
Supported Capabilities	Bridge
Enabled Capabilities	Bridge
Port ID	GE2
Port ID Subtype	Local
Port Description	

Management Address Table

Address Subtype	Address	Interface Subtype	Interface Number
0 results found.			

MAC/PHY Detail

Auto-Negotiation Supported	N/A
Auto-Negotiation Enabled	N/A
Auto-Negotiation Advertised Capabilities	N/A
Operational MAU Type	N/A

802.3 Detail

802.3 Maximum Frame Size	N/A

802.3 Link Aggregation

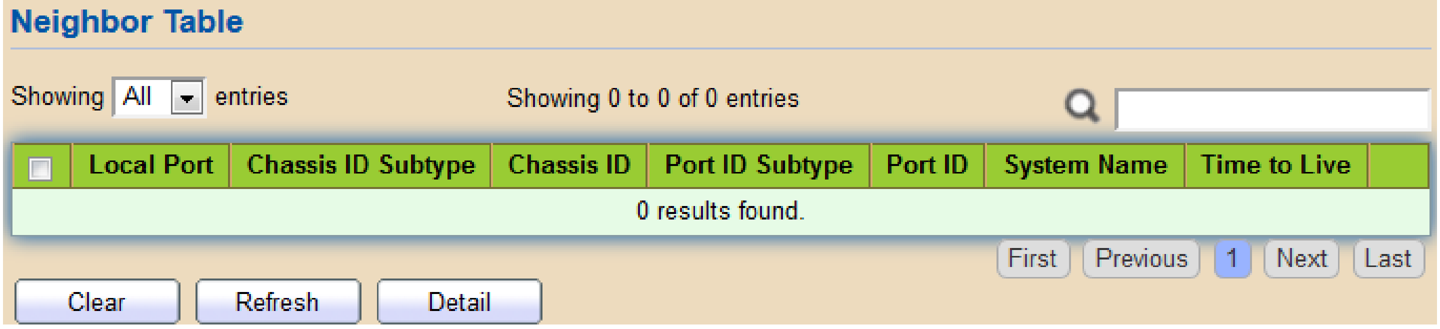
Aggregation Capability	N/A
Aggregation Status	N/A
Aggregation Port ID	N/A

Figure 73 - Discovery > LLDP > Local Information > Detail

4.8.1.5. Neighbor

Use the LLDP Neighbor page to view LLDP neighbors information.

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



Neighbor Table

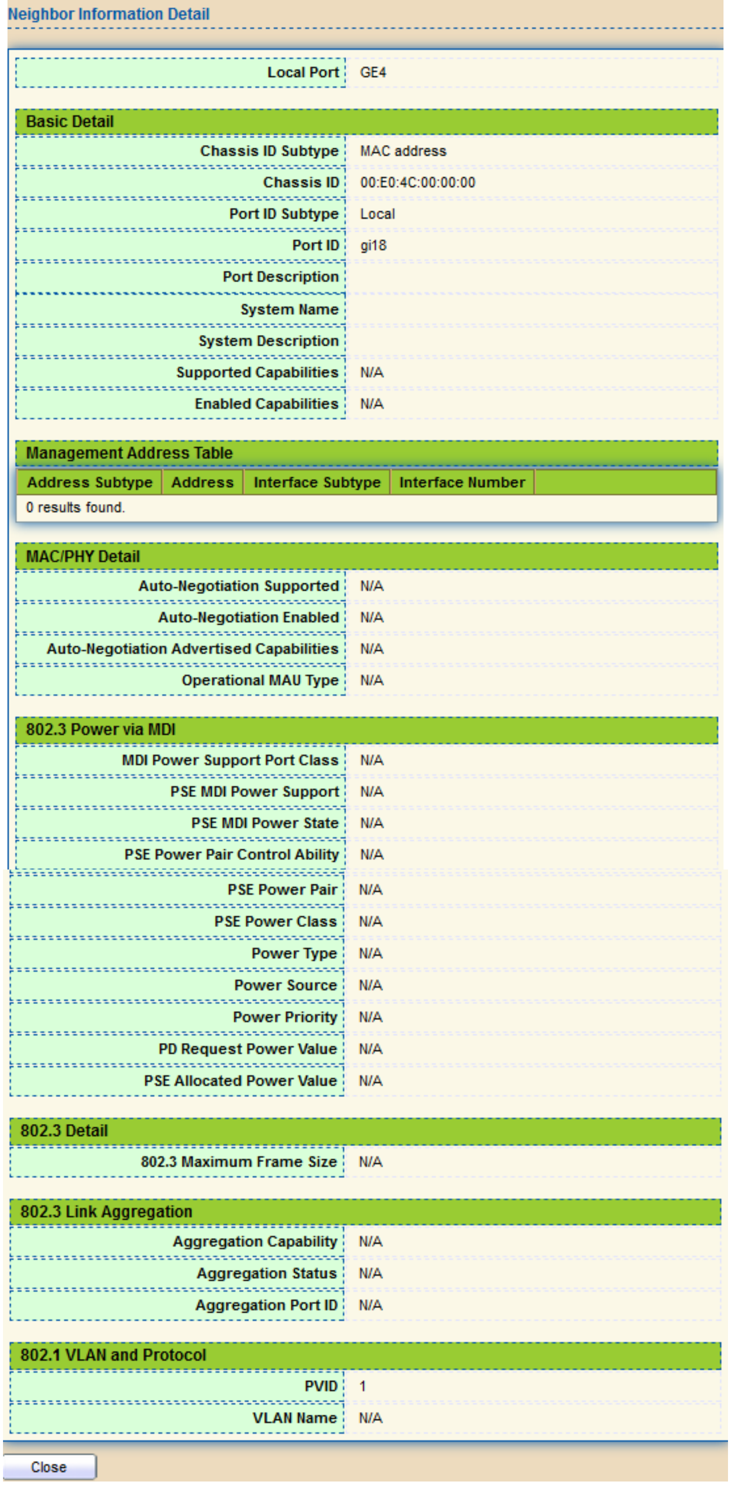
Showing All entries   Showing 0 to 0 of 0 entries

□	Local Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	System Name	Time to Live
0 results found.							

Figure 74 - 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



Neighbor Information Detail

Local Port	GE4

Basic Detail

Chassis ID Subtype	MAC address
Chassis ID	00:E0:4C:00:00:00
Port ID Subtype	Local
Port ID	gi18
Port Description	
System Name	
System Description	
Supported Capabilities	N/A
Enabled Capabilities	N/A

Management Address Table

Address Subtype	Address	Interface Subtype	Interface Number
0 results found.			

MAC/PHY Detail

Auto-Negotiation Supported	N/A
Auto-Negotiation Enabled	N/A
Auto-Negotiation Advertised Capabilities	N/A
Operational MAU Type	N/A

802.3 Power via MDI

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

802.3 Detail

802.3 Maximum Frame Size	N/A

802.3 Link Aggregation

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

802.1 VLAN and Protocol

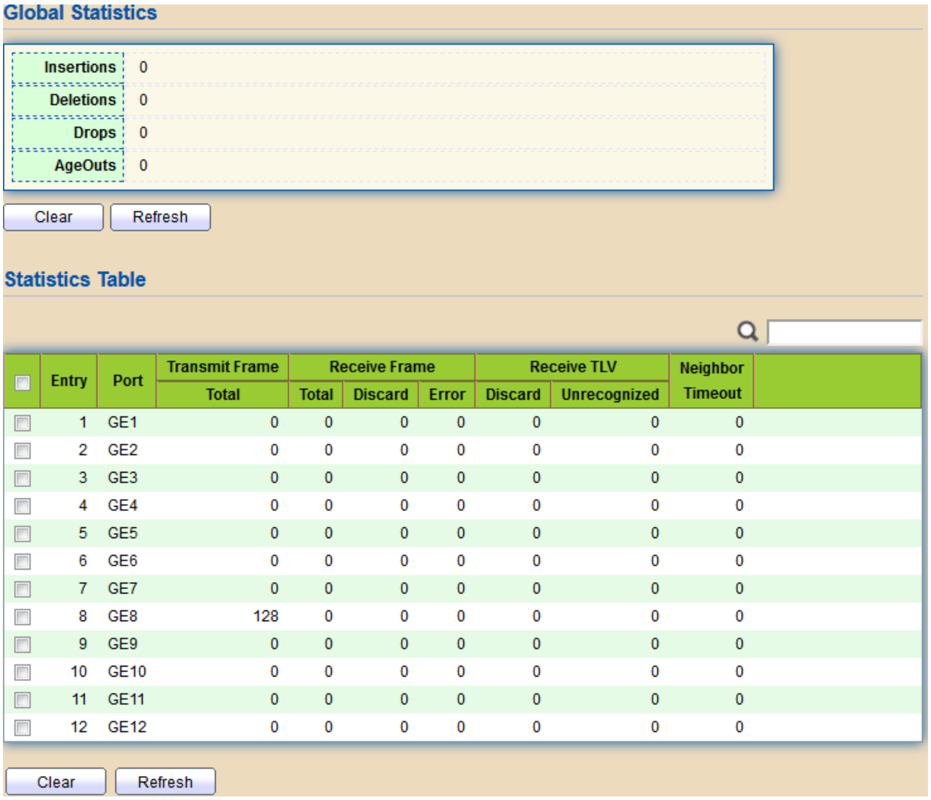
PVID	1
VLAN Name	N/A

Figure 75 LLDP Neighbor Detail Page

4.8.1.6. 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**.



Global Statistics

Insertions	0
Deletions	0
Drops	0
AgeOuts	0

Statistics Table

☐	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	128	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

Figure 76 - 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 unrecognized while the LLDP agent is enabled.
Neighbor Timeout	Number of age out LLDP frames.

4.9. Multicast

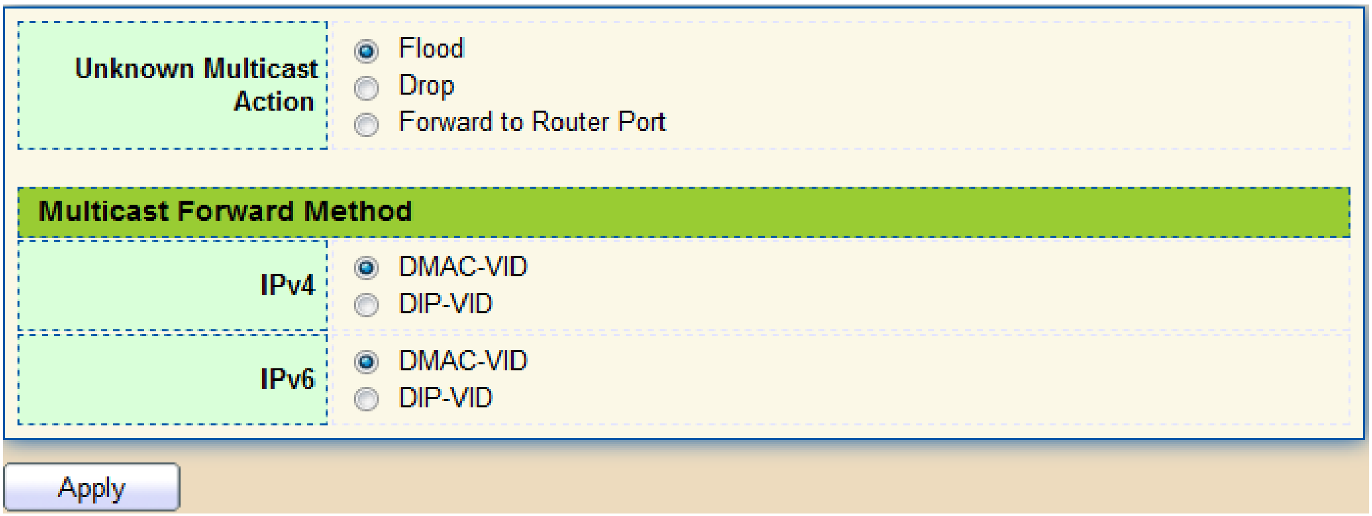
Use this section to configure Multicast.

4.9.1. General

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

4.9.1.1. Property

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



Unknown Multicast Action: ● Flood ○ Drop ○ Forward to Router Port

Multicast Forward Method

IPv4: ● DMAC-VID ○ DIP-VID

IPv6: ● DMAC-VID ○ DIP-VID

Figure 77 - Multicast > General > Property

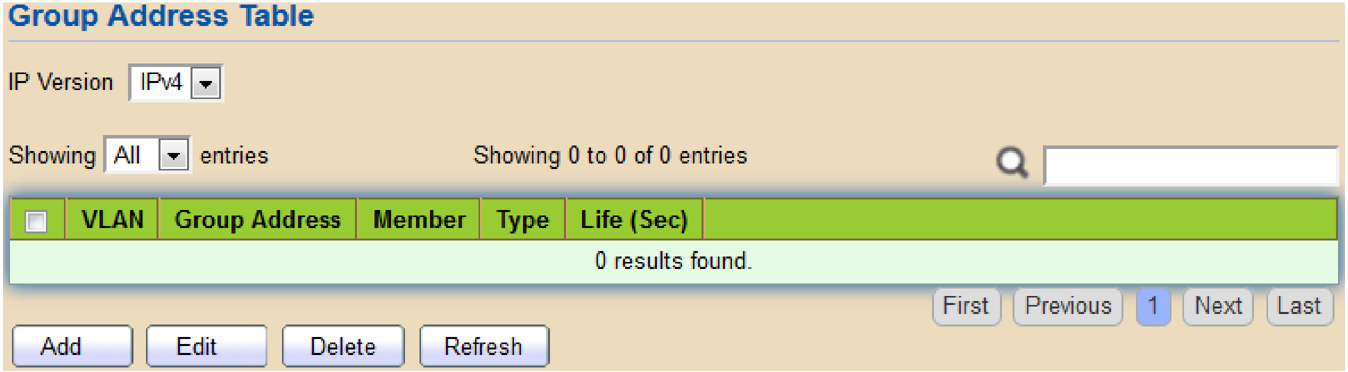
Item	Description
Unknown Multicast Action	Set the unknown multicast action • Flood: flood the unknown multicast data. • Drop: drop the unknown multicast data. • Router port: forward the unknown multicast data to router port.
IPv4	Set the ipv4 multicast forward method. • MAC-VID: forward method dmac+vid. • 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).

4.9.1.2. 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**


Group Address Table

IP Version: IPv4

Showing All entries Showing 0 to 0 of 0 entries

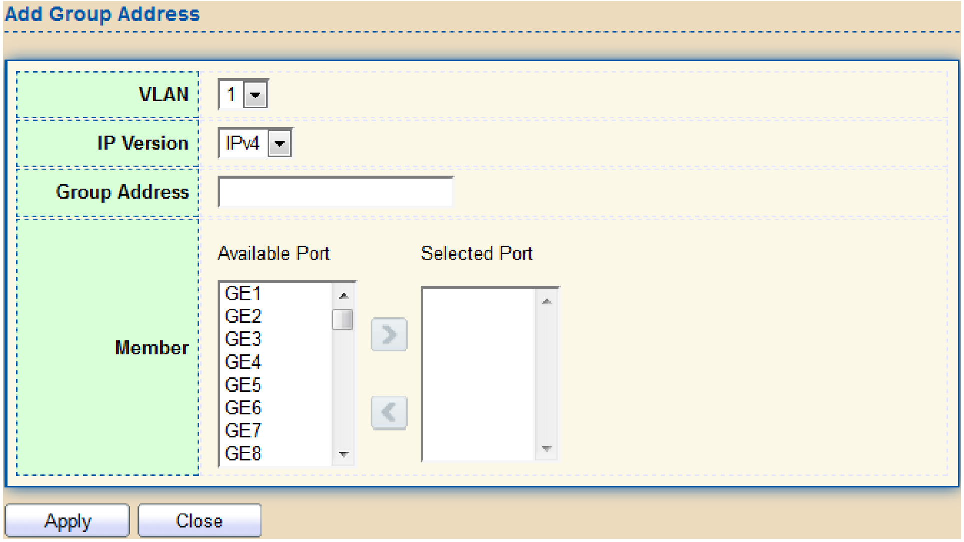
☐	VLAN	Group Address	Member	Type	Life (Sec)
0 results found.					

Figure 78 - 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.



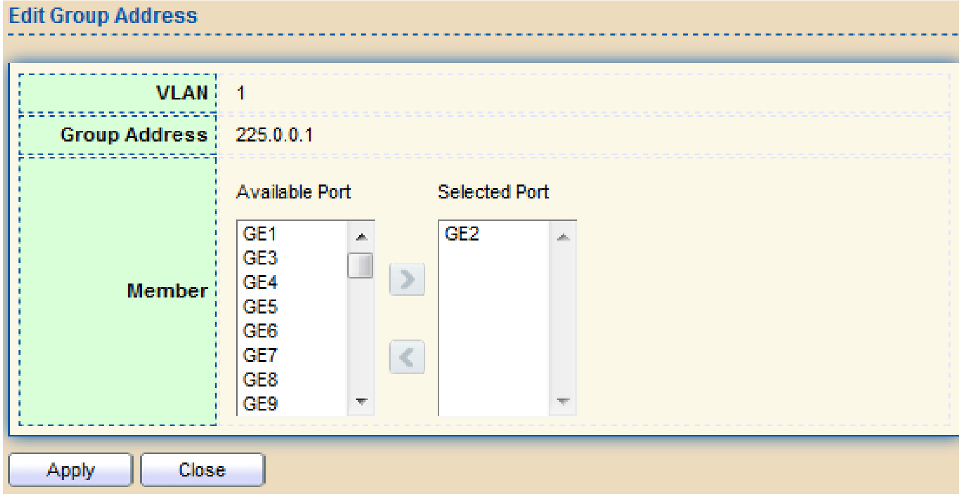
Add Group Address

VLAN: 1

IP Version: IPv4

Group Address:

Member



Edit Group Address

VLAN: 1

Group Address: 225.0.0.1

Member

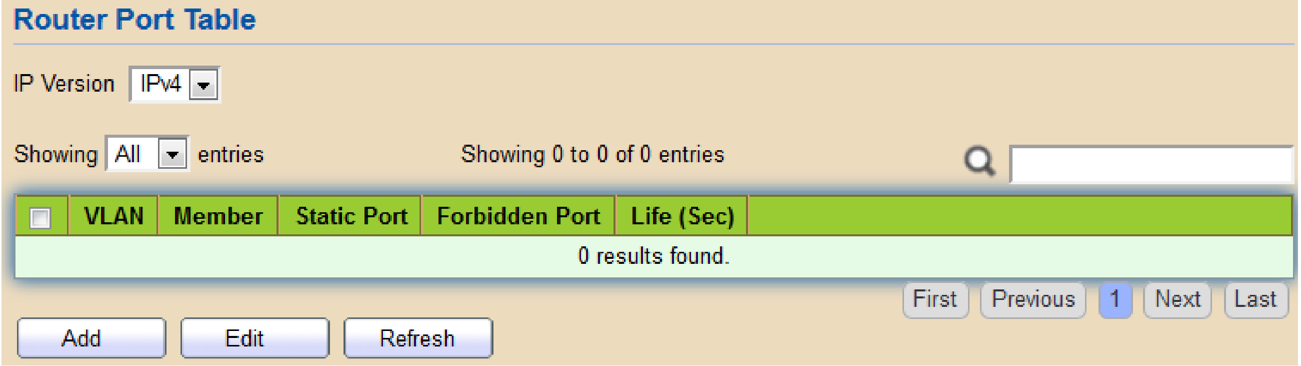
Figure 79 - Multicast > General > Group Address > Add/Edit Group Address

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

4.9.1.3. 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**



Router Port Table

IP Version: IPv4

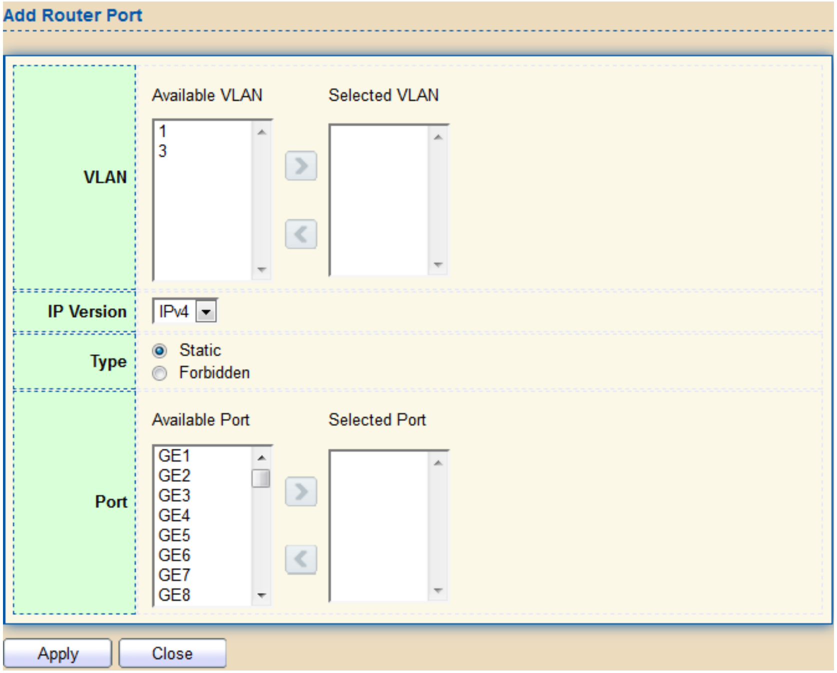
Showing All entries   Showing 0 to 0 of 0 entries

□	VLAN	Member	Static Port	Forbidden Port	Life (Sec)
0 results found.					

Figure 80 - 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.



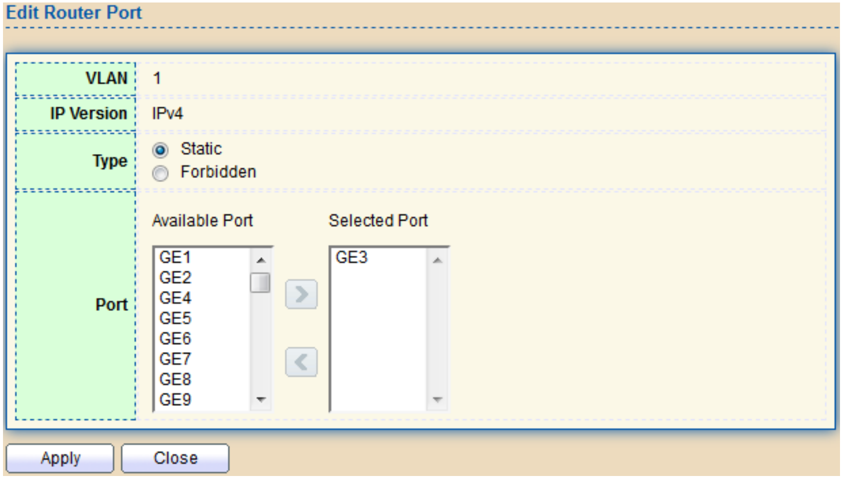
Add Router Port

VLAN: Available VLAN: 1, 3; Selected VLAN:

IP Version: IPv4

Type: ● Static ○ Forbidden

Port: Available Port: GE1, GE2, GE3, GE4, GE5, GE6, GE7, GE8; Selected Port:



Edit Router Port

VLAN	1
IP Version	IPv4
Type	● Static ○ Forbidden
Port	Available Port: GE1, GE2, GE4, GE5, GE6, GE7, GE8, GE9 Selected Port: GE3

Figure 81 - 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

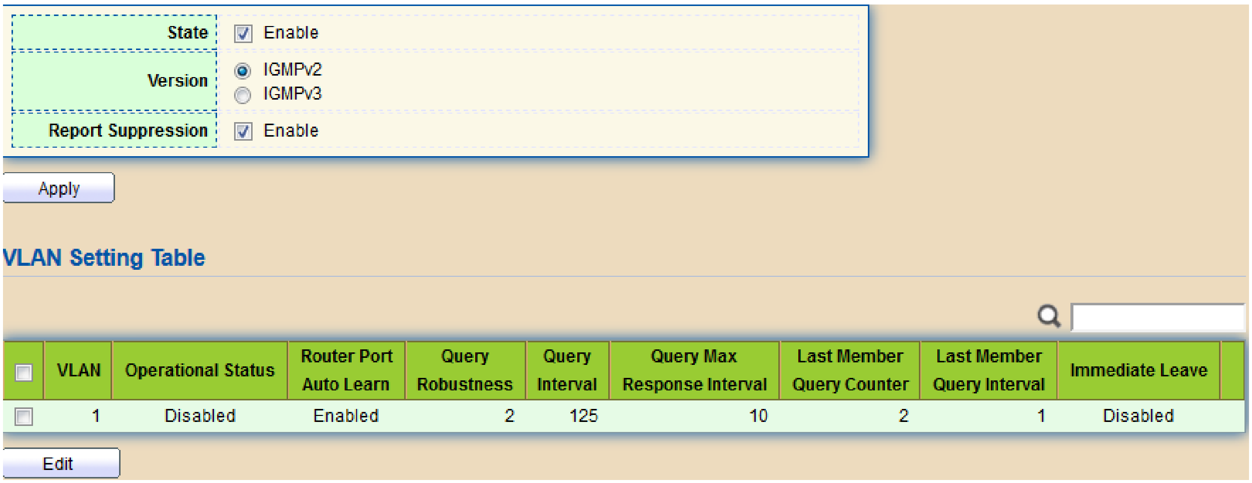
4.9.2. IGMP Snooping

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

4.9.2.1. 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**



State	☑ Enable
Version	● IGMPv2 ○ IGMPv3
Report Suppression	☑ Enable

Apply

VLAN Setting Table

□	VLAN	Operational Status	Router Port Auto Learn	Query Robustness	Query Interval	Query Max Response Interval	Last Member Query Counter	Last Member Query Interval	Immediate Leave
□	1	Disabled	Enabled	2	125	10	2	1	Disabled

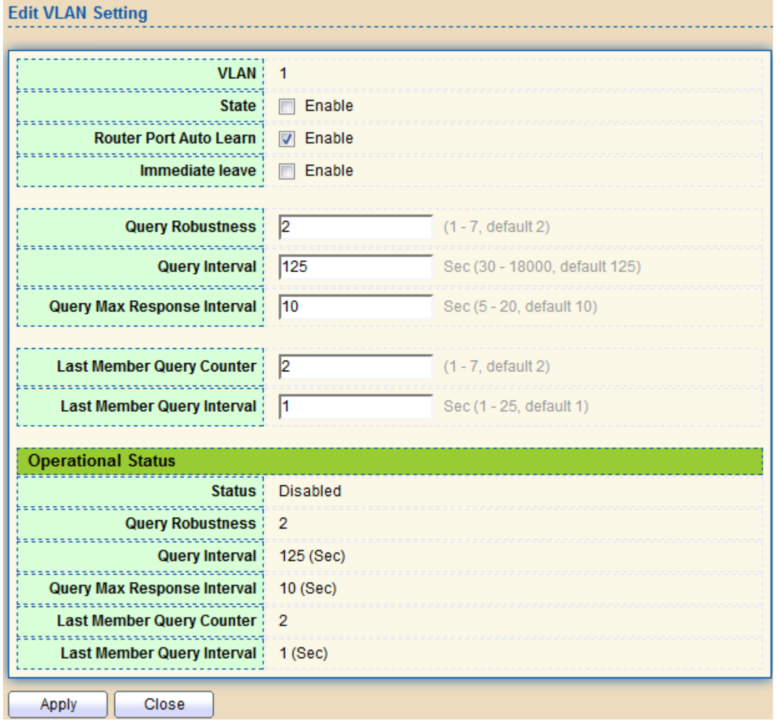
Edit

Figure 82 - 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.



Edit VLAN Setting

VLAN	1
State	□ Enable
Router Port Auto Learn	☑ Enable
Immediate leave	□ Enable
Query Robustness	2 (1 - 7, default 2)
Query Interval	125 Sec (30 - 18000, default 125)
Query Max Response Interval	10 Sec (5 - 20, default 10)
Last Member Query Counter	2 (1 - 7, default 2)
Last Member Query Interval	1 Sec (1 - 25, default 1)
Operational Status	
Status	Disabled
Query Robustness	2
Query Interval	125 (Sec)
Query Max Response Interval	10 (Sec)
Last Member Query Counter	2
Last Member Query Interval	1 (Sec)

Figure 83 - 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.

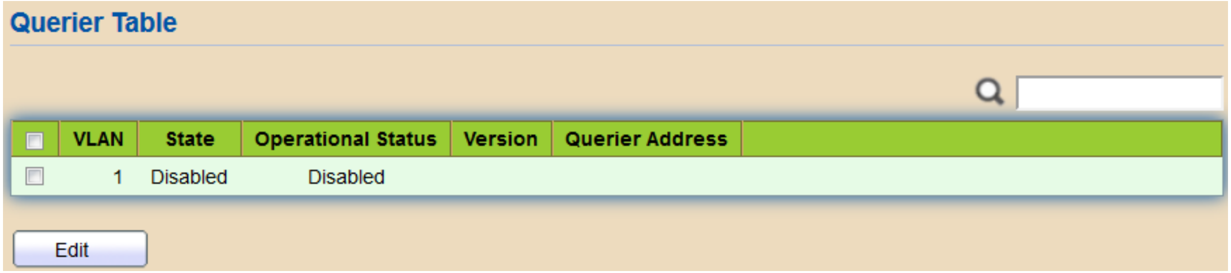
	- Enable: If checked Enable immediate leave, else disable immediate leave.
Query Robustness	The Admin Query Robustness allows tuning for the expected packet loss on a subnet.
Query Interval	The Admin interval of querier to send general query.
Query Max Response Interval	The Admin query max response interval, 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.

4.9.2.2. 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**



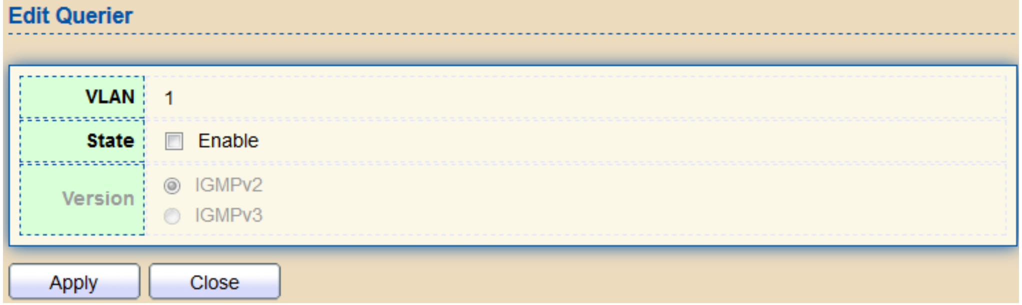
Querier Table

□	VLAN	State	Operational Status	Version	Querier Address
□	1	Disabled	Disabled		

Figure 84 - 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.



Edit Querier

VLAN	1
State	□ Enable
Version	● IGMPv2 ○ IGMPv3

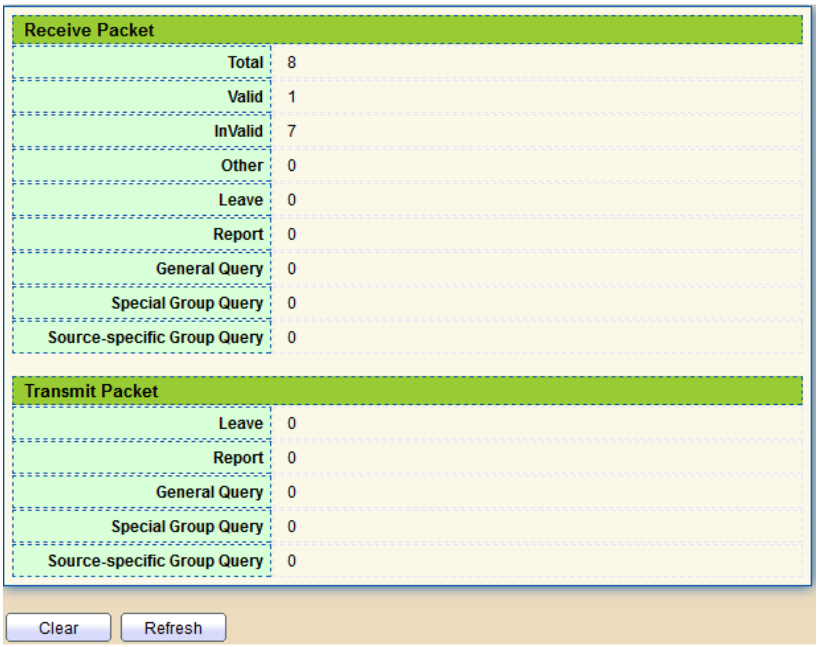
Figure 85 - Multicast > IGMP Snooping > Querier > Edit Querier

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)

4.9.2.3. Statistics

This page allow user to clear igmp snooping statics.

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



Receive Packet	
Total	8
Valid	1
InValid	7
Other	0
Leave	0
Report	0
General Query	0
Special Group Query	0
Source-specific Group Query	0

Transmit Packet	
Leave	0
Report	0
General Query	0
Special Group Query	0
Source-specific Group Query	0

Figure 96 - 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.

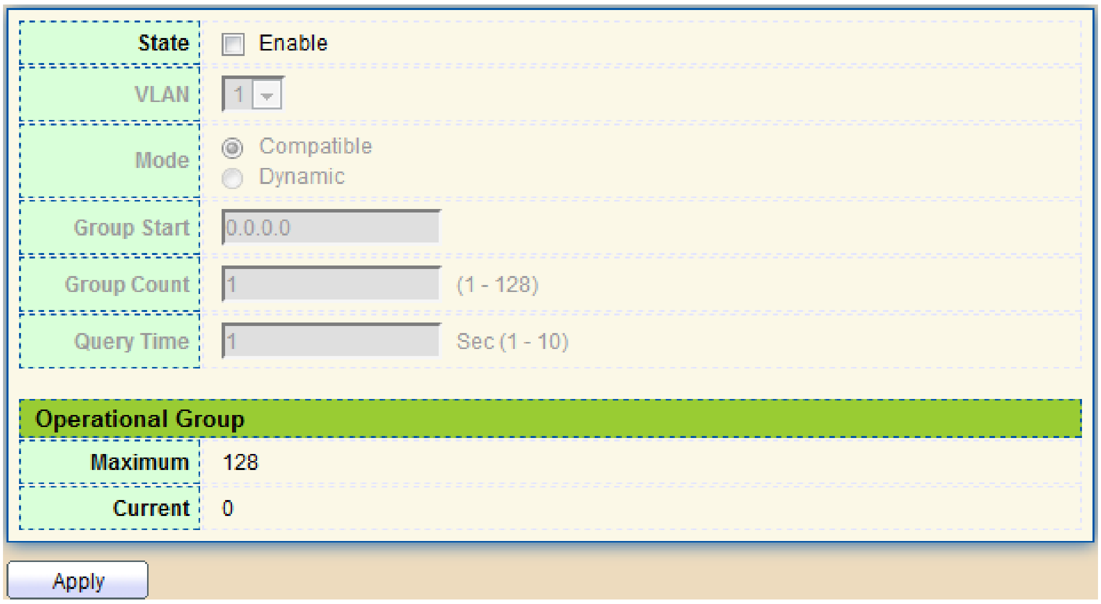
Source-specific Group Query	IGMP Special Source and Group General Query packet.
Transmit Packet	
Leave	IGMP leave packet
Report	IGMP join and report packet
General Query	IGMP general query packet include querier transmit general query packet.
Special Group Query	IGMP special group query packet include querier transmit special group query packet.
Source-specific Group Query	IGMP Special Source and Group General Query packet.

4.9.4 MVR

Use the MVR pages to configure settings of MVR function.

4.9.4.1. Property

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



State	□ Enable
VLAN	1
Mode	● Compatible ○ Dynamic
Group Start	0.0.0.0
Group Count	1 (1 - 128)
Query Time	1 Sec (1 - 10)

Operational Group

Maximum	128
Current	0

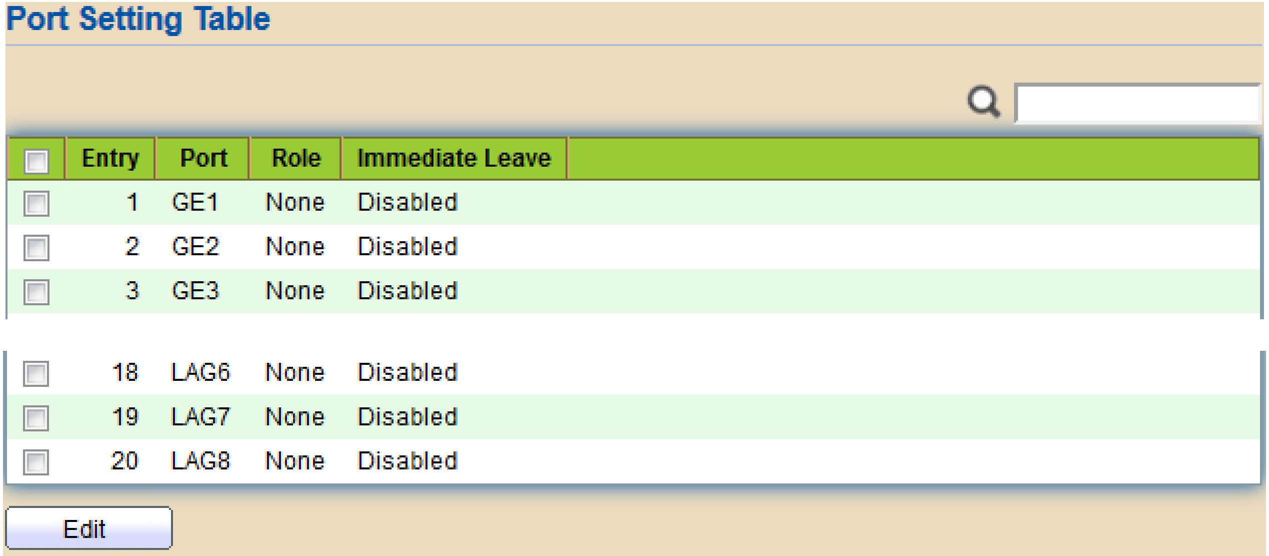
Figure 87 - Multicast > MVR > Property

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: dynamic mode, will 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

4.9.4.2. 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**



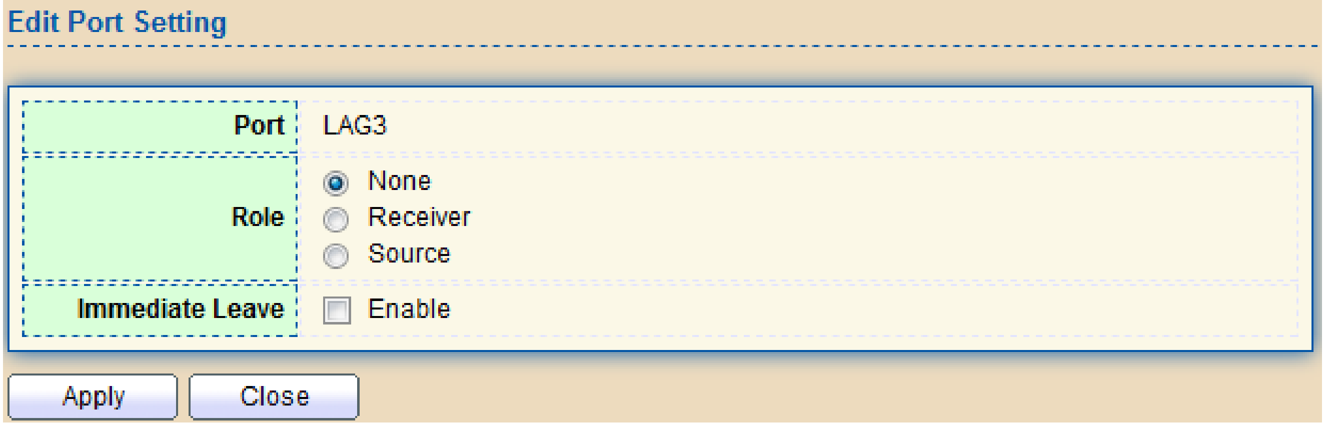
Port Setting Table

□	Entry	Port	Role	Immediate Leave
□	1	GE1	None	Disabled
□	2	GE2	None	Disabled
□	3	GE3	None	Disabled
□	18	LAG6	None	Disabled
□	19	LAG7	None	Disabled
□	20	LAG8	None	Disabled

Figure 88 - 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.



Edit Port Setting

Port	LAG3
Role	● None ○ Receiver ○ Source
Immediate Leave	□ Enable

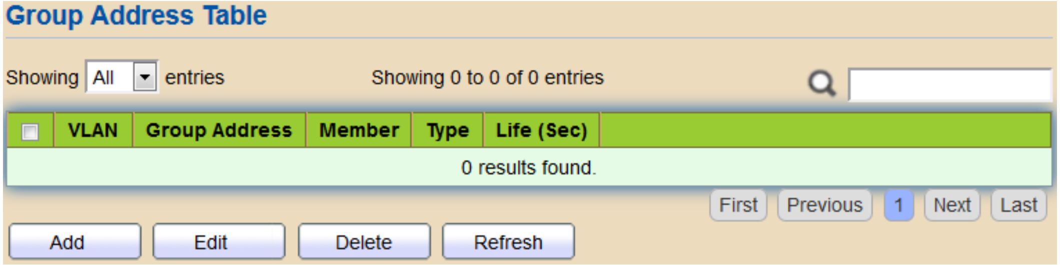
Figure 89 - Multicast > MVR > Port Setting > Edit Port Setting

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.

4.9.4.3. 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**



Group Address Table

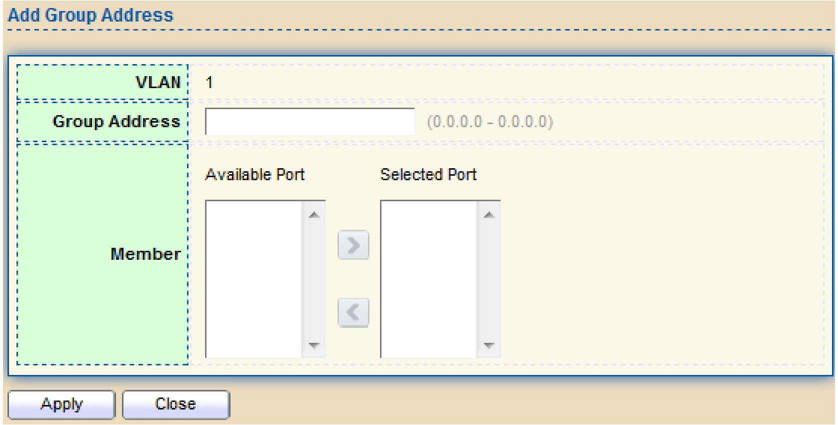
Showing All entries Showing 0 to 0 of 0 entries

□	VLAN	Group Address	Member	Type	Life (Sec)
0 results found.					

Figure 90 - Multicast > MVR > Group Address

Item 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 Group Address Table menu.



Add Group Address

VLAN 1

Group Address (0.0.0.0 - 0.0.0.0)

Member

Figure 91 - 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

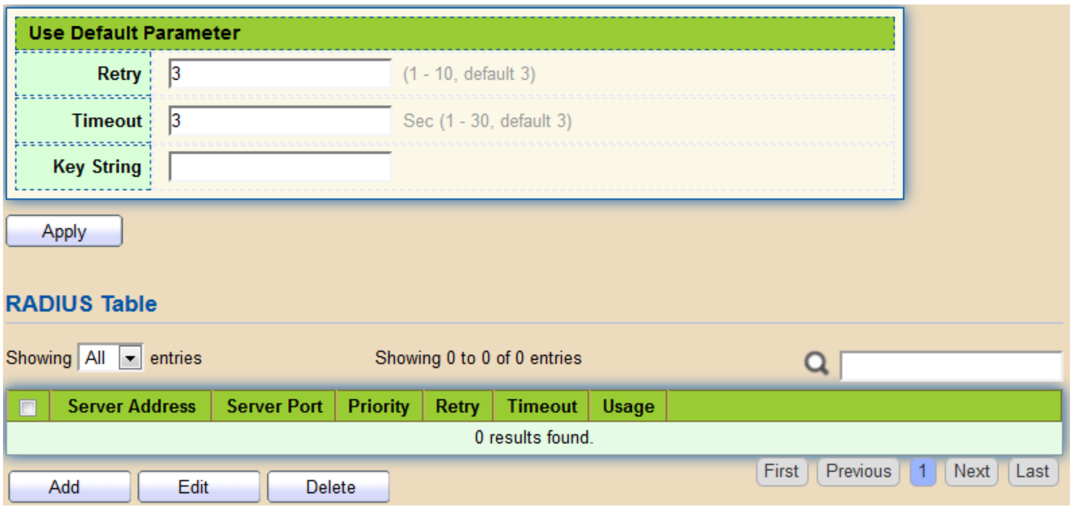
4.10. Security

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

4.10.1. 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**



Use Default Parameter

Retry	3	(1 - 10, default 3)
Timeout	3	Sec (1 - 30, default 3)
Key String		

Apply

RADIUS Table

Showing All entries   Showing 0 to 0 of 0 entries

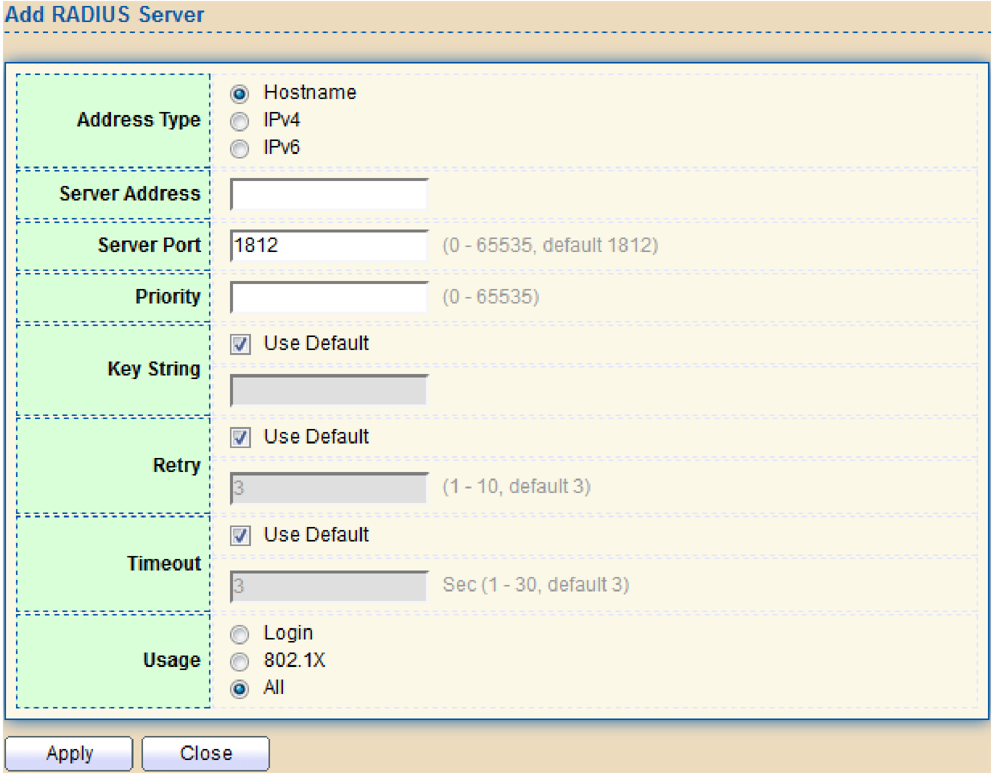
□	Server Address	Server Port	Priority	Retry	Timeout	Usage
0 results found.						

Add Edit Delete   First Previous 1 Next Last

Figure 92 - Security > RADIUS

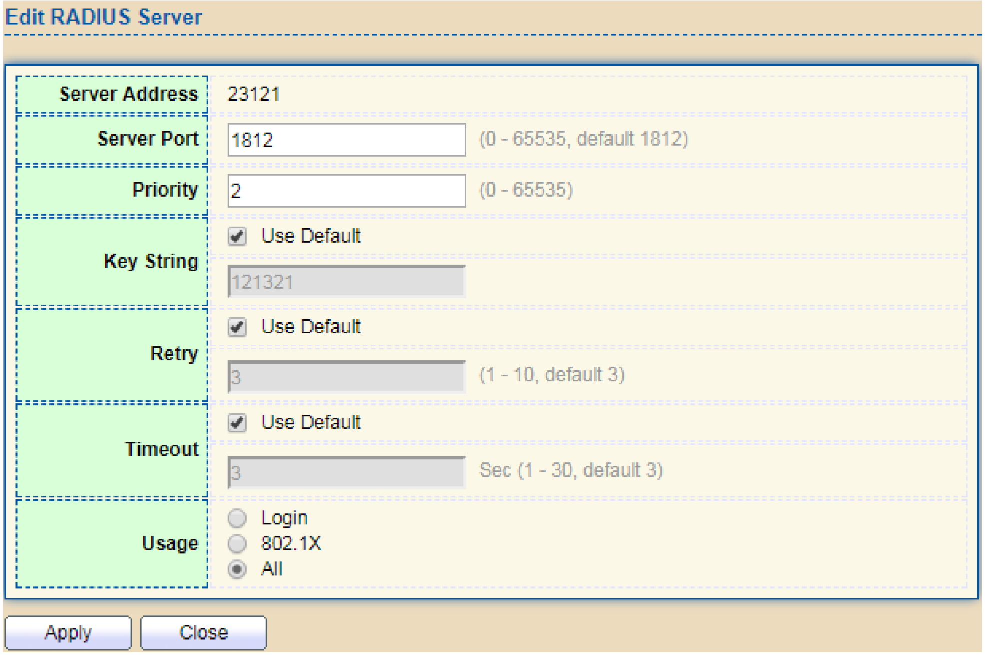
Item	Description
Retry	Set default retry number.
Timeout	Set default timeout value.
Key String	Set default RADIUS key string
RADIUS Table	
Server Address	RADIUS server address.
Server Port	RADIUS server port.
Priority	RADIUS server priority (smaller value has higher priority). RADIUS session will try 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 authentication. • 802.1x: For 802.1x authentication. • All: For all types.

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



Add RADIUS Server

Address Type	● Hostname ○ IPv4 ○ IPv6
Server Address	
Server Port	1812 (0 - 65535, default 1812)
Priority	(0 - 65535)
Key String	☑ Use Default
Retry	☑ Use Default 3 (1 - 10, default 3)
Timeout	☑ Use Default 3 Sec (1 - 30, default 3)
Usage	○ Login ○ 802.1X ● All



Edit RADIUS Server

Server Address	23121
Server Port	1812 (0 - 65535, default 1812)
Priority	2 (0 - 65535)
Key String	☑ Use Default 121321
Retry	☑ Use Default 3 (1 - 10, default 3)
Timeout	☑ Use Default 3 Sec (1 - 30, default 3)
Usage	○ Login ○ 802.1X ● All

Figure 93 - 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 authentication. • 802.1x: For 802.1x authentication. • All: For all types.

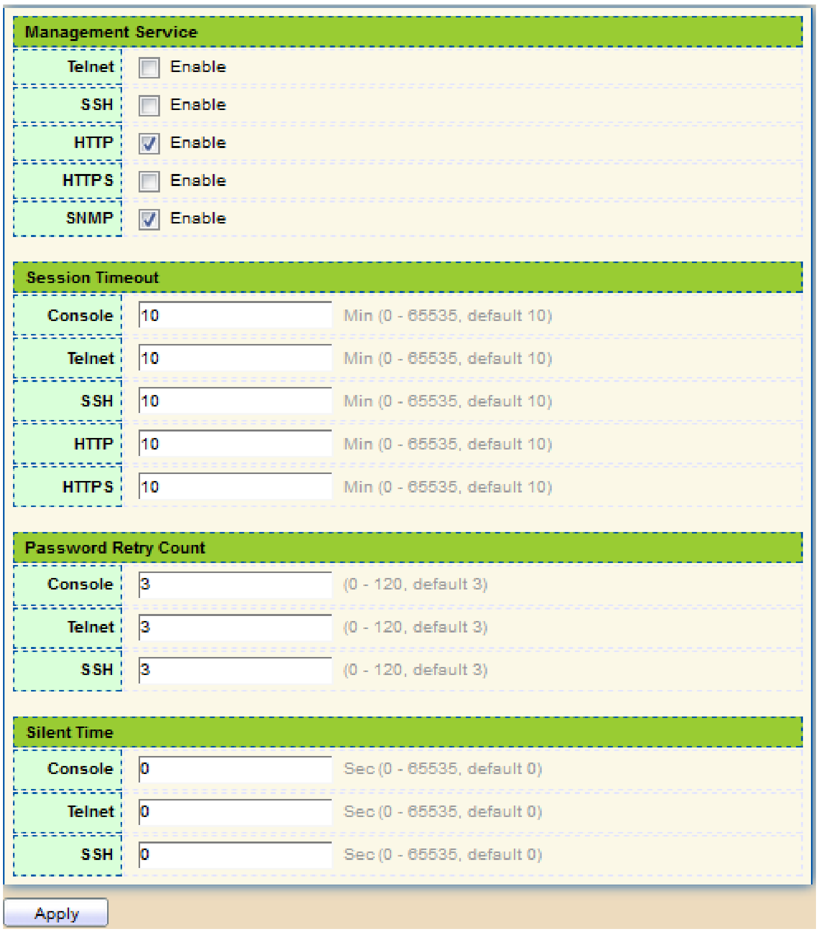
4.10.2. Management Access

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

4.10.2.1. Management Service

This page allow user to change management services related configurations.

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



Management Service

Telnet	□ Enable
SSH	□ Enable
HTTP	☑ Enable
HTTPS	□ Enable
SNMP	☑ Enable

Session Timeout

Console	10	Min (0 - 65535, default 10)
Telnet	10	Min (0 - 65535, default 10)
SSH	10	Min (0 - 65535, default 10)
HTTP	10	Min (0 - 65535, default 10)
HTTPS	10	Min (0 - 65535, default 10)

Password Retry Count

Console	3	(0 - 120, default 3)
Telnet	3	(0 - 120, default 3)
SSH	3	(0 - 120, default 3)

Silent Time

Console	0	Sec (0 - 65535, default 0)
Telnet	0	Sec (0 - 65535, default 0)
SSH	0	Sec (0 - 65535, default 0)

Figure 94 - 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 Count	Retry count is the number which CLI password input error tolerance count. After input error password exceeds this count, the CLI will freeze after silent time.
Silent Time	After input error password exceeds password retry count, the CLI will freeze after silent time.

4.10.2.2. 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**

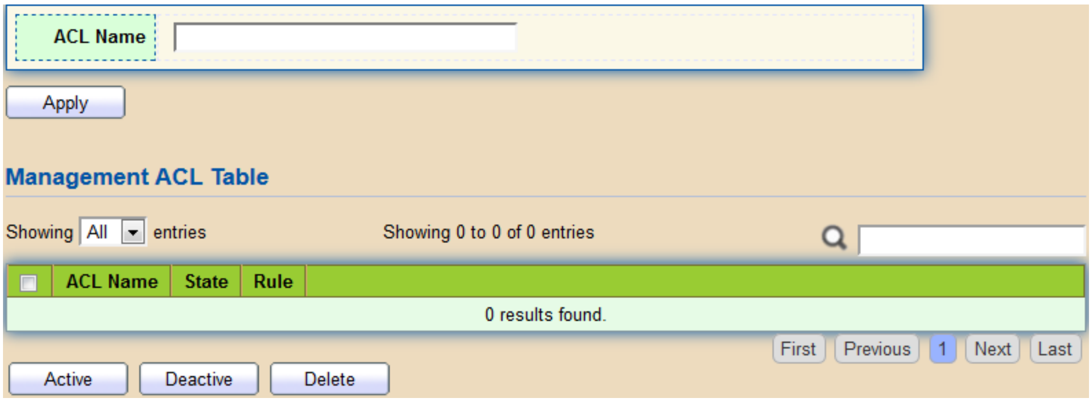


Figure 95 - Security > Management Access > Management ACL

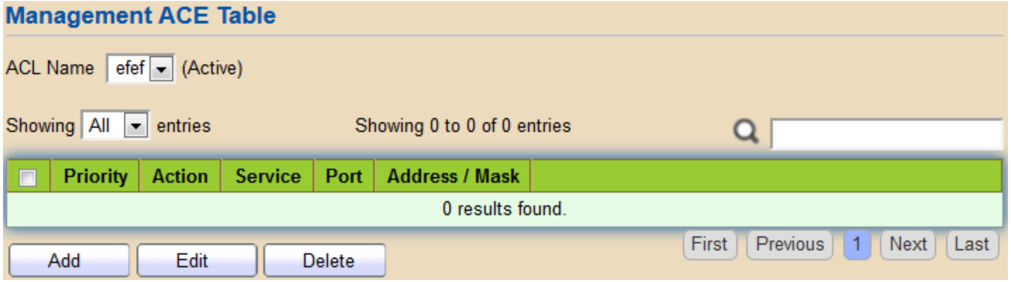
Item	Description
ACL Name	Input MAC ACL name.
Management ACL	
ACL Name	Display Management ACL name.

State	Display Management ACL whether active.
Rule	Display the number Management ACE rule of ACL.

4.10.2.3. 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**



Management ACE Table

ACL Name efef (Active)

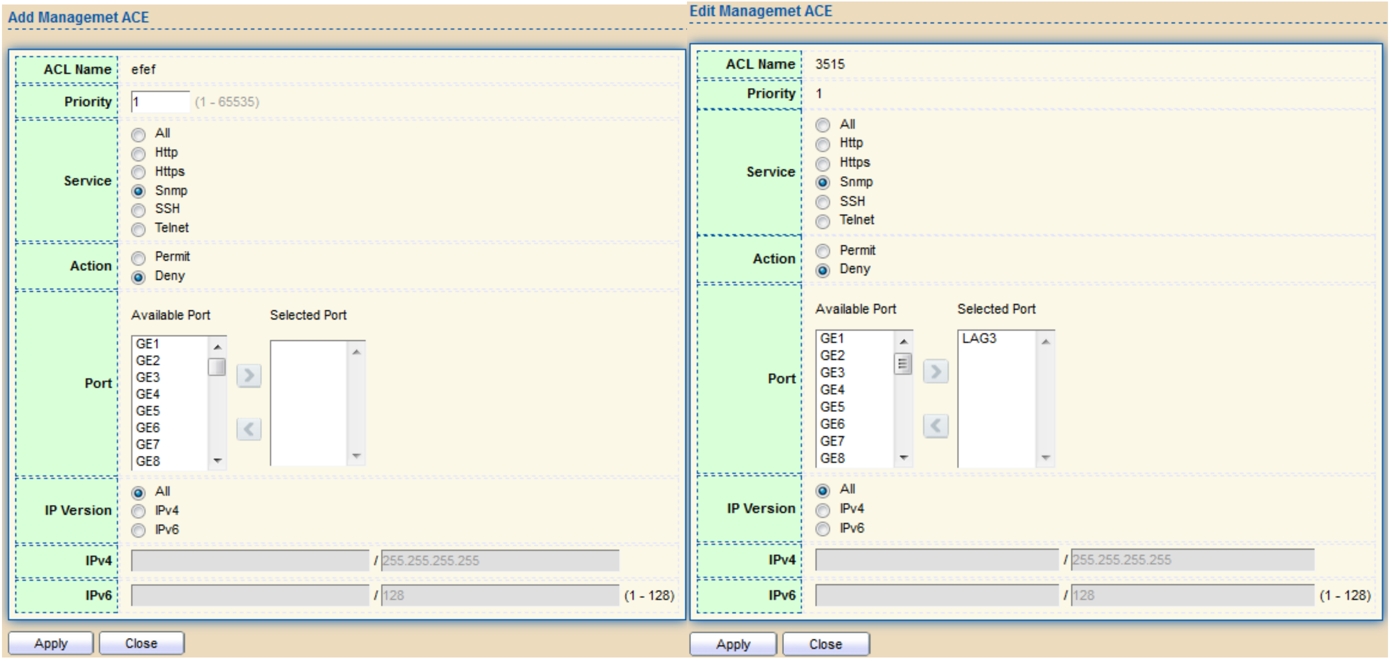
Showing All entries Showing 0 to 0 of 0 entries

□	Priority	Action	Service	Port	Address / Mask
0 results found.					

Figure 96 - 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.



Add Managemet ACE

ACL Name	efef
Priority	1 (1 - 65535)
Service	○ All ○ Http ○ Https ● Snmp ○ SSH ○ Telnet
Action	○ Permit ● Deny
Port	Available Port: GE1, GE2, GE3, GE4, GE5, GE6, GE7, GE8 Selected Port:
IP Version	● All ○ IPv4 ○ IPv6
IPv4	/ 255.255.255.255
IPv6	/ 128 (1 - 128)

Apply Close

Edit Managemet ACE

ACL Name	3515
Priority	1
Service	○ All ○ Http ○ Https ● Snmp ○ SSH ○ Telnet
Action	○ Permit ● Deny
Port	Available Port: GE1, GE2, GE3, GE4, GE5, GE6, GE7, GE8 Selected Port: LAG3
IP Version	● All ○ IPv4 ○ IPv6
IPv4	/ 255.255.255.255
IPv6	/ 128 (1 - 128)

Apply Close

Figure 97 - Security > Management Access > Add 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. ・

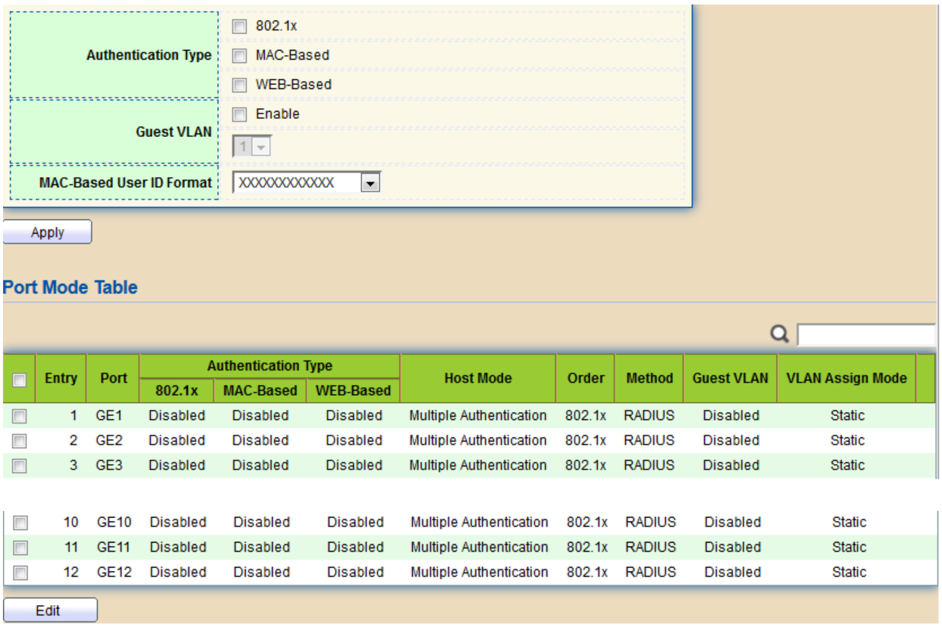
	● Permit: Forward packets that meet the ACE criteria. ● Deny: Drop packets that meet the ACE criteria.
Port	Select ports which will be matched.
IP Version	Select the type of source IP address. · ● All: All IP addresses can access. · ● IPv4: Specify IPv4 address ca access. · ● IPv6: Specify IPv6 address 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.

4.10.3. Authentication Manager

4.10.3.1. Property

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

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



Authentication Type	□ 802.1x □ MAC-Based □ WEB-Based
Guest VLAN	□ Enable 1
MAC-Based User ID Format	XXXXXXXXXXXX

Apply

Port Mode Table

□	Entry	Port	Authentication Type			Host Mode	Order	Method	Guest VLAN	VLAN Assign Mode
			802.1x	MAC-Based	WEB-Based					
□	1	GE1	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
□	2	GE2	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
□	3	GE3	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
□	10	GE10	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
□	11	GE11	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
□	12	GE12	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static

Edit

Figure 98 - Security > Authentication Manager > Property

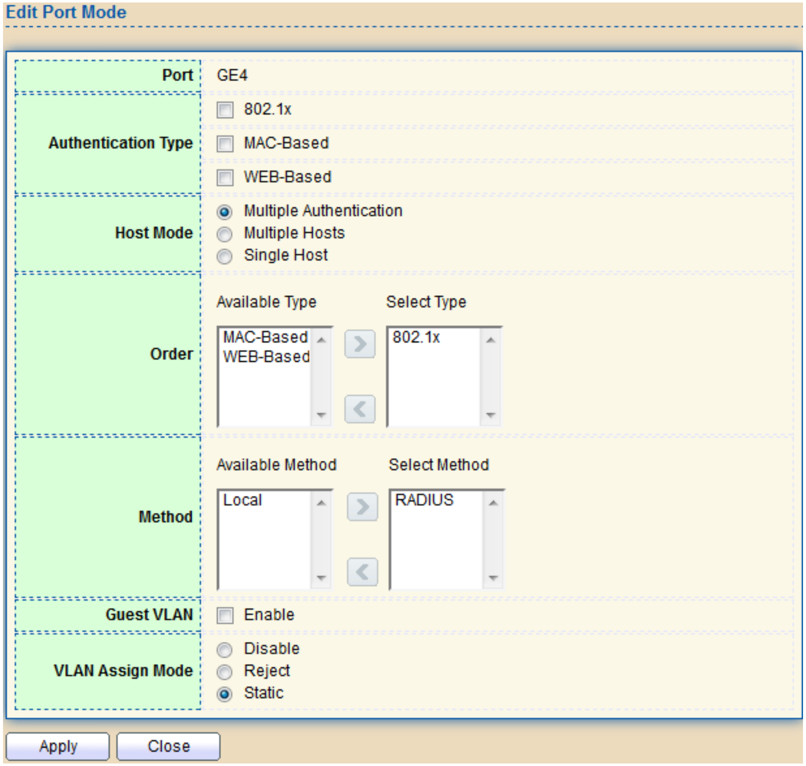
Item	Description
Authentication Type	Set checkbox to enable/disable following authentication types • 802.1x: Use IEEE 802.1x to do authentication • MAC-Based: Use MAC address to do authentication • WEB-Based: Prompt authentication web page for user to do authentication
Guest VLAN	Set checkbox to enable/disable 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 • Xxxxxxxxxxxx • 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
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.



Edit Port Mode

Port	GE4
Authentication Type	□ 802.1x □ MAC-Based □ WEB-Based
Host Mode	● Multiple Authentication ○ Multiple Hosts ○ Single Host
Order	Available Type: MAC-Based, WEB-Based Select Type: 802.1x
Method	Available Method: Local Select Method: RADIUS
Guest VLAN	□ Enable
VLAN Assign Mode	○ Disable ○ Reject ● Static

Figure 99 - Security > Authentication Manager > Property > Edit Port Mode

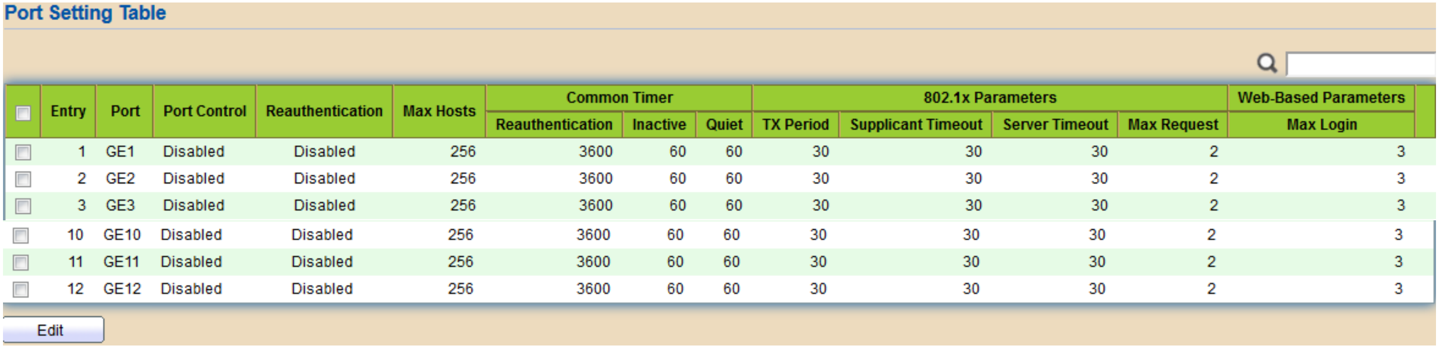
Item	**Descriptio n**
Port	Selected port list.
Authentication Type	Set checkbox to enable/disable authentication types.
Host Mode	Select authenticating host mode • Multiple Authentication: In this mode, every client need to pass authenticate procedure individually. • Multiple Hosts: In this mode, only 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.

4.10.3.2. 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.**



Port Setting Table

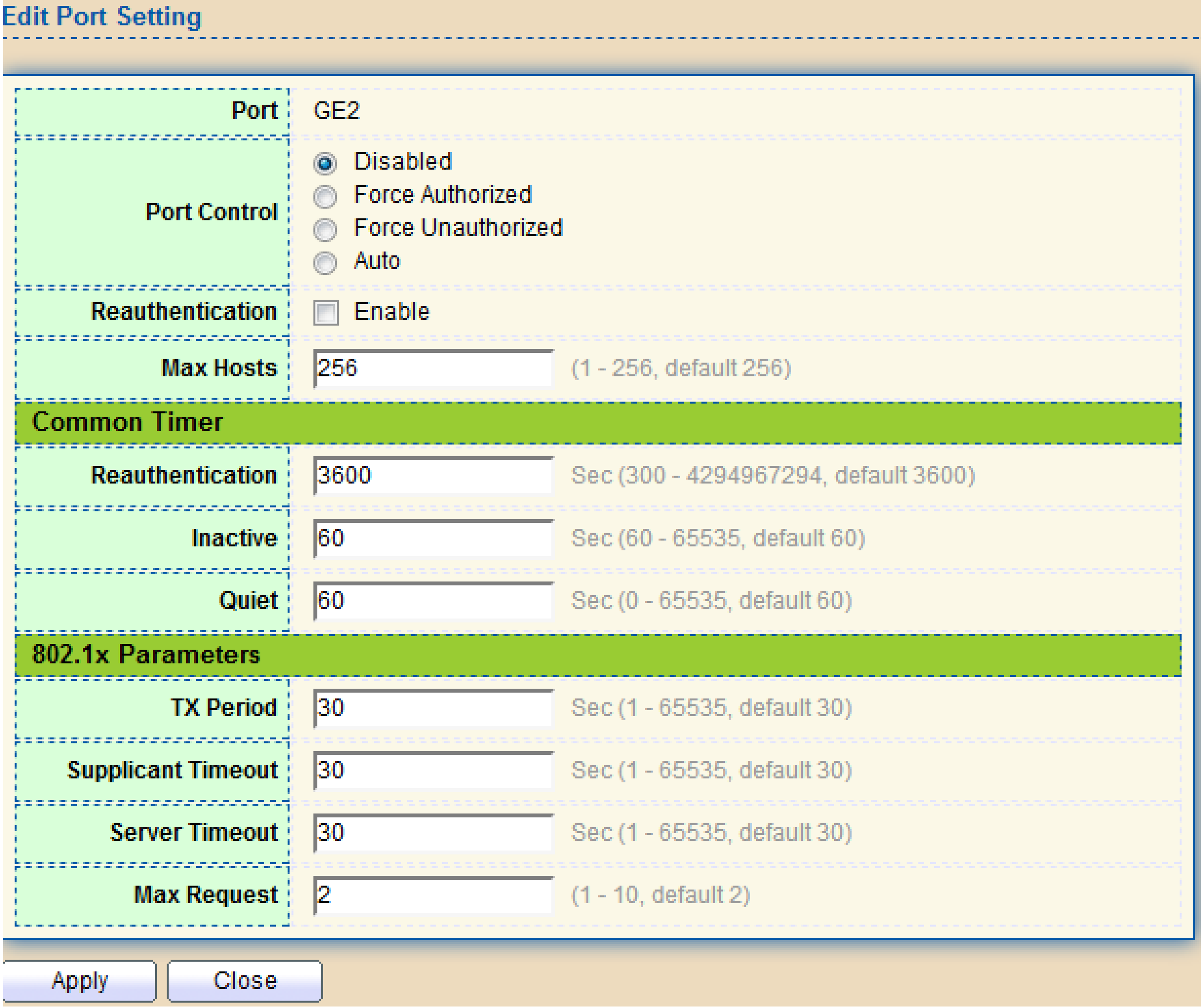
□	Entry	Port	Port Control	Reauthentication	Max Hosts	Common Timer			802.1x Parameters				Web-Based Parameters
						Reauthentication	Inactive	Quiet	TX Period	Supplicant Timeout	Server Timeout	Max Request	Max Login
□	1	GE1	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
□	2	GE2	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
□	3	GE3	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
□	10	GE10	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
□	11	GE11	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
□	12	GE12	Disabled	Disabled	256	3600	60	60	30	30	30	2	3

Figure 100 - 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	Reauthenticate 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.



Edit Port Setting

Port	GE2	
Port Control	● Disabled ○ Force Authorized ○ Force Unauthorized ○ Auto	
Reauthentication	□ Enable	
Max Hosts	256	(1 - 256, default 256)
Common Timer		
Reauthentication	3600	Sec (300 - 4294967294, default 3600)
Inactive	60	Sec (60 - 65535, default 60)
Quiet	60	Sec (0 - 65535, default 60)
802.1x Parameters		
TX Period	30	Sec (1 - 65535, default 30)
Supplicant Timeout	30	Sec (1 - 65535, default 30)
Server Timeout	30	Sec (1 - 65535, default 30)
Max Request	2	(1 - 10, default 2)

Figure 101 - 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

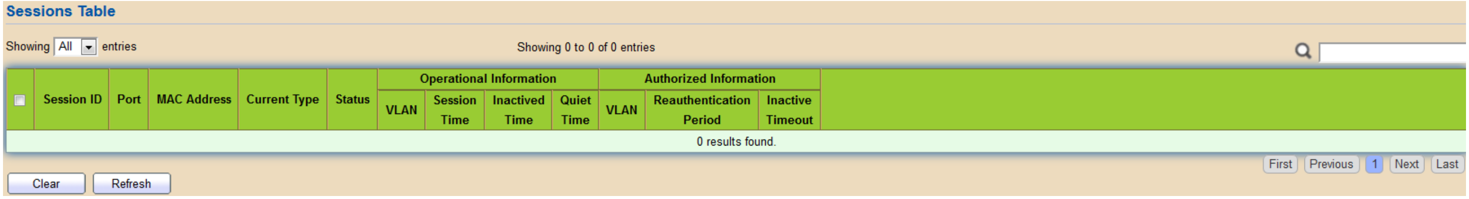
	network accessibility.
Reauthentication	Set checkbox to enable/disable reuauthentication.
Max Hosts	In Multiple Authentication mode, total host number cannot not exceed max hosts number.
Common Timer	
Reauthentication	After re-authenticate period, host will return to initial state and need to pass authentication 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.

4.10.3.3. 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**



Sessions Table

Showing All entries

Showing 0 to 0 of 0 entries

☐	Session ID	Port	MAC Address	Current Type	Status	Operational Information				Authorized Information		
						VLAN	Session Time	Inactived Time	Quiet Time	VLAN	Reauthentication Period	Inactive Timeout
0 results found.												

Figure 102 - 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)

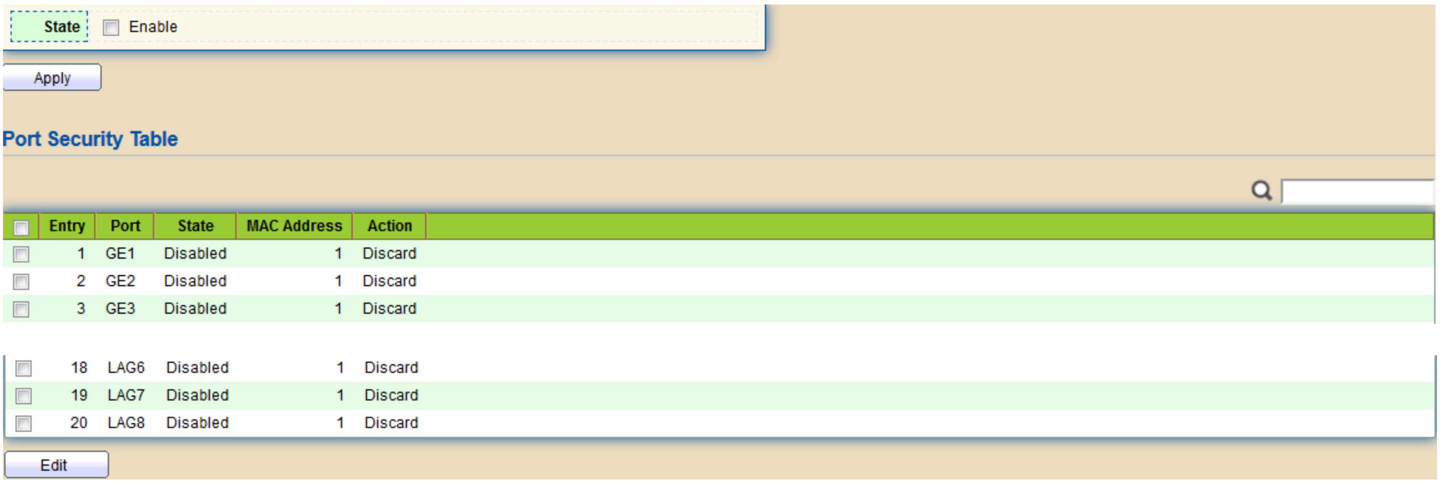
	- Disable: This session is ready to be deleted - Running: Authentication process is running - Authorized: Authentication is passed and getting network accessibility. - Unauthorized: Authentication is not passed and not getting network accessibility. - Locked: Host is locked and do not allow to do
	- 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	Shows inactive timeout given from authorized procedure.

Timeouts)	

4.10.4. 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**



State □ Enable

Port Security Table

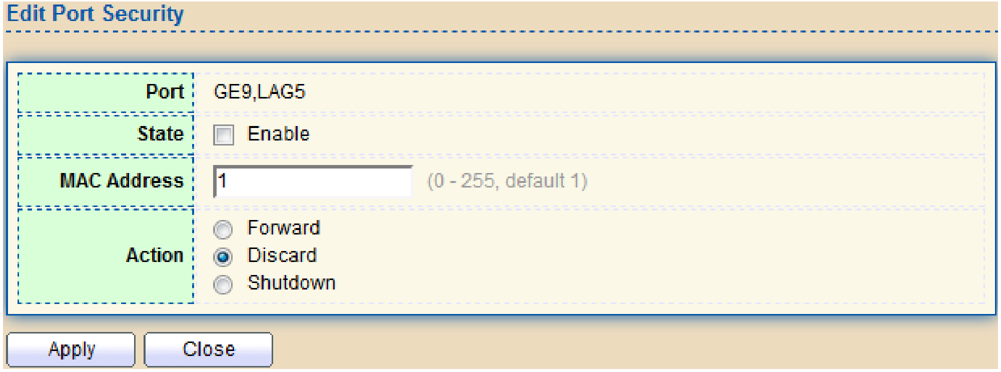
□	Entry	Port	State	MAC Address	Action
□	1	GE1	Disabled	1	Discard
□	2	GE2	Disabled	1	Discard
□	3	GE3	Disabled	1	Discard
□	18	LAG6	Disabled	1	Discard
□	19	LAG7	Disabled	1	Discard
□	20	LAG8	Disabled	1	Discard

Figure 103 - 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.



Edit Port Security

Port	GE9,LAG5
State	□ Enable
MAC Address	1 (0 - 255, default 1)
Action	○ Forward ● Discard ○ Shutdown

Figure 104 - Security > Port Security > Edit Port Security

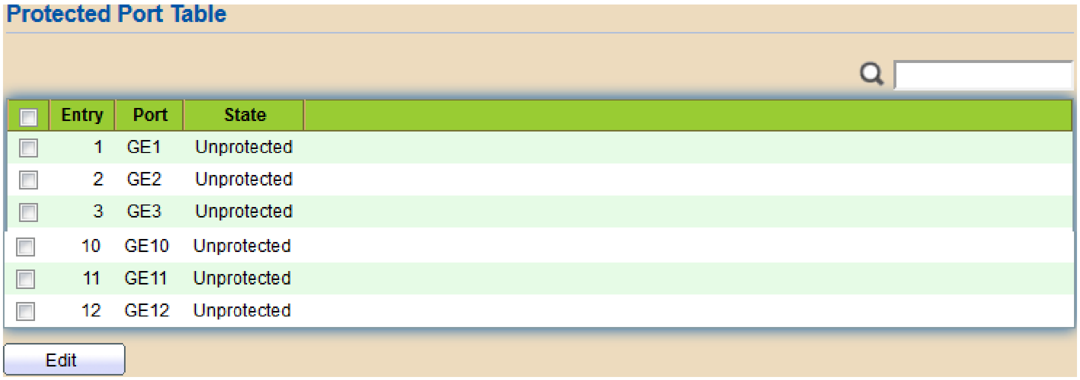
Item	Description
Port	Select one or multiple ports to configure.
State	Select the status of port security • Disable: Disable port security function. • Enable: Enable port security function.
MAC Address	Specify the number of how many mac addresses can be learned.

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.

4.10.5. Protected Port

This page allow user to configure protected port setting to prevent the selected ports from communication with each other. Protected port is only allowed to communicate with unprotected port. In other words, protected port is not allowed to communicate with another protected port.

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



Protected Port Table

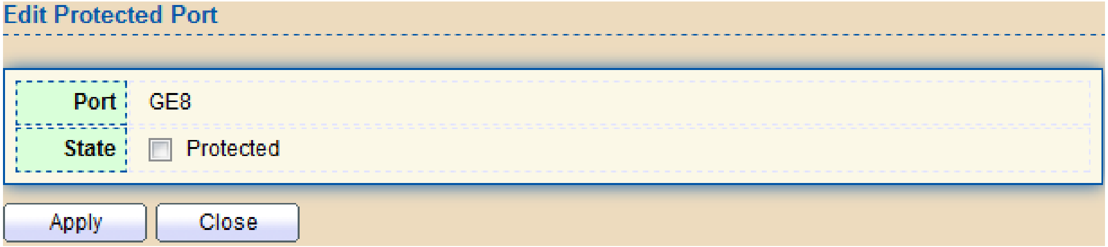
□	Entry	Port	State
□	1	GE1	Unprotected
□	2	GE2	Unprotected
□	3	GE3	Unprotected
□	10	GE10	Unprotected
□	11	GE11	Unprotected
□	12	GE12	Unprotected

Figure 105 - Security > Protected Port

Item	**Description**
Port	Port Name.
State	Port protected admin state.

	· Protected: Port is protected. · Unprotected: Port is unprotected

Click "Edit" button to view Edit Protected Port menu.



Edit Protected Port

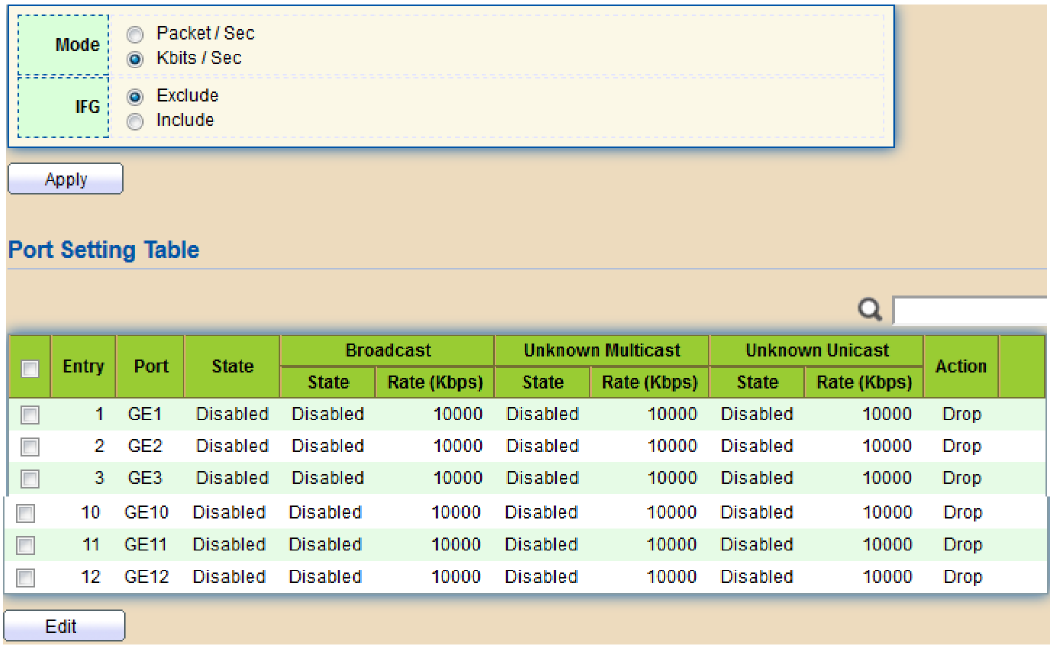
Port	GE8
State	□ Protected

Figure 106 - Security > Protected Port > Edit Protected Port

Item	Description
Port	Selected port list.
State	Port protected admin state. • Protected: Enable protecting function. • Unprotected: Disable protecting function.

4.10.6. Storm Control

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



Mode: ○ Packet / Sec ● Kbits / Sec

IFG: ● Exclude ○ Include

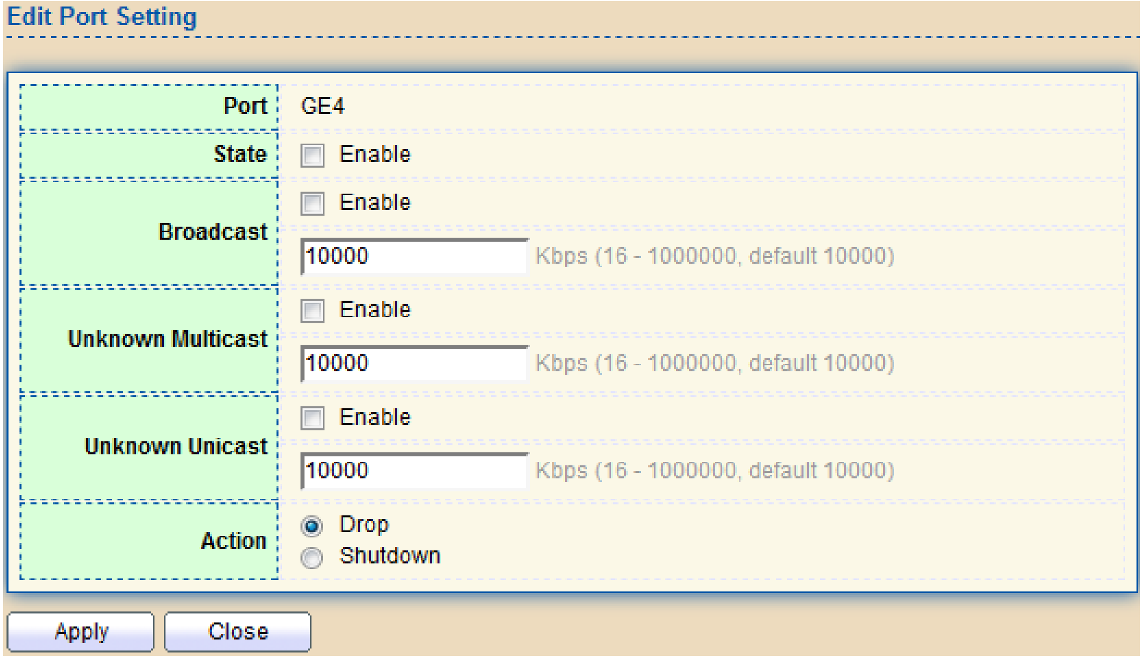
Port Setting Table

□	Entry	Port	State	Broadcast		Unknown Multicast		Unknown Unicast		Action
				State	Rate (Kbps)	State	Rate (Kbps)	State	Rate (Kbps)	
□	1	GE1	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
□	2	GE2	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
□	3	GE3	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
□	10	GE10	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
□	11	GE11	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
□	12	GE12	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop

Figure 107 - 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.



Edit Port Setting

Port	GE4
State	□ Enable
Broadcast	□ Enable 10000 Kbps (16 - 1000000, default 10000)
Unknown Multicast	□ Enable 10000 Kbps (16 - 1000000, default 10000)
Unknown Unicast	□ Enable 10000 Kbps (16 - 1000000, default 10000)
Action	● Drop ○ Shutdown

Figure 108 - 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.

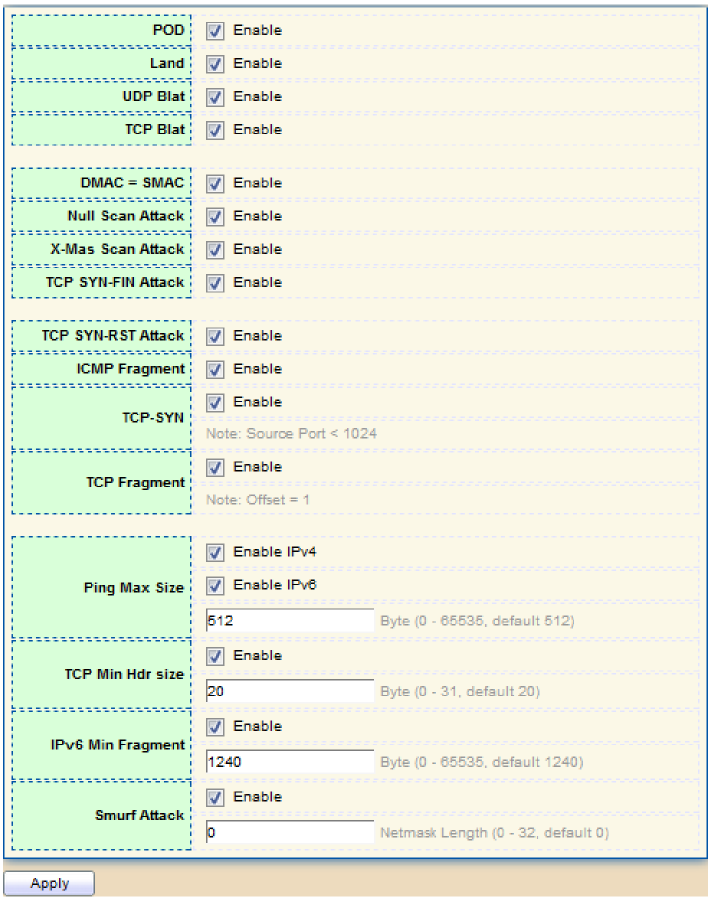
4.10.7. DoS

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.

4.10.7.1. Property

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



POD	☑ Enable
Land	☑ Enable
UDP Blat	☑ Enable
TCP Blat	☑ Enable
DMAC = SMAC	☑ Enable
Null Scan Attack	☑ Enable
X-Mas Scan Attack	☑ Enable
TCP SYN-FIN Attack	☑ Enable
TCP SYN-RST Attack	☑ Enable
ICMP Fragment	☑ Enable
TCP-SYN	☑ Enable Note: Source Port < 1024
TCP Fragment	☑ Enable Note: Offset = 1
Ping Max Size	☑ Enable IPv4 ☑ Enable IPv6 512 Byte (0 - 65535, default 512)
TCP Min Hdr size	☑ Enable 20 Byte (0 - 31, default 20)
IPv6 Min Fragment	☑ Enable 1240 Byte (0 - 65535, default 1240)
Smurf Attack	☑ Enable 0 Netmask Length (0 - 32, default 0)

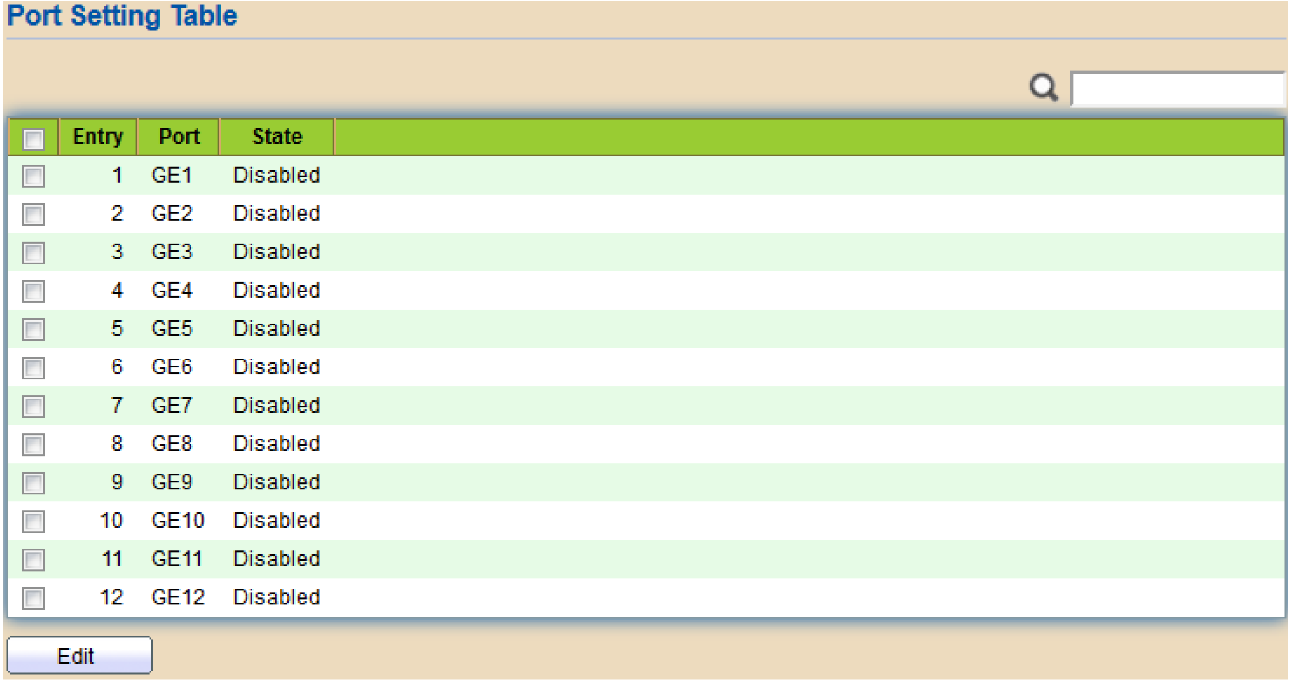
Figure 109 - Security > DoS > Property

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 Flagment	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 Flagment	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.

4.10.7.2. Port Setting

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



Port Setting Table

□	Entry	Port	State
□	1	GE1	Disabled
□	2	GE2	Disabled
□	3	GE3	Disabled
□	4	GE4	Disabled
□	5	GE5	Disabled
□	6	GE6	Disabled
□	7	GE7	Disabled
□	8	GE8	Disabled
□	9	GE9	Disabled
□	10	GE10	Disabled
□	11	GE11	Disabled
□	12	GE12	Disabled

Figure 110 - Security > DoS > Port Setting

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

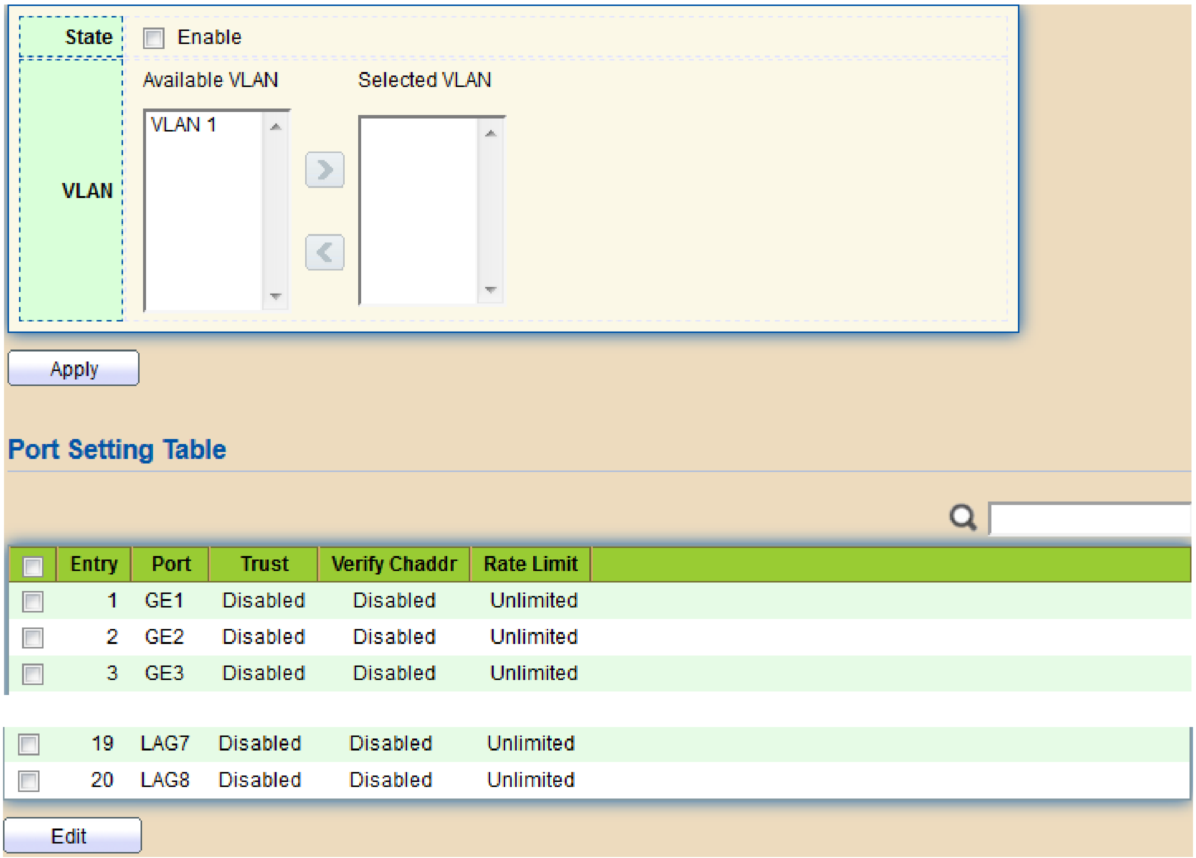
4.10.8. DHCP Snooping

Use the DHCP Snooping pages to configure settings of DHCP Snooping

4.10.8.1. Property

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

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



State: ☐ Enable

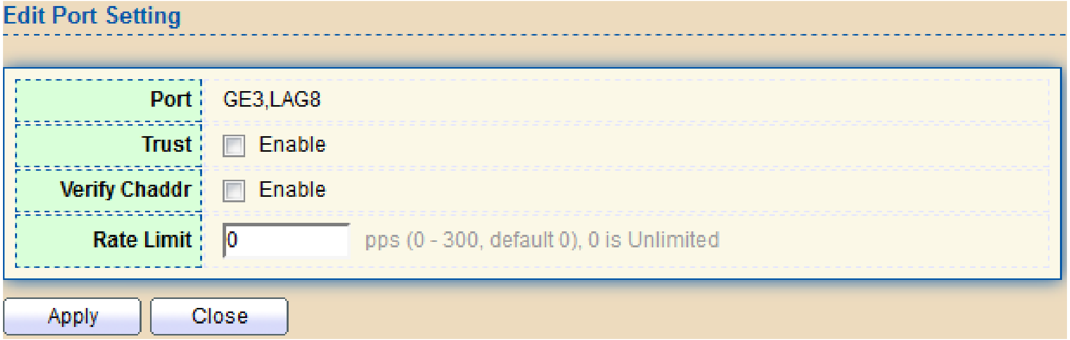
VLAN: Available VLAN: VLAN 1 | Selected VLAN:

☐	Entry	Port	Trust	Verify Chaddr	Rate Limit
☐	1	GE1	Disabled	Disabled	Unlimited
☐	2	GE2	Disabled	Disabled	Unlimited
☐	3	GE3	Disabled	Disabled	Unlimited
☐	19	LAG7	Disabled	Disabled	Unlimited
☐	20	LAG8	Disabled	Disabled	Unlimited

Figure 111 - 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.



Edit Port Setting

Port	GE3,LAG8
Trust	□ Enable
Verify Chaddr	□ Enable
Rate Limit	0 pps (0 - 300, default 0), 0 is Unlimited

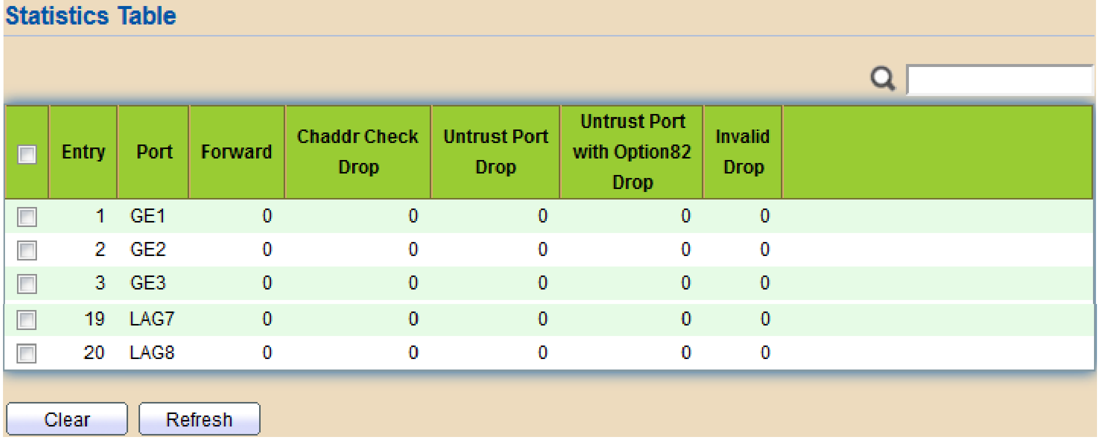
Figure 112 - Security > DHCP Snooping > Property > Edit Port Setting

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.

4.10.8.2. 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** .



Statistics Table

□	Entry	Port	Forward	Chaddr Check Drop	Untrust Port Drop	Untrust Port with Option82 Drop	Invalid Drop
□	1	GE1	0	0	0	0	0
□	2	GE2	0	0	0	0	0
□	3	GE3	0	0	0	0	0
□	19	LAG7	0	0	0	0	0
□	20	LAG8	0	0	0	0	0

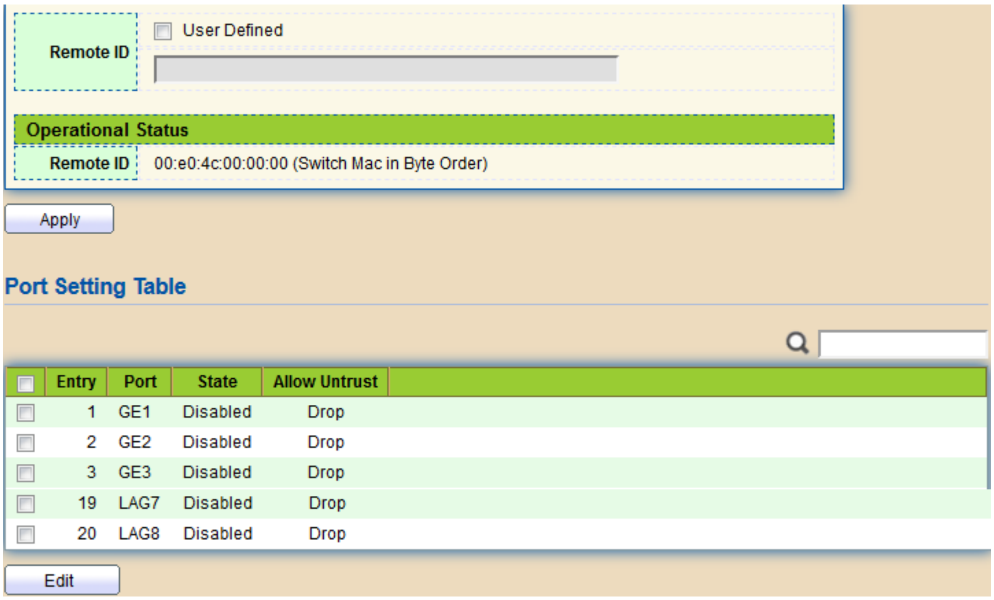
Figure 113 - Security > DHCP Snooping > Statistics

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.

4.10.8.3. 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**



Remote ID ☐ User Defined

Operational Status

Remote ID 00:e0:4c:00:00:00 (Switch Mac in Byte Order)

Apply

Port Setting Table

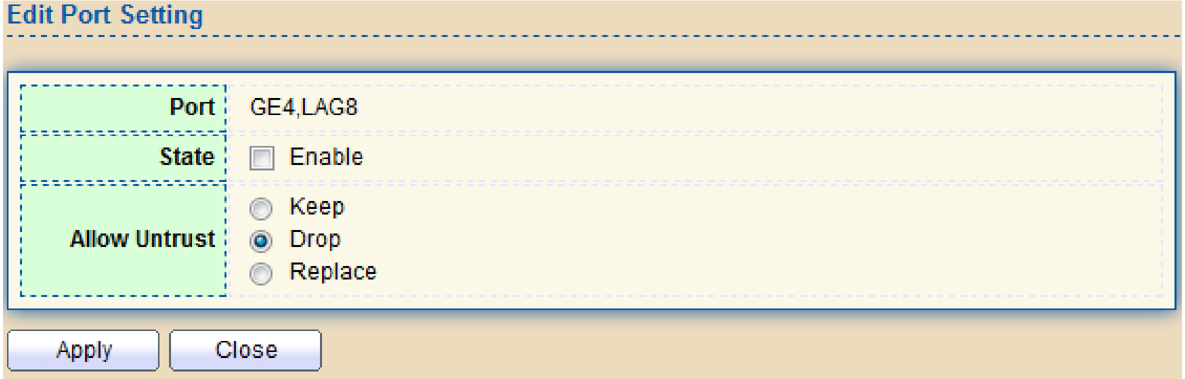
☐	Entry	Port	State	Allow Untrust
☐	1	GE1	Disabled	Drop
☐	2	GE2	Disabled	Drop
☐	3	GE3	Disabled	Drop
☐	19	LAG7	Disabled	Drop
☐	20	LAG8	Disabled	Drop

Edit

Figure 114- 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.



Edit Port Setting

Port	GE4,LAG8
State	□ Enable
Allow Untrust	○ Keep ● Drop ○ Replace

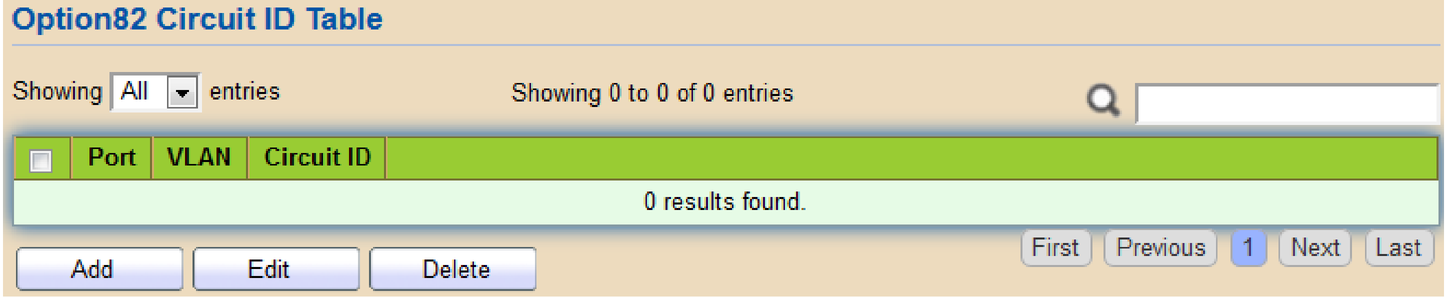
Figure 115 - Security > DHCP Snooping > Option82 Property > Edit Port Setting

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

4.10.8.4. 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**



Option82 Circuit ID Table

Showing All entries Showing 0 to 0 of 0 entries

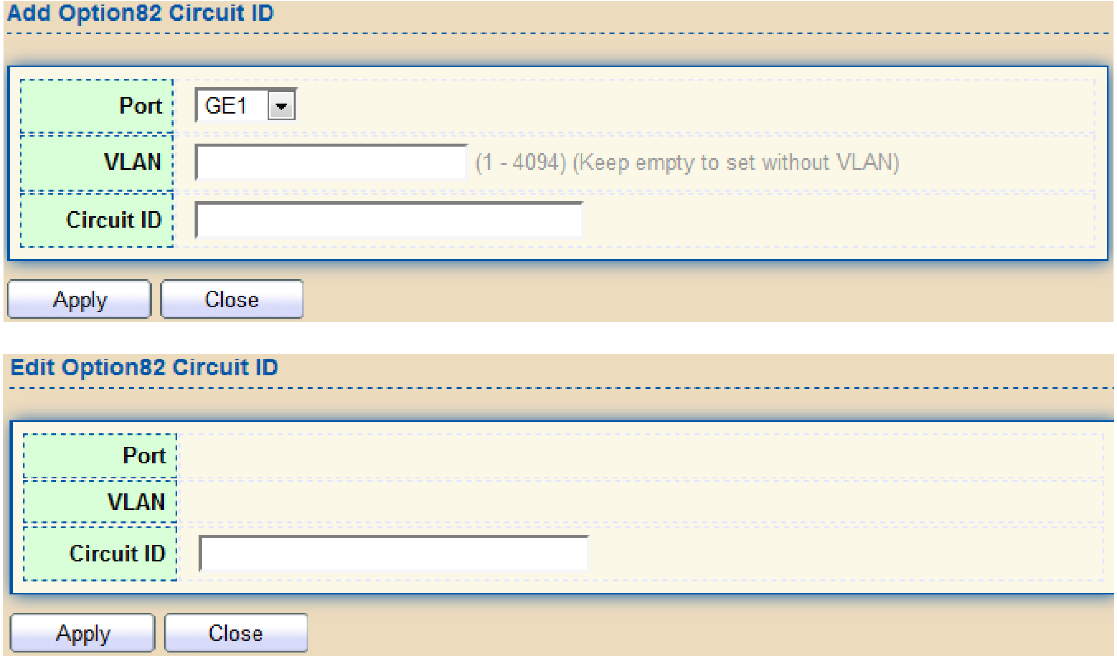
□	Port	VLAN	Circuit ID

0 results found.

Figure 116 - 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.



Add Option82 Circuit ID

Port	GE1
VLAN	(1 - 4094) (Keep empty to set without VLAN)
Circuit ID	

Edit Option82 Circuit ID

Port	
VLAN	
Circuit ID	

Figure 117 - 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.

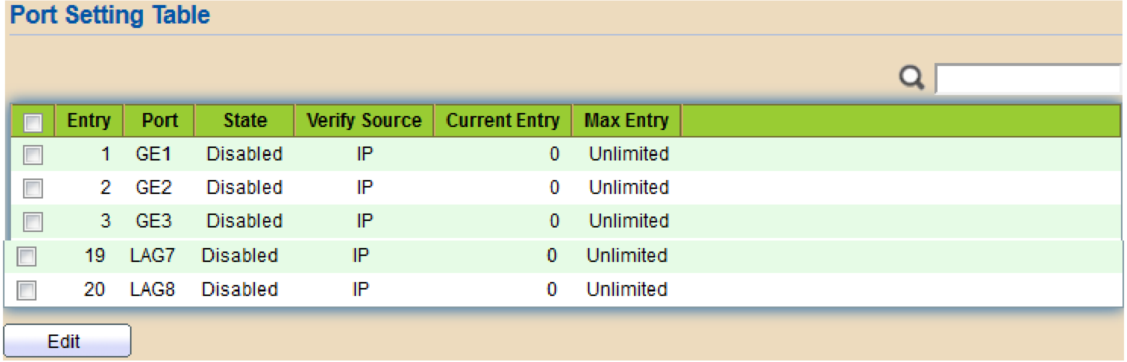
4.10.9. IP Source Guard

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

4.10.9.1. 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**



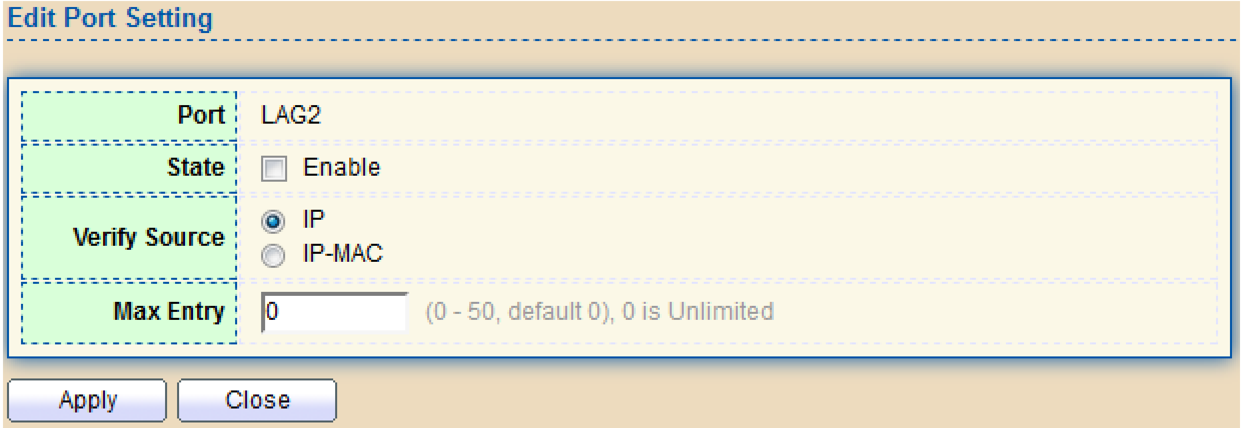
Port Setting Table

□	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
□	19	LAG7	Disabled	IP	0	Unlimited
□	20	LAG8	Disabled	IP	0	Unlimited

Figure 118 - 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.



Edit Port Setting

Port	LAG2
State	□ Enable
Verify Source	● IP ○ IP-MAC
Max Entry	0 (0 - 50, default 0), 0 is Unlimited

Figure 119 - Security > IP Source Guard > Port Setting > Edit Port Setting

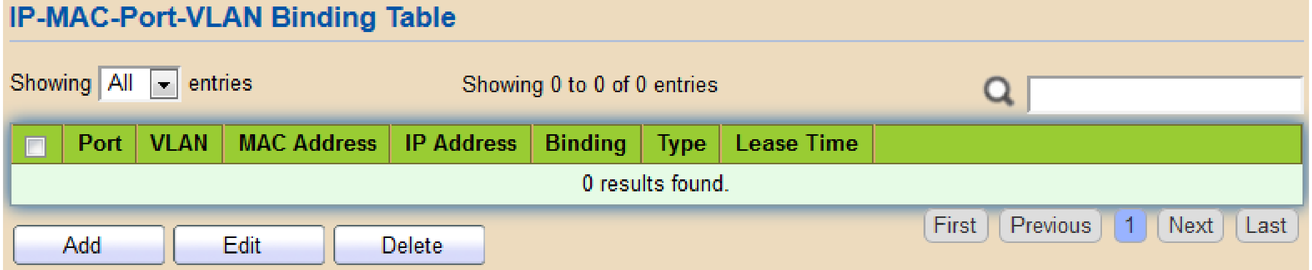
Item	Description
Port	Display selected port to be edited.
Status	Set checkbox to enable or disable IP Source Guard function. Default is disabled.

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.

4.10.9.2. 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**



IP-MAC-Port-VLAN Binding Table

Showing All entries   Showing 0 to 0 of 0 entries

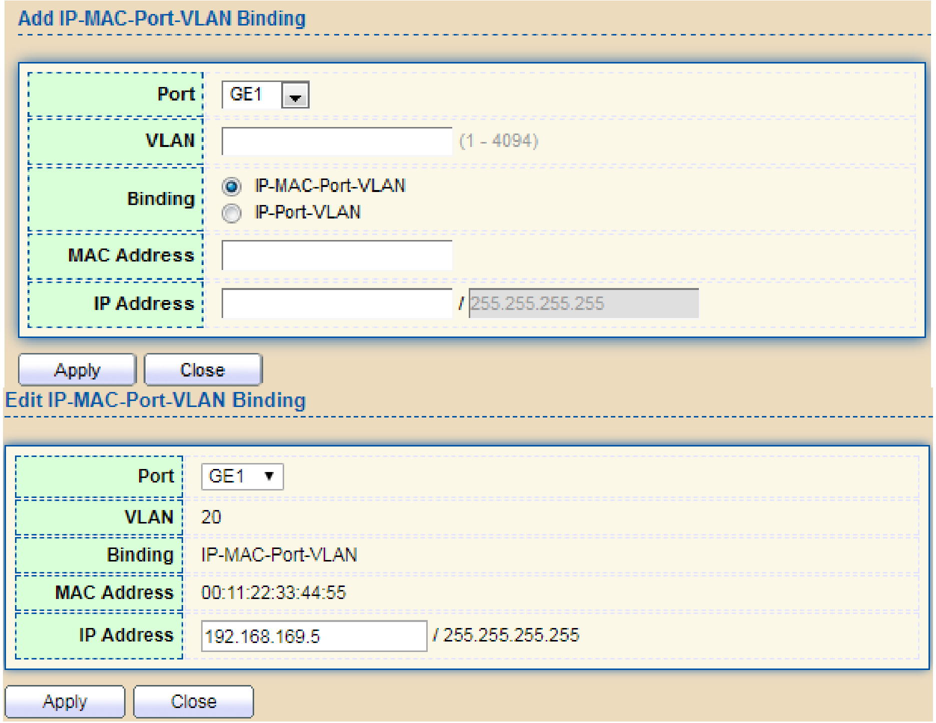
□	Port	VLAN	MAC Address	IP Address	Binding	Type	Lease Time
0 results found.							

Figure 120 - 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.



Add IP-MAC-Port-VLAN Binding

Port	GE1
VLAN	(1 - 4094)
Binding	● IP-MAC-Port-VLAN ○ IP-Port-VLAN
MAC Address	
IP Address	/ 255.255.255.255

Edit IP-MAC-Port-VLAN Binding

Port	GE1
VLAN	20
Binding	IP-MAC-Port-VLAN
MAC Address	00:11:22:33:44:55
IP Address	192.168.169.5 / 255.255.255.255

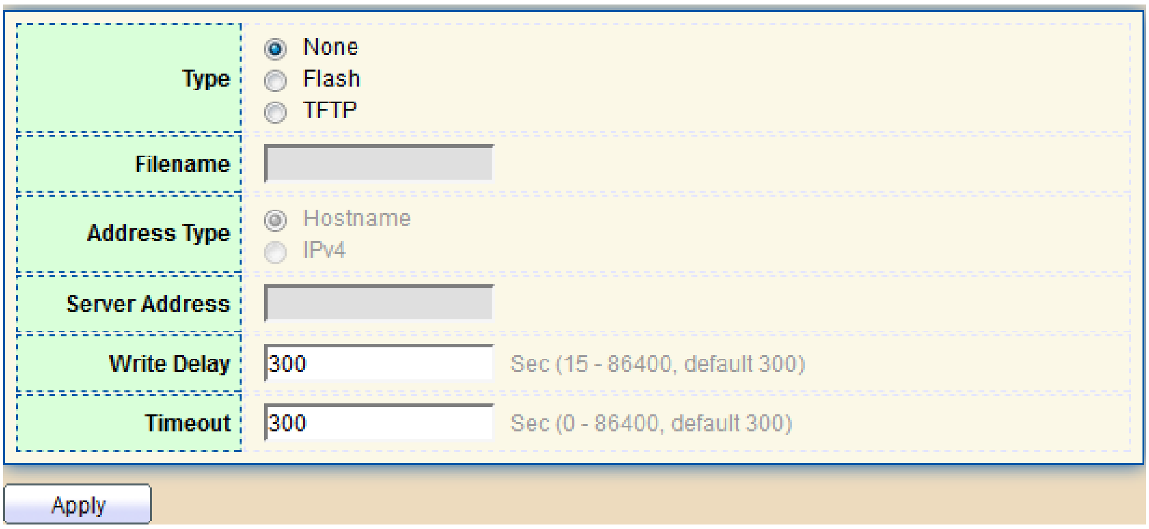
Figure 121 - Security > IP Source Guard > Add/Edit IP-MAC-Port-VLAN Binding

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.

4.10.9.3. 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**.



Type	● None ○ Flash ○ TFTP
Filename	
Address Type	● Hostname ○ IPv4
Server Address	
Write Delay	300 Sec (15 - 86400, default 300)
Timeout	300 Sec (0 - 86400, default 300)

Figure 122 - 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.

4.11. ACL

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

4.11.1. 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**

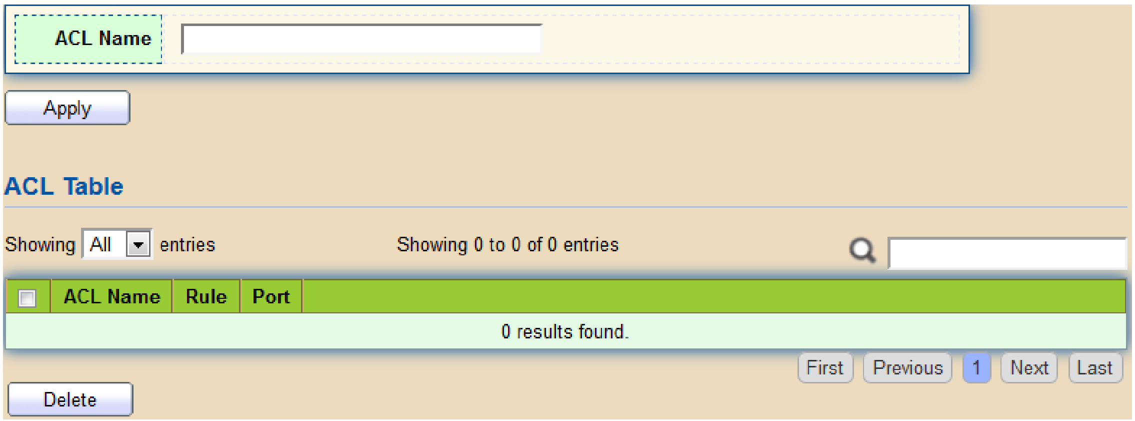


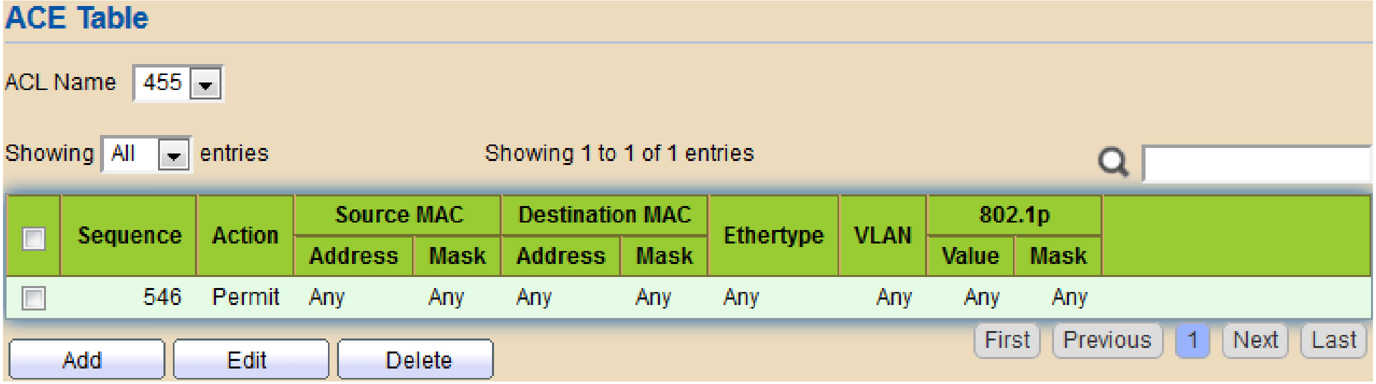
Figure 123 - ACL > MAC ACL

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.

4.11.2. 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**



ACE Table

ACL Name 455

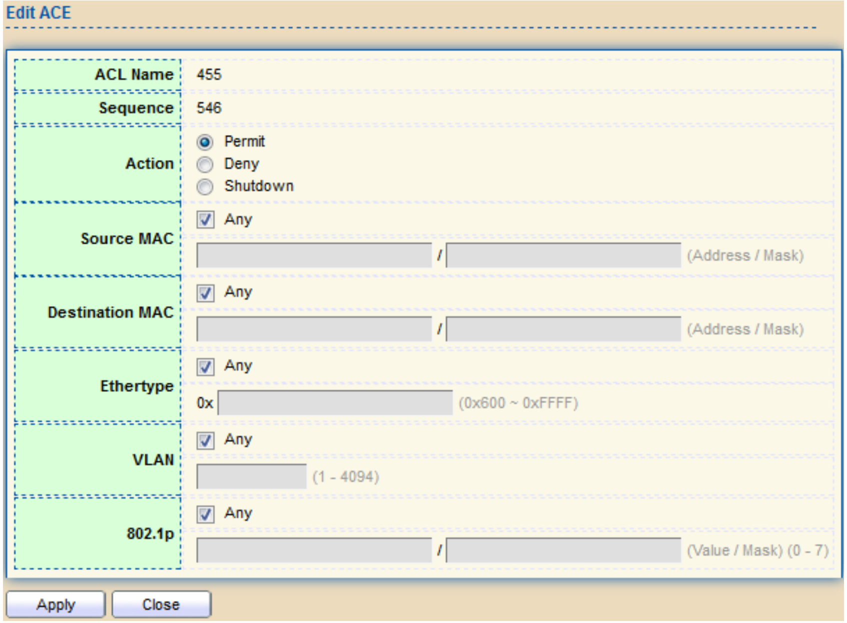
Showing All entries   Showing 1 to 1 of 1 entries

□	Sequence	Action	Source MAC		Destination MAC		Ethertype	VLAN	802.1p	
			Address	Mask	Address	Mask			Value	Mask
□	546	Permit	Any	Any	Any	Any	Any	Any	Any	Any

Figure 124 - 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.



Edit ACE

ACL Name	455
Sequence	546
Action	● Permit ○ Deny ○ Shutdown
Source MAC	☑ Any / (Address / Mask)
Destination MAC	☑ Any / (Address / Mask)
Ethertype	☑ Any 0x (0x600 ~ 0xFFFF)
VLAN	☑ Any (1 - 4094)
802.1p	☑ Any / (Value / Mask) (0 - 7)

Figure 125 - 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.
	Select the type for source MAC address. ·

Source MAC	● 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.

4.11.3. 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**

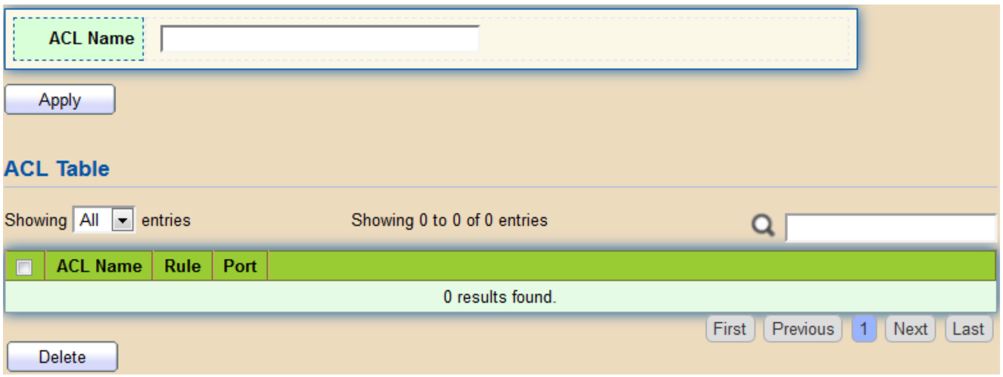


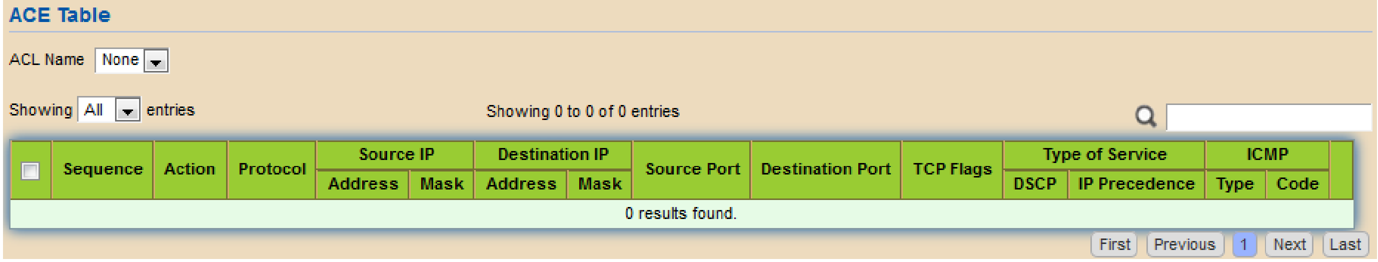
Figure 126 - ACL > IPv4 ACL

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.

4.11.4. 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**



ACE Table

ACL Name None

Showing All entries

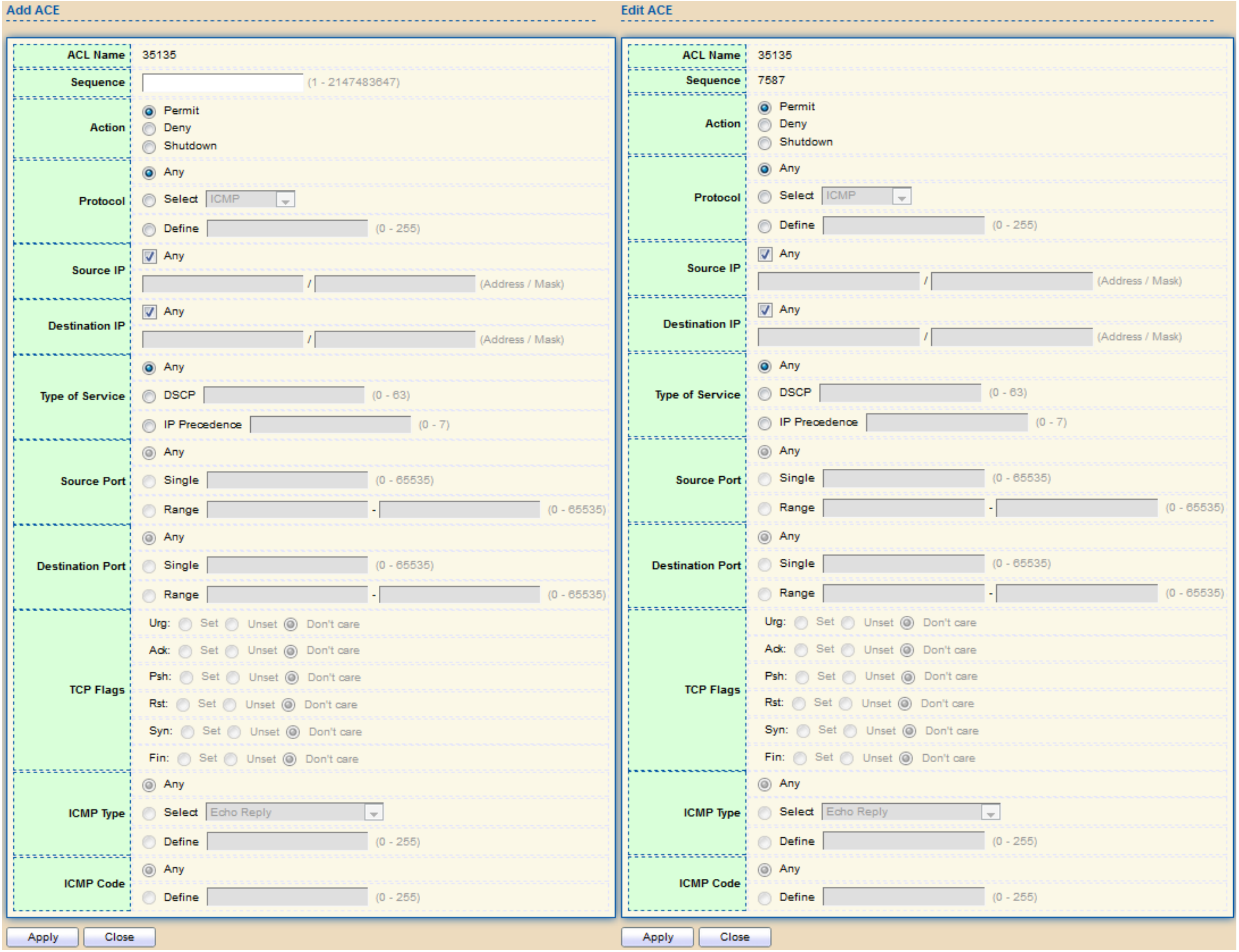
Showing 0 to 0 of 0 entries

□	Sequence	Action	Protocol	Source IP		Destination IP		Source Port	Destination Port	TCP Flags	Type of Service		ICMP	
				Address	Mask	Address	Mask				DSCP	IP Precedence	Type	Code
0 results found.														

Figure 127 - 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.



Add ACE

ACL Name	35135
Sequence	(1 - 2147483647)
Action	● Permit ○ Deny ○ Shutdown
Protocol	● Any ○ Select ICMP ○ Define (0 - 255)
Source IP	☑ Any / (Address / Mask)
Destination IP	☑ Any / (Address / Mask)
Type of Service	● Any ○ DSCP (0 - 63) ○ IP Precedence (0 - 7)
Source Port	● Any ○ Single (0 - 65535) ○ Range - (0 - 65535)
Destination Port	● Any ○ Single (0 - 65535) ○ Range - (0 - 65535)
TCP Flags	Urg: ○ Set ○ Unset ● Don't care Ack: ○ Set ○ Unset ● Don't care Psh: ○ Set ○ Unset ● Don't care Rst: ○ Set ○ Unset ● Don't care Syn: ○ Set ○ Unset ● Don't care Fin: ○ Set ○ Unset ● Don't care
ICMP Type	● Any ○ Select Echo Reply ○ Define (0 - 255)
ICMP Code	● Any ○ Define (0 - 255)

Apply Close

Edit ACE

ACL Name	35135
Sequence	7587
Action	● Permit ○ Deny ○ Shutdown
Protocol	● Any ○ Select ICMP ○ Define (0 - 255)
Source IP	☑ Any / (Address / Mask)
Destination IP	☑ Any / (Address / Mask)
Type of Service	● Any ○ DSCP (0 - 63) ○ IP Precedence (0 - 7)
Source Port	● Any ○ Single (0 - 65535) ○ Range - (0 - 65535)
Destination Port	● Any ○ Single (0 - 65535) ○ Range - (0 - 65535)
TCP Flags	Urg: ○ Set ○ Unset ● Don't care Ack: ○ Set ○ Unset ● Don't care Psh: ○ Set ○ Unset ● Don't care Rst: ○ Set ○ Unset ● Don't care Syn: ○ Set ○ Unset ● Don't care Fin: ○ Set ○ Unset ● Don't care
ICMP Type	● Any ○ Select Echo Reply ○ Define (0 - 255)
ICMP Code	● Any ○ Define (0 - 255)

Apply Close

Figure 128 - 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.
	Select the action for a match. ·

Action	● 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

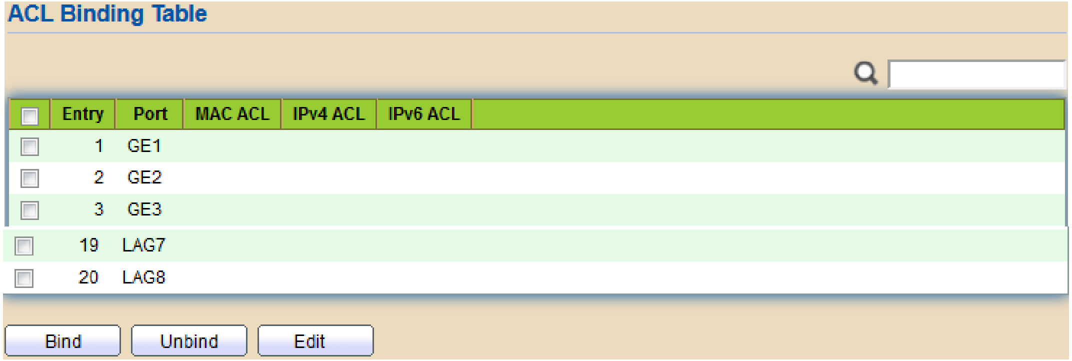
	packets are matched. · ● Range: Select a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
Destination Port	Select the type of protocol 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.
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.

4.11.5. 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**



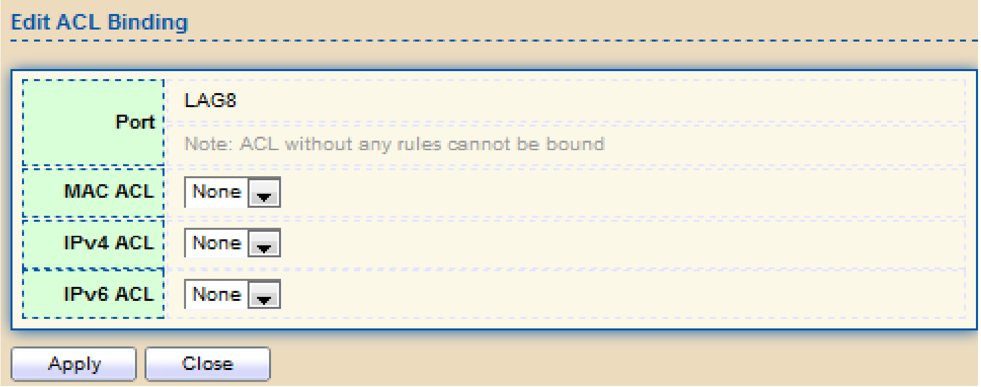
ACL Binding Table

□	Entry	Port	MAC ACL	IPv4 ACL	IPv6 ACL
□	1	GE1			
□	2	GE2			
□	3	GE3			
□	19	LAG7			
□	20	LAG8			

Figure 129 - 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.



Edit ACL Binding

Port	LAG8 Note: ACL without any rules cannot be bound
MAC ACL	None
IPv4 ACL	None
IPv6 ACL	None

Figure 130 - 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.

4.12. QoS

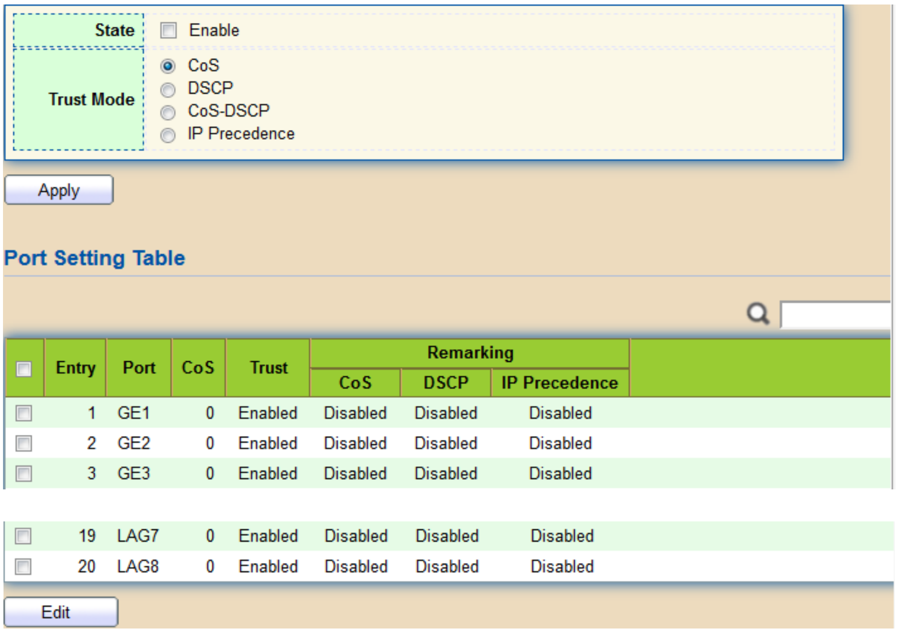
Use the QoS pages to configure settings for the switch QoS interface.

4.12.1. General

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

4.12.1.1. Property

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



State	□ Enable
Trust Mode	● CoS ○ DSCP ○ CoS-DSCP ○ IP Precedence

Port Setting Table

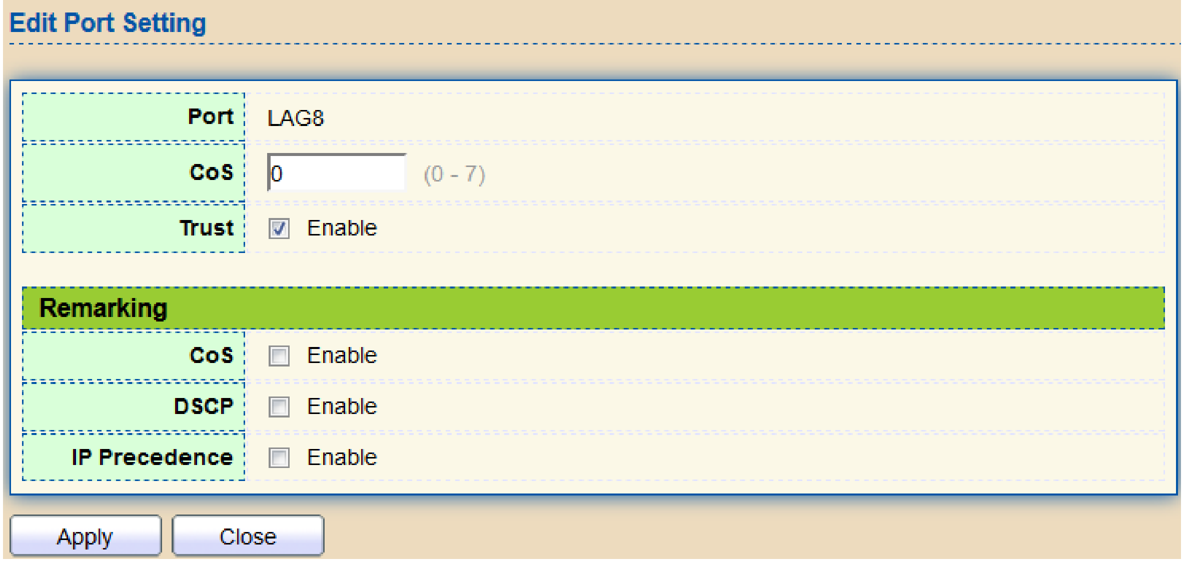
□	Entry	Port	CoS	Trust	Remarking		
					CoS	DSCP	IP Precedence
□	1	GE1	0	Enabled	Disabled	Disabled	Disabled
□	2	GE2	0	Enabled	Disabled	Disabled	Disabled
□	3	GE3	0	Enabled	Disabled	Disabled	Disabled
□	19	LAG7	0	Enabled	Disabled	Disabled	Disabled
□	20	LAG8	0	Enabled	Disabled	Disabled	Disabled

Figure 131 - 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.



Edit Port Setting

Port	LAG8
CoS	0 (0 - 7)
Trust	☑ Enable

Remarking

CoS	□ Enable
DSCP	□ Enable
IP Precedence	□ Enable

Figure 132 - 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.

4.12.1.2. 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).

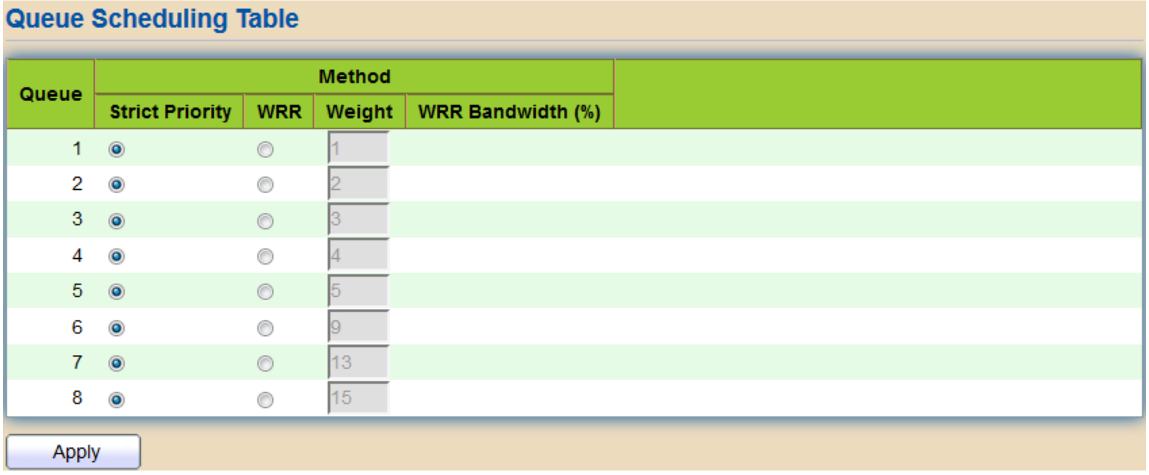
· Strict Priority (SP)–Egress traffic from the highest priority queue is transmitted first. Traffic from the lower queues is processed only after the highest queue has been transmitted, which provide the highest level of priority of traffic to the highest numbered queue.

· 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**



Queue Scheduling Table

Queue	Method			
	Strict Priority	WRR	Weight	WRR Bandwidth (%)
1	●	○	1	
2	●	○	2	
3	●	○	3	
4	●	○	4	
5	●	○	5	
6	●	○	9	
7	●	○	13	
8	●	○	15	

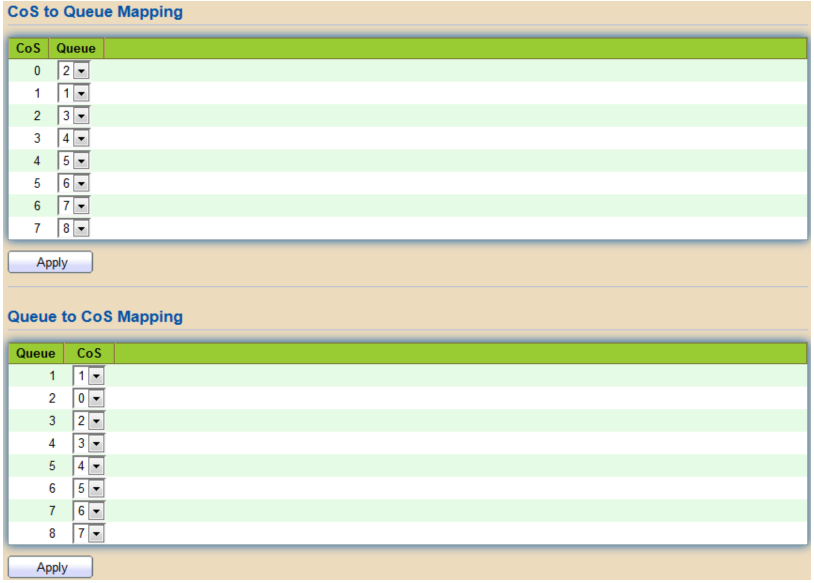
Figure 133 - QoS > General > Queue Scheduling

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.

4.12.1.3. 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**



CoS to Queue Mapping

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

Queue to CoS Mapping

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

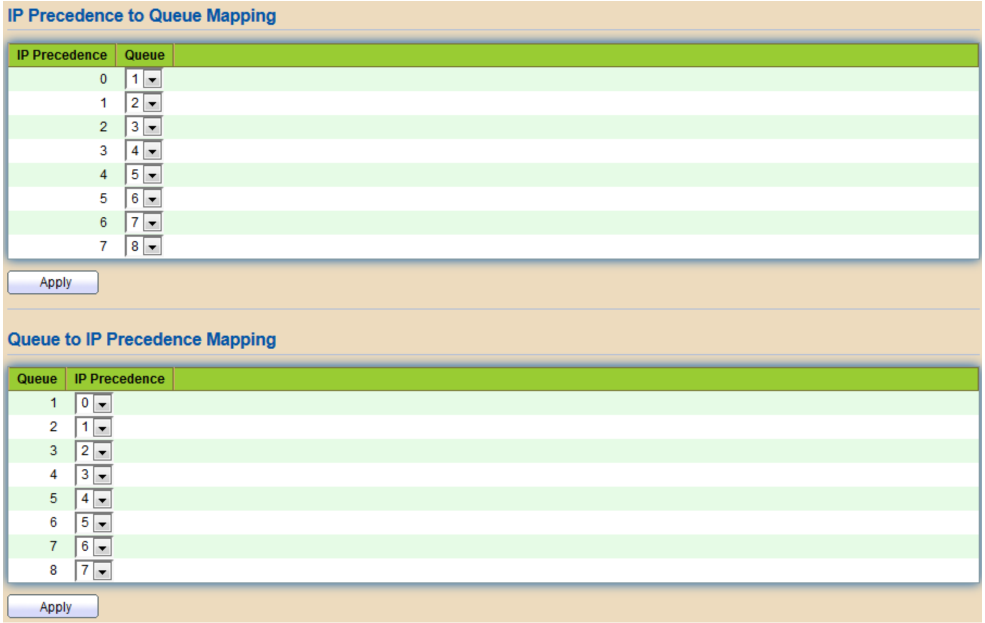
Figure 134 - QoS > General > Cos Mapping

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.

4.12.1.5. 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**



IP Precedence to Queue Mapping

IP Precedence	Queue
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

Queue to IP Precedence Mapping

Queue	IP Precedence
1	0
2	1
3	2
4	3
5	4
6	5
7	6
8	7

Figure 135 - QoS > General > IP Precedence 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.

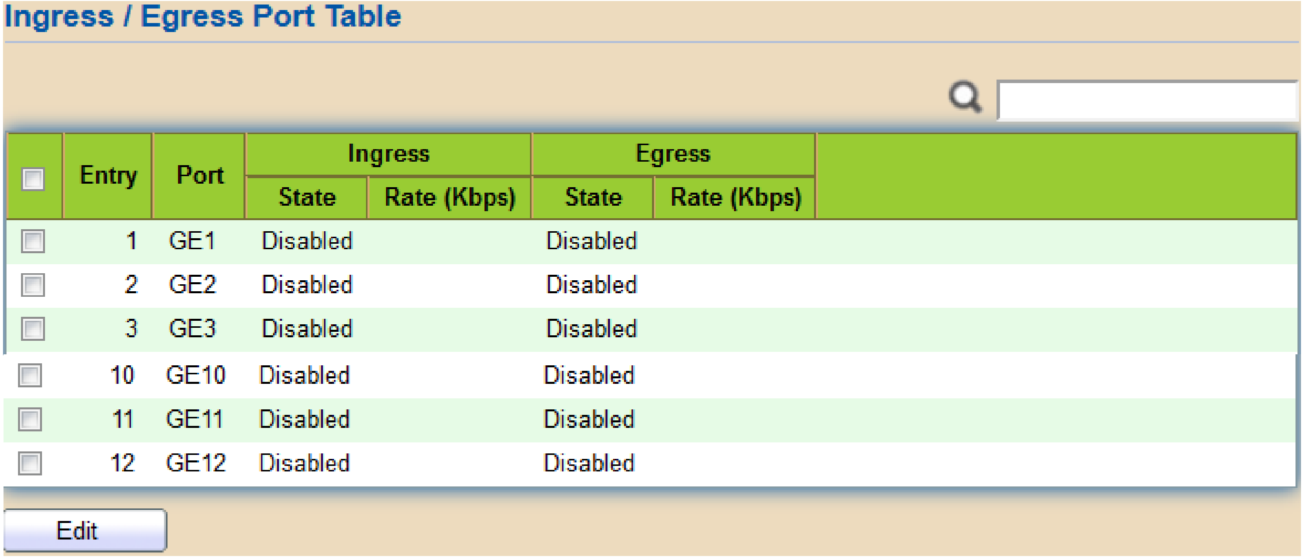
4.12.2. Rate Limit

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

4.12.2.1. 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**



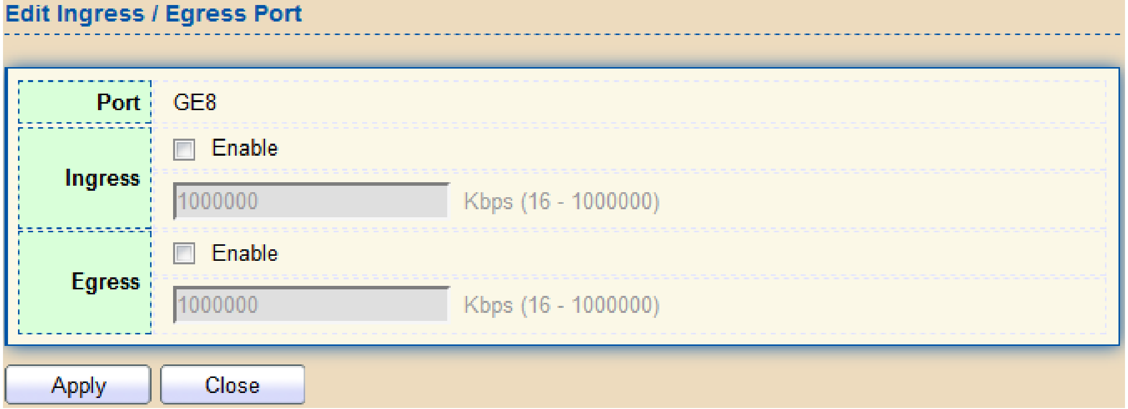
Ingress / Egress Port Table

□	Entry	Port	Ingress		Egress		
			State	Rate (Kbps)	State	Rate (Kbps)	
□	1	GE1	Disabled		Disabled		
□	2	GE2	Disabled		Disabled		
□	3	GE3	Disabled		Disabled		
□	10	GE10	Disabled		Disabled		
□	11	GE11	Disabled		Disabled		
□	12	GE12	Disabled		Disabled		

Figure 136 - 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.



Edit Ingress / Egress Port

Port	GE8
Ingress	□ Enable 1000000 Kbps (16 - 1000000)
Egress	□ Enable 1000000 Kbps (16 - 1000000)

Figure 137 - 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.

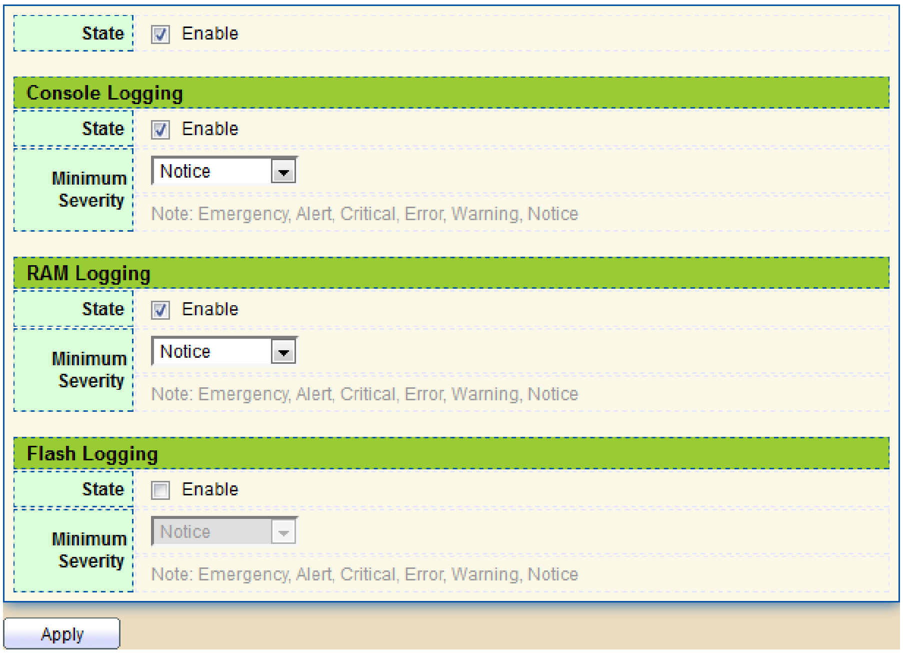
4.13. Diagnostics

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

4.13.1. Logging

4.13.1.1. Property

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



State	☑ Enable

Console Logging

State	☑ Enable
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice

RAM Logging

State	☑ Enable
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice

Flash Logging

State	□ Enable
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice

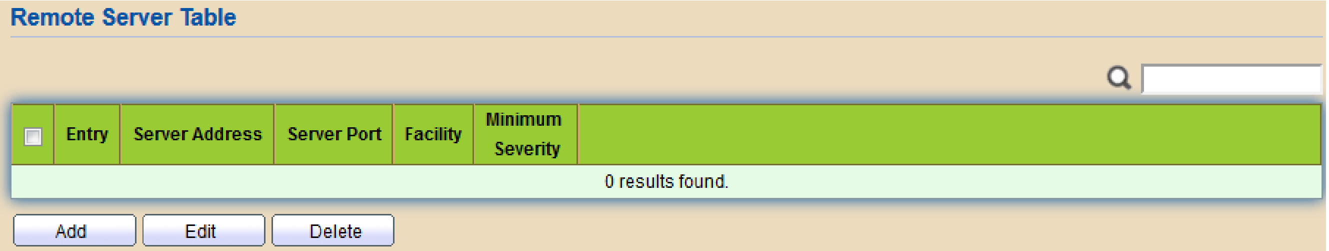
Figure 138 - Diagnostics > Logging > Property

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 login.

4.13.1.2. Remote Server

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



Remote Server Table

☐	Entry	Server Address	Server Port	Facility	Minimum Severity
0 results found.					

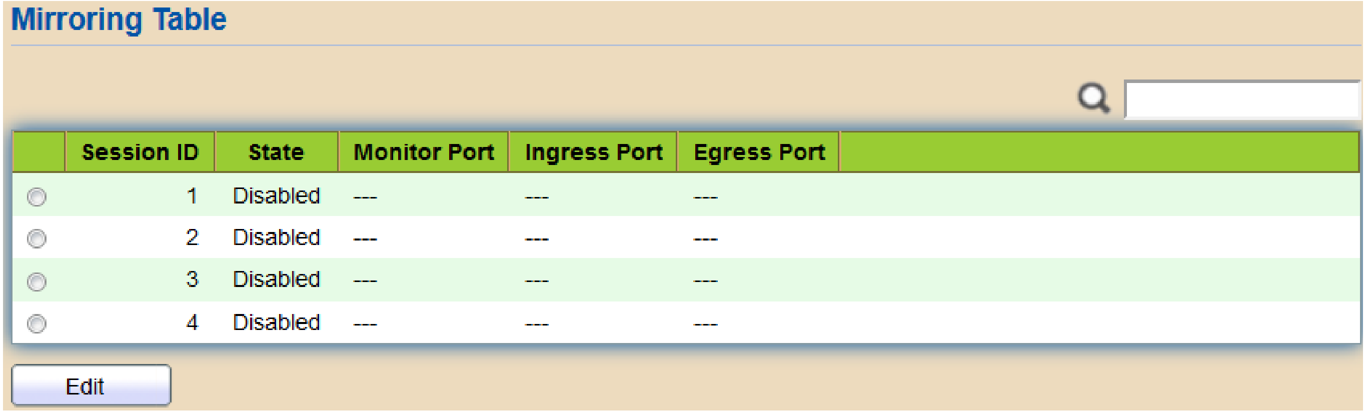
Figure 139 - Diagnostics > Logging > Remote Server

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.
Severity	The minimum severity. • Emergence: System is not usable. • Alert: Immediate action is needed. • Critical: System is in the critical condition. • Error: System is in error condition • Warning: System warning has occurred

	• Notice: System is functioning properly, but a system notice has occurred. • Informational: Device information. • Debug: Provides detailed information about an event.

4.13.2. Mirroring

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



Mirroring Table

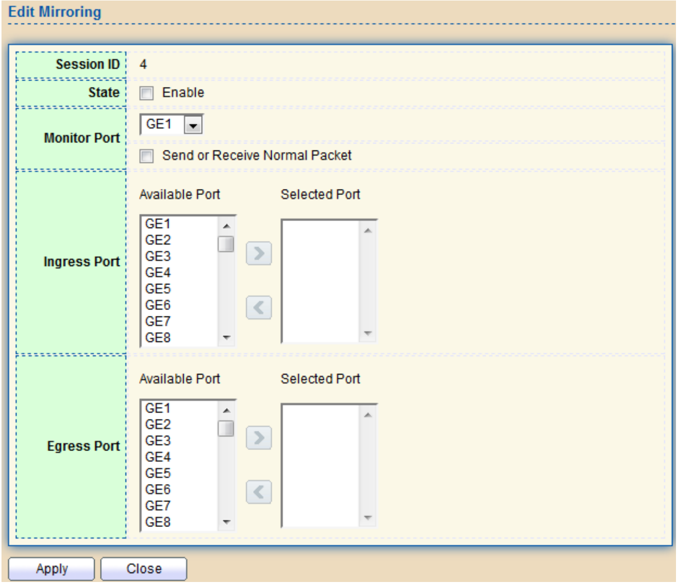
	Session ID	State	Monitor Port	Ingress Port	Egress Port
○	1	Disabled	---	---	---
○	2	Disabled	---	---	---
○	3	Disabled	---	---	---
○	4	Disabled	---	---	---

Figure 140 - 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.



Edit Mirroring

Session ID	4
State	□ Enable
Monitor Port	GE1 ▾ □ Send or Receive Normal Packet
Ingress Port	Available Port: GE1, GE2, GE3, GE4, GE5, GE6, GE7, GE8 Selected Port:
Egress Port	Available Port: GE1, GE2, GE3, GE4, GE5, GE6, GE7, GE8 Selected Port:

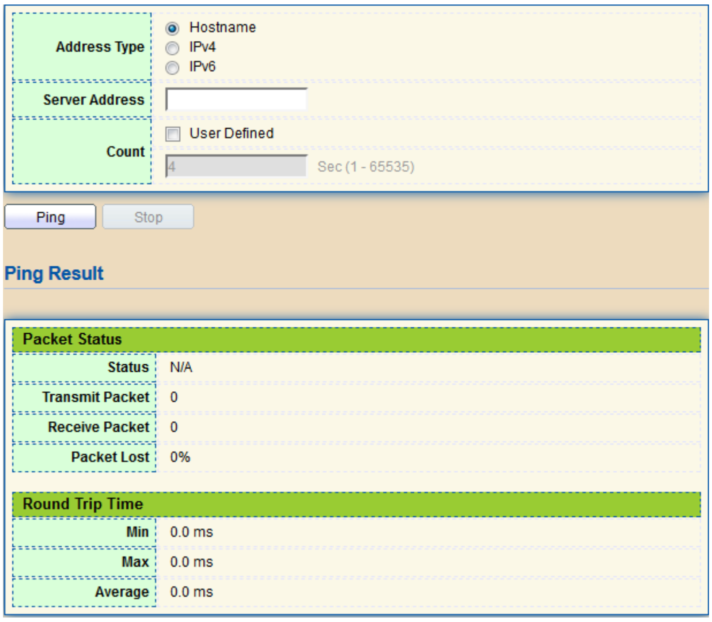
Figure 141- Diagnostics > Mirroring > Edit Mirroring

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.

4.13.3. Ping

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



Address Type	● Hostname ○ IPv4 ○ IPv6
Server Address	
Count	□ User Defined 4 Sec (1 - 65535)

Ping Result

Packet Status	
Status	N/A
Transmit Packet	0
Receive Packet	0
Packet Lost	0%

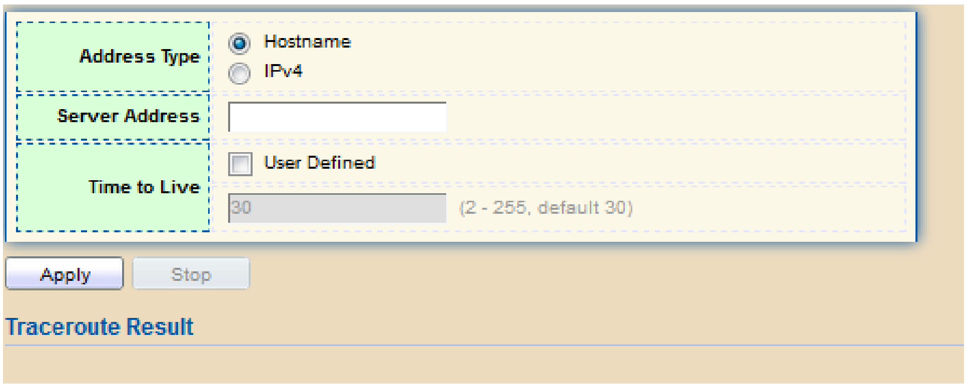
Round Trip Time	
Min	0.0 ms
Max	0.0 ms
Average	0.0 ms

Figure 142 - 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.

4.13.4. Traceroute

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



Address Type	● Hostname ○ IPv4
Server Address	
Time to Live	□ User Defined 30 (2 - 255, default 30)

Figure 143 - 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.

4.14. Management

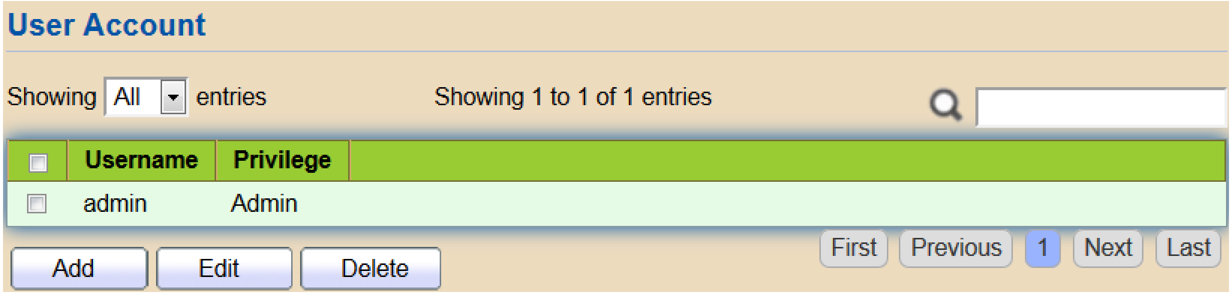
Use the Management pages to configure settings for the switch management features.

4.14.1. 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**



User Account

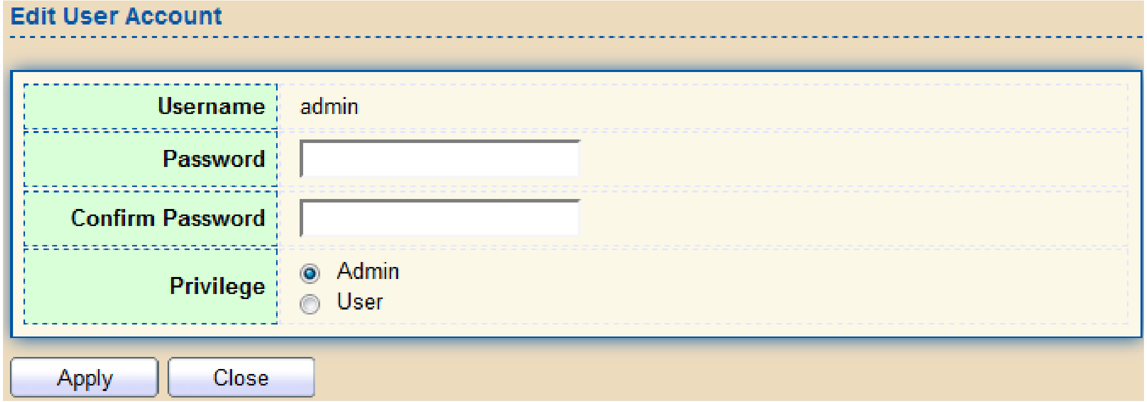
Showing All entries Showing 1 to 1 of 1 entries

□	Username	Privilege
□	admin	Admin

Figure 150 - Management > User Account

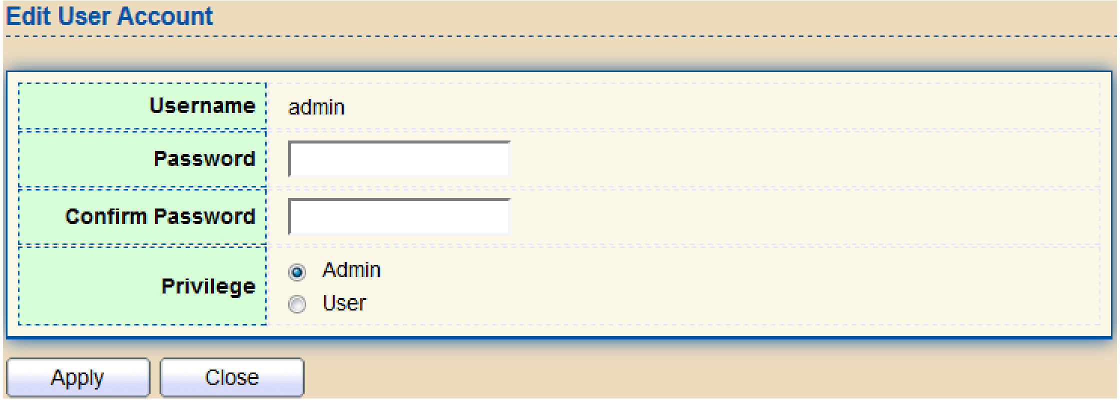
Item	Description
Username	User name of the account.
Privilege	Select privilege level for new account. • Admin: Allow to change switch settings. Privilege value equals to 15. • User: See switch settings only. Not allow to change it. Privilege level equals to 1.

Click "Add"or “Edit” button to view the Add/Edit User Account menu.



Edit User Account

Username	admin
Password	
Confirm Password	
Privilege	● Admin ○ User



Edit User Account

Username	admin
Password	
Confirm Password	
Privilege	● Admin ○ User

Figure 151 - Management > User Account > Add/Edit User Account

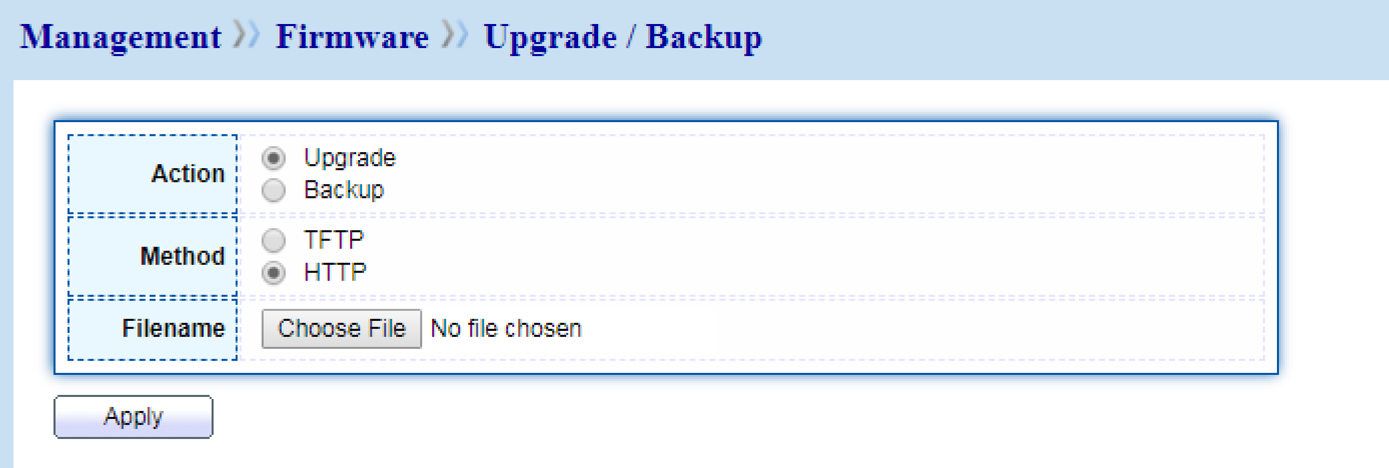
Item	Description
Username	User name of the account.
Password	Set password of the account.
Confirm Password	Set the same password of the account as in “Password” field.
Privilege	Select privilege level for new account. • Admin: Allow to change switch settings. Privilege value equals to 15. • User: See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

4.14.2. Firmware

4.14.2.1. 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**



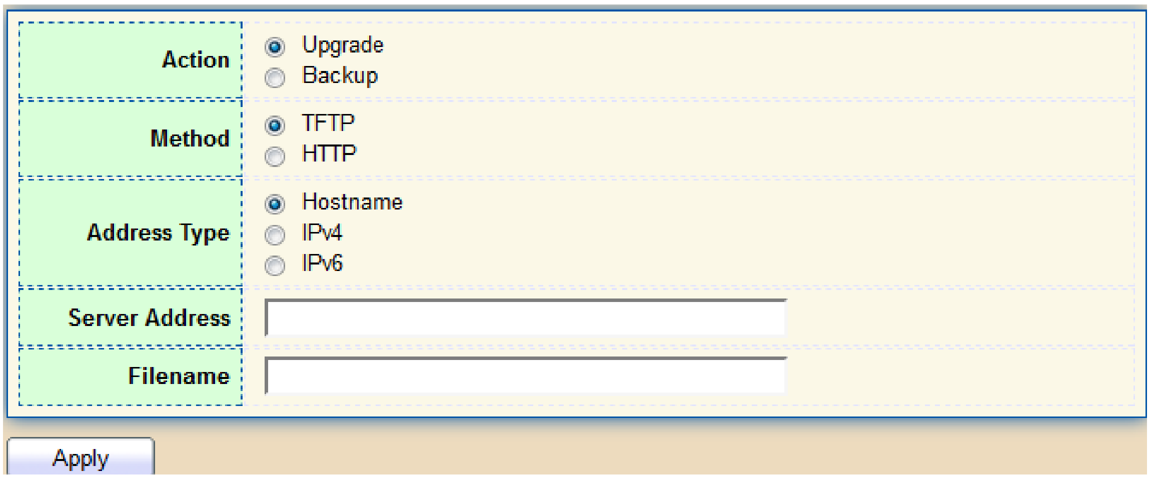
Management » Firmware » Upgrade / Backup

Action	● Upgrade ○ Backup
Method	○ TFTP ● HTTP
Filename	Choose File No file chosen

Figure 152 - Management > Firmware > Upgrade/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**

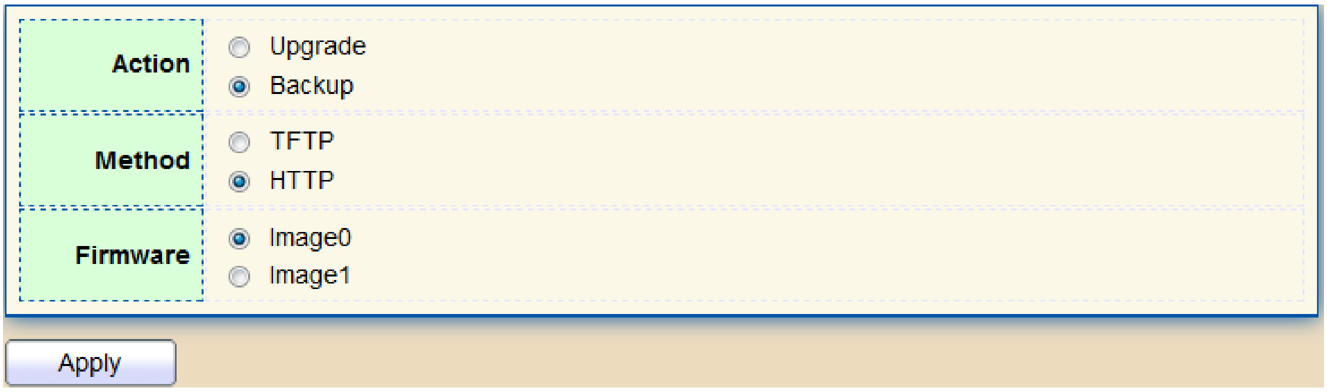


Action	● Upgrade ○ Backup
Method	● TFTP ○ HTTP
Address Type	● Hostname ○ IPv4 ○ IPv6
Server Address	
Filename	

Figure 153 - Management > Firmware > Upgrade/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**

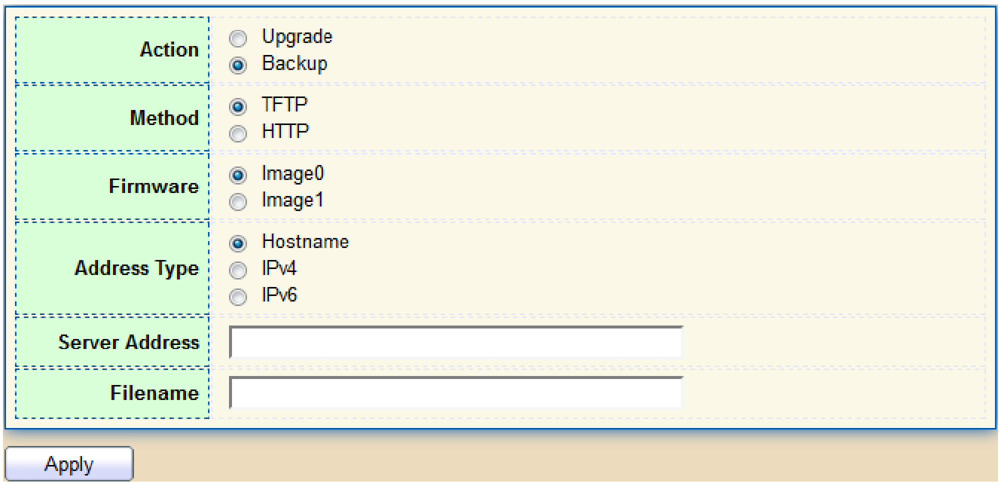


Action	○ Upgrade ● Backup
Method	○ TFTP ● HTTP
Firmware	● Image0 ○ Image1

Figure 154 - Management > Firmware > Upgrade/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 view the Firmware Upgrade/Backup menu, navigate to **Management > Firmware > Upgrade/Backup**.



Action	○ Upgrade ● Backup
Method	● TFTP ○ HTTP
Firmware	● Image0 ○ Image1
Address Type	● Hostname ○ IPv4 ○ IPv6
Server Address	
Filename	

Figure 155 - Management > Firmware >Upgrade/Backup

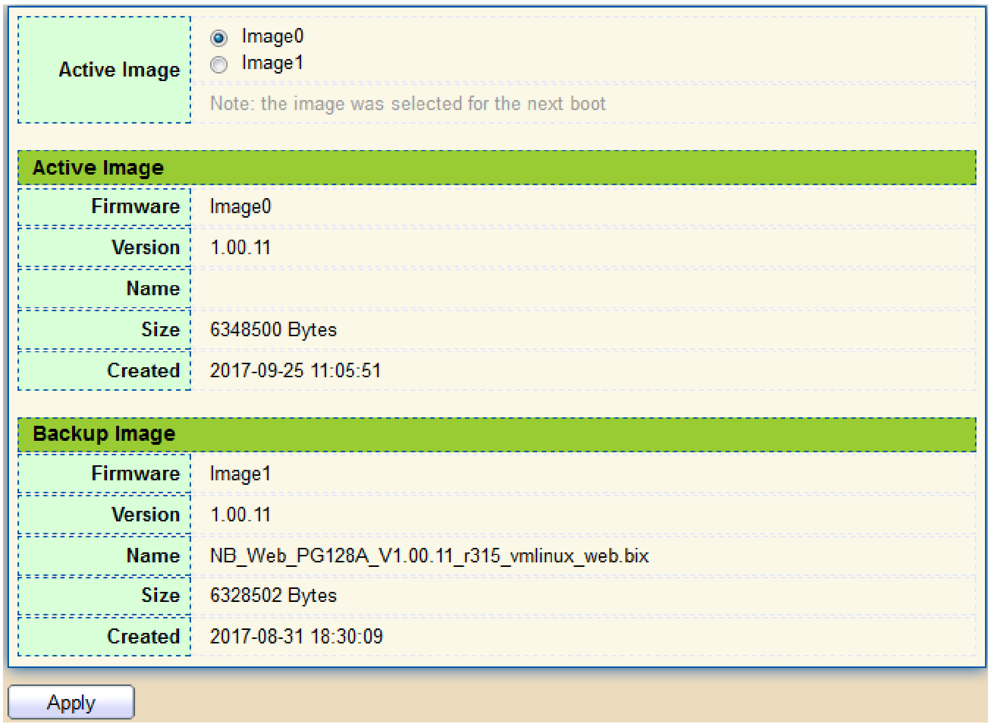
Item	Description
Action	Firmware operations • Upgrade: Upgrade firmware from remote host to DUT • Backup: Backup firmware image from DUT to remote host
Method	Firmware upgrade / backup method • TFTP: Using TFTP to upgrade/backup firmware. • HTTP: Using WEB browser to upgrade/backup firmware.
Firmware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

4.14.2.2. 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**.



Active Image
● Image0
○ Image1
Note: the image was selected for the next boot

Active Image

Firmware	Image0
Version	1.00.11
Name	
Size	6348500 Bytes
Created	2017-09-25 11:05:51

Backup Image

Firmware	Image1
Version	1.00.11
Name	NB_Web_PG128A_V1.00.11_r315_vmlinux_web.bix
Size	6328502 Bytes
Created	2017-08-31 18:30:09

Figure 156 - Management > Firmware > Active Image

Item	Description
Active Image	Select firmware image to use on next booting

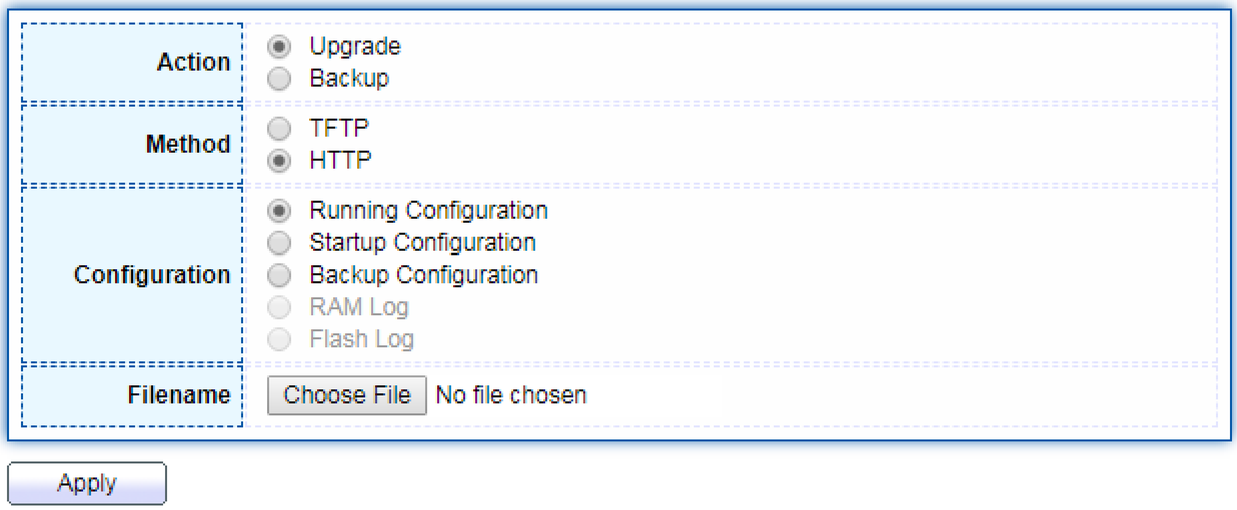
Firmware	Firmware flash partition name.
Version	Firmware version.
Name	Firmware name.
Size	Firmware image size.
Created	Firmware image created date.

4.14.3. Configuration

4.14.3.1. 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**

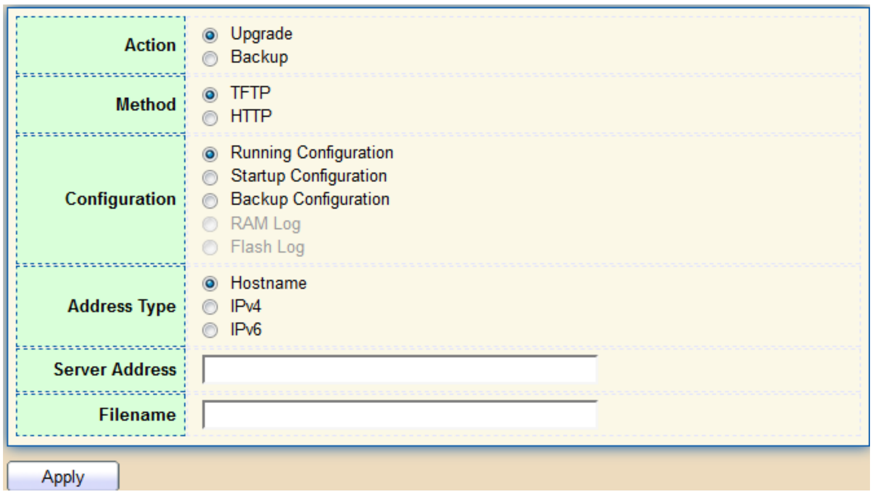


Action	● Upgrade ○ Backup
Method	○ TFTP ● HTTP
Configuration	● Running Configuration ○ Startup Configuration ○ Backup Configuration ○ RAM Log ○ Flash Log
Filename	Choose File No file chosen

Figure 157 - 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**



Action: ● Upgrade ○ Backup

Method: ● TFTP ○ HTTP

Configuration: ● Running Configuration ○ Startup Configuration ○ Backup Configuration ○ RAM Log ○ Flash Log

Address Type: ● Hostname ○ IPv4 ○ IPv6

Server Address:

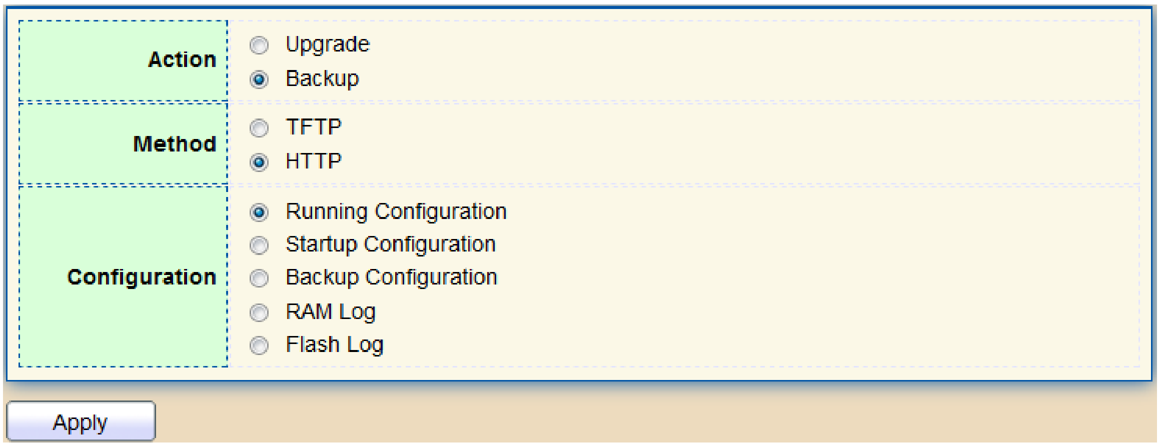
Filename:

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
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	File name saved on remote TFTP server

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



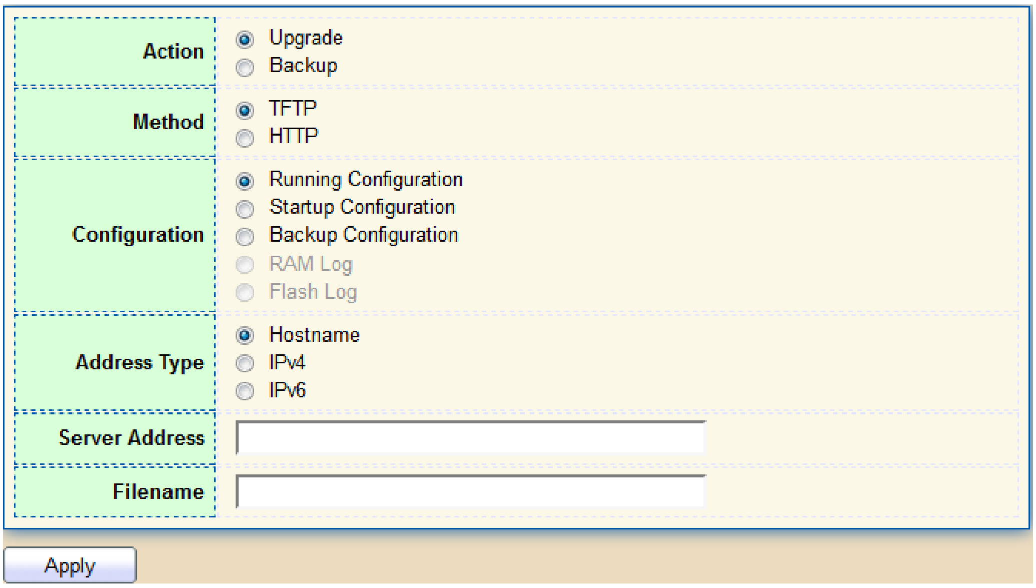
Action	○ Upgrade ● Backup
Method	○ TFTP ● HTTP
Configuration	● Running Configuration ○ Startup Configuration ○ Backup Configuration ○ RAM Log ○ Flash Log

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: Backup running configuration file. • Startup Configuration: Backup start configuration file. • Backup Configuration: 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**



Action	● Upgrade ○ Backup
Method	● TFTP ○ HTTP
Configuration	● Running Configuration ○ Startup Configuration ○ Backup Configuration ○ RAM Log ○ Flash Log
Address Type	● Hostname ○ IPv4 ○ IPv6
Server Address	
Filename	

Figure 160 - Management > Configuration > Upgrade/Backup

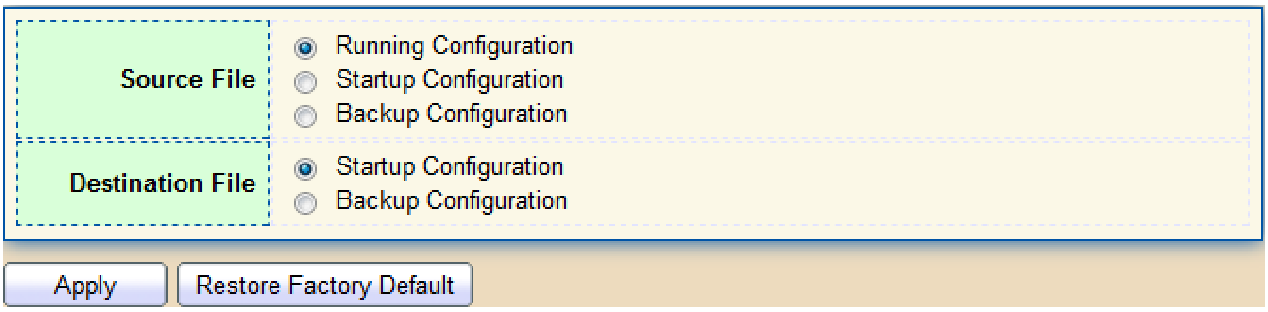
Item	Description
Action	Configuration operations • Upgrade: Upgrade firmware from remote host to DUT

	• 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 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.
Filename	File name saved on remote TFTP server.

4.14.3.2. 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**



Source File
● Running Configuration
○ Startup Configuration
○ Backup Configuration

Destination File
● Startup Configuration
○ Backup Configuration

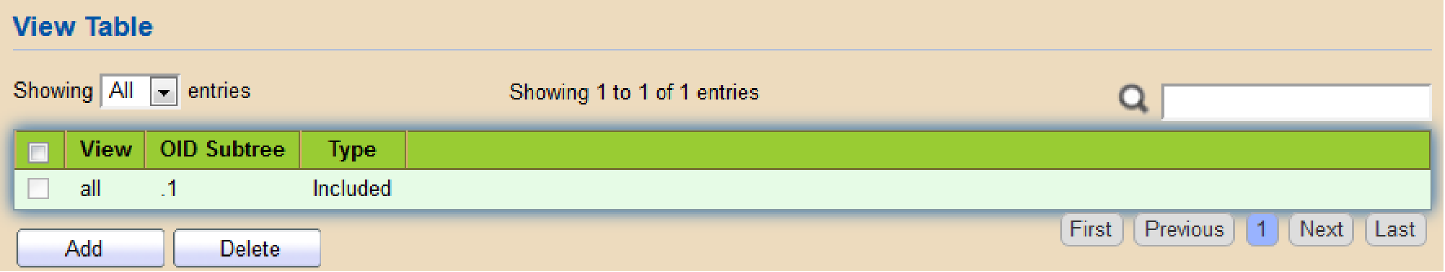
Figure 161 - Management > Configuration > Save Configuration

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.

4.14.4. SNMP

4.14.4.1. View

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



View Table

Showing All entries — Showing 1 to 1 of 1 entries

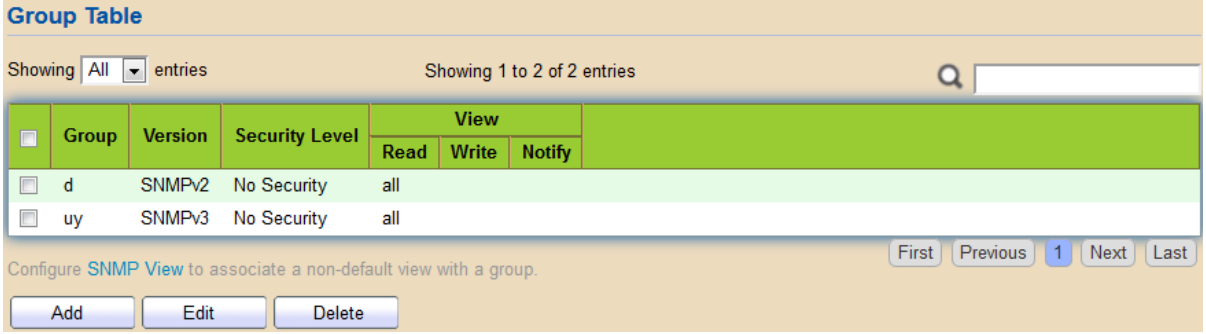
□	View	OID Subtree	Type
□	all	.1	Included

Figure 162 - 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

4.14.4.2. Group

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



Group Table

Showing All entries — Showing 1 to 2 of 2 entries

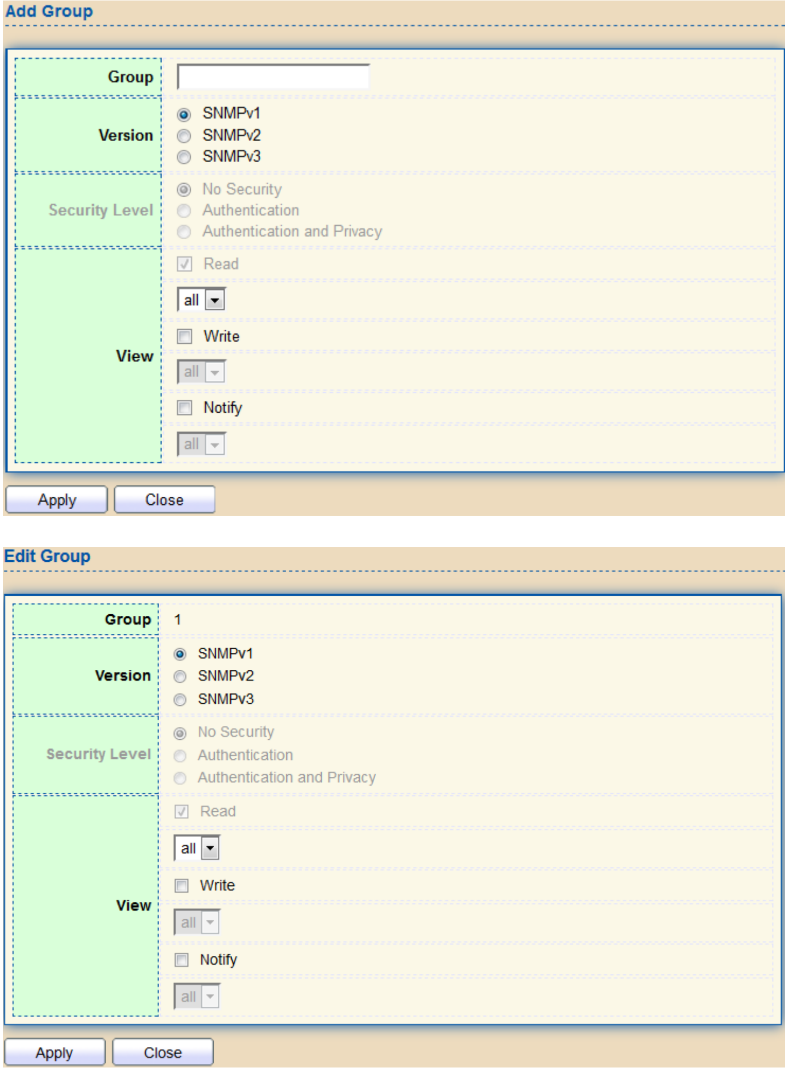
□	Group	Version	Security Level	View		
				Read	Write	Notify
□	d	SNMPv2	No Security	all		
□	uy	SNMPv3	No Security	all		

Configure SNMP View to associate a non-default view with a group.

Figure 163 - 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.



Add Group

Group	
Version	● SNMPv1 ○ SNMPv2 ○ SNMPv3
Security Level	● No Security ○ Authentication ○ Authentication and Privacy
View	☑ Read all □ Write all □ Notify all

Apply Close

Edit Group

Group	1
Version	● SNMPv1 ○ SNMPv2 ○ SNMPv3
Security Level	● No Security ○ Authentication ○ Authentication and Privacy
View	☑ Read all □ Write all □ Notify all

Apply Close

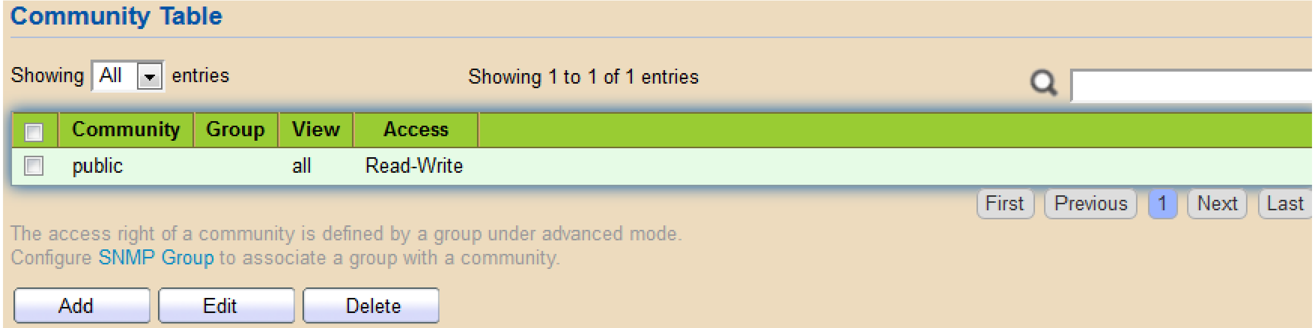
Figure 164 - Management > SNMP > Group > Add/Edit Group

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	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.

4.14.4.3. Community

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



Community Table

Showing All entries   Showing 1 to 1 of 1 entries

□	Community	Group	View	Access
□	public		all	Read-Write

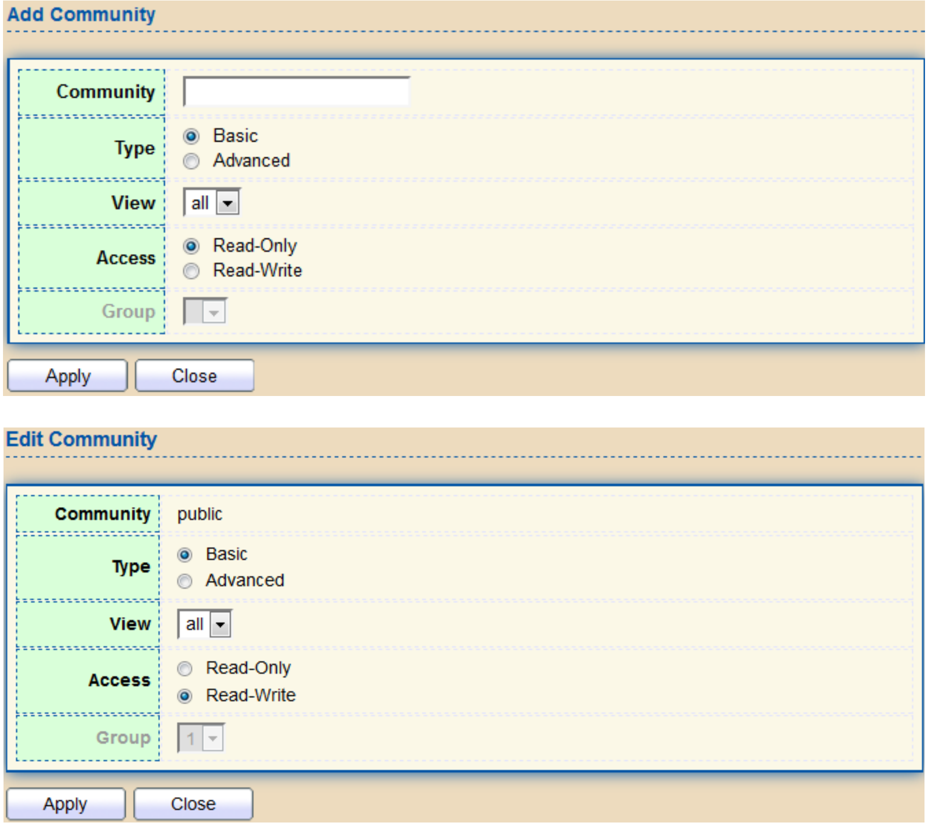
The access right of a community is defined by a group under advanced mode.
Configure SNMP Group to associate a group with a community.

Figure 165 - 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.



Add Community

Community:

Type: ● Basic ○ Advanced

View: all

Access: ● Read-Only ○ Read-Write

Group:

Edit Community

Community: public

Type: ● Basic ○ Advanced

View: all

Access: ○ Read-Only ● Read-Write

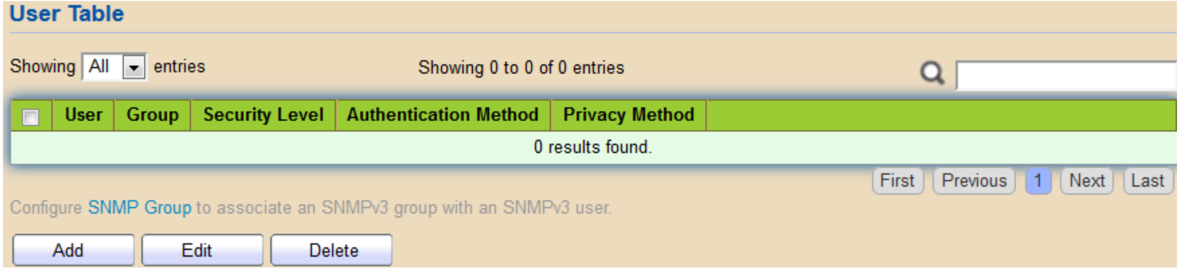
Group: 1

Figure 166 - 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.

4.14.4.4. User

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



User Table

Showing All entries   Showing 0 to 0 of 0 entries

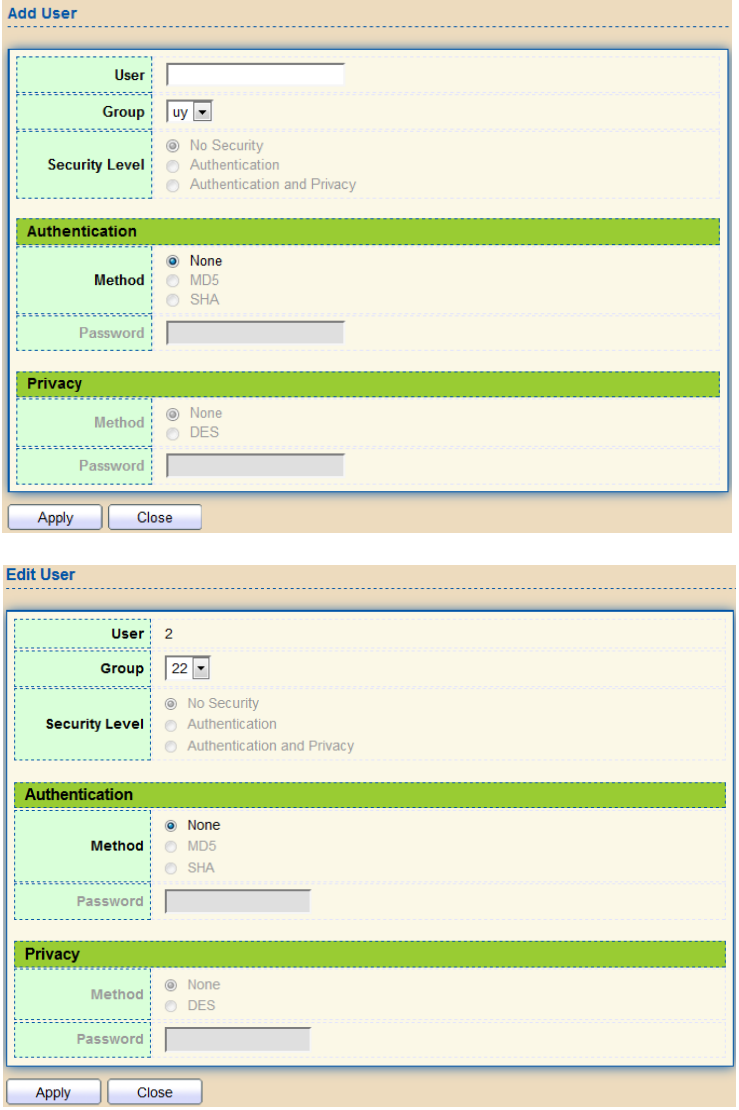
□	User	Group	Security Level	Authentication Method	Privacy Method
0 results found.					

Configure SNMP Group to associate an SNMPv3 group with an SNMPv3 user.

Figure 167 - 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.



Add User

User

Group: uy

Security Level: ● No Security ○ Authentication ○ Authentication and Privacy

Authentication

Method: ● None ○ MD5 ○ SHA

Password

Privacy

Method: ● None ○ DES

Password

Apply Close

Edit User

User: 2

Group: 22

Security Level: ● No Security ○ Authentication ○ Authentication and Privacy

Authentication

Method: ● None ○ MD5 ○ SHA

Password

Privacy

Method: ● None ○ DES

Password

Apply Close

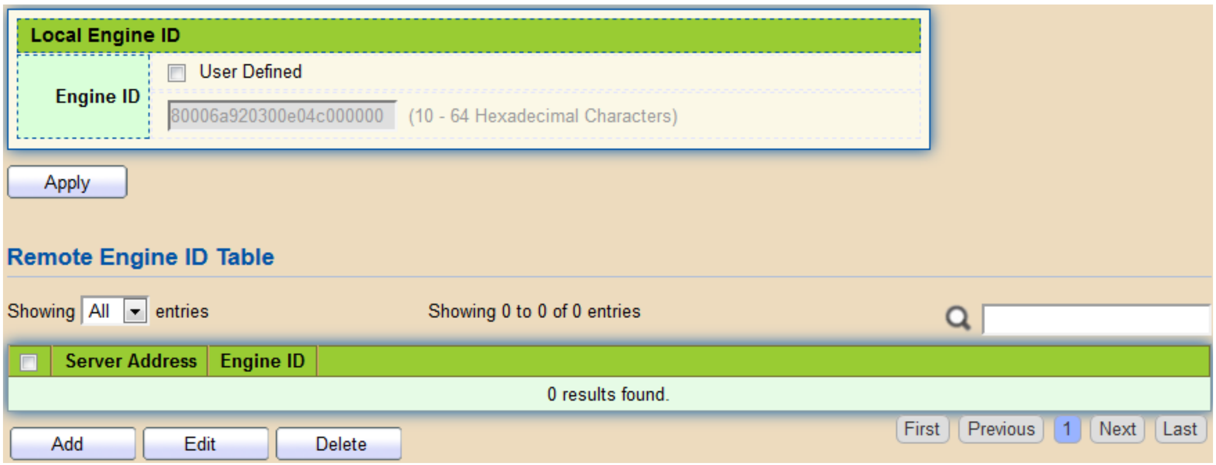
Figure 168 - Management > SNMP > User > Add/Edit User

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.

4.14.4.5. Engine ID

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


Local Engine ID

Engine ID ☐ User Defined

80006a920300e04c000000 (10 - 64 Hexadecimal Characters)

Apply

Remote Engine ID Table

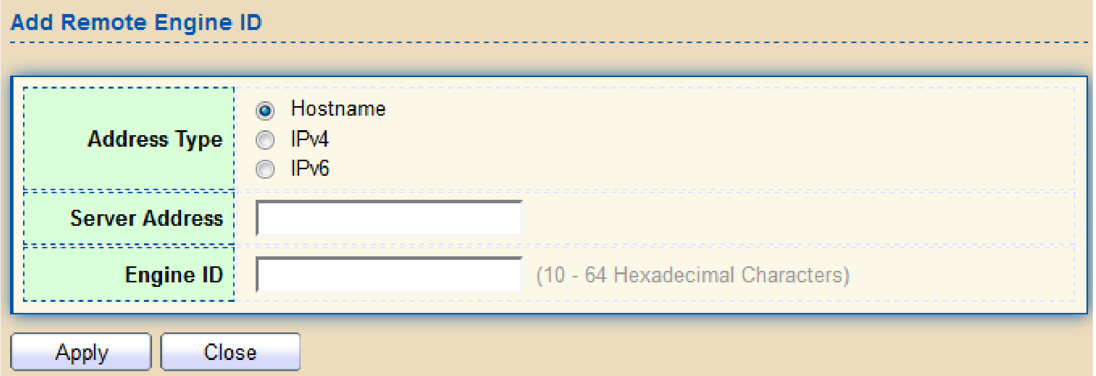
Showing All entries Showing 0 to 0 of 0 entries

☐	Server Address	Engine ID
0 results found.		

Figure 169 - 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.



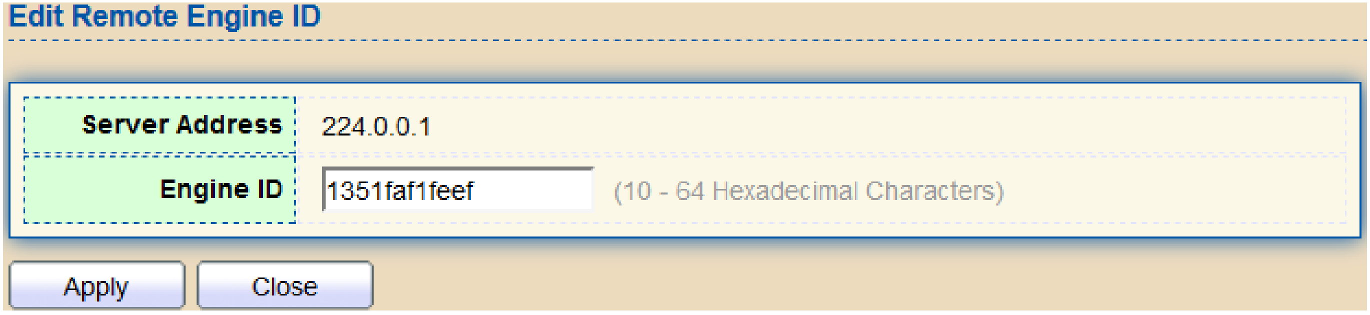
Add Remote Engine ID

Address Type	● Hostname ○ IPv4 ○ IPv6
Server Address	
Engine ID	(10 - 64 Hexadecimal Characters)

Figure 170 - 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.



Edit Remote Engine ID

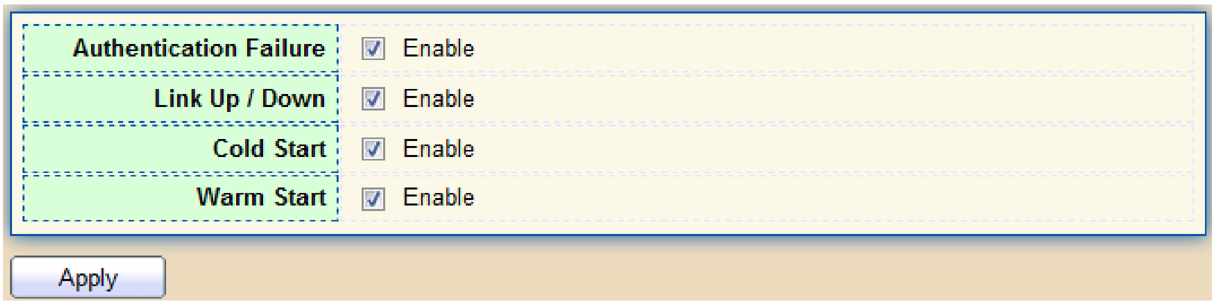
Server Address	224.0.0.1
Engine ID	1351faf1feef (10 - 64 Hexadecimal Characters)

Figure 171 - 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.

4.14.4.6. Trap Event

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



Authentication Failure ☑ Enable

Link Up / Down ☑ Enable

Cold Start ☑ Enable

Warm Start ☑ Enable

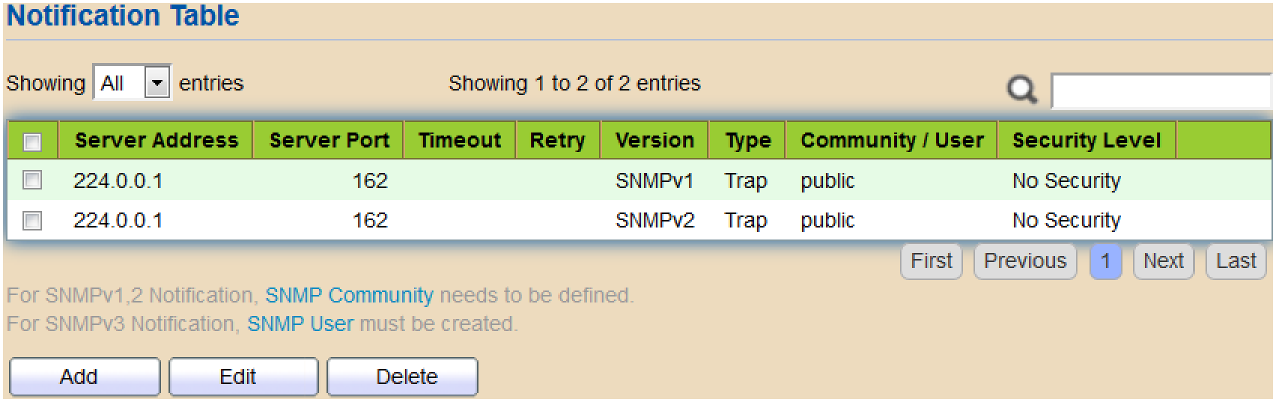
Figure 172 - Management > SNMP > Trap Event

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.

4.14.4.7. Notification

To configure the hosts to receive SNMPv1/v2/v3 notification, click **Management**

> SNMP > Notification.



Notification Table

Showing All entries   Showing 1 to 2 of 2 entries

□	Server Address	Server Port	Timeout	Retry	Version	Type	Community / User	Security Level
□	224.0.0.1	162			SNMPv1	Trap	public	No Security
□	224.0.0.1	162			SNMPv2	Trap	public	No Security

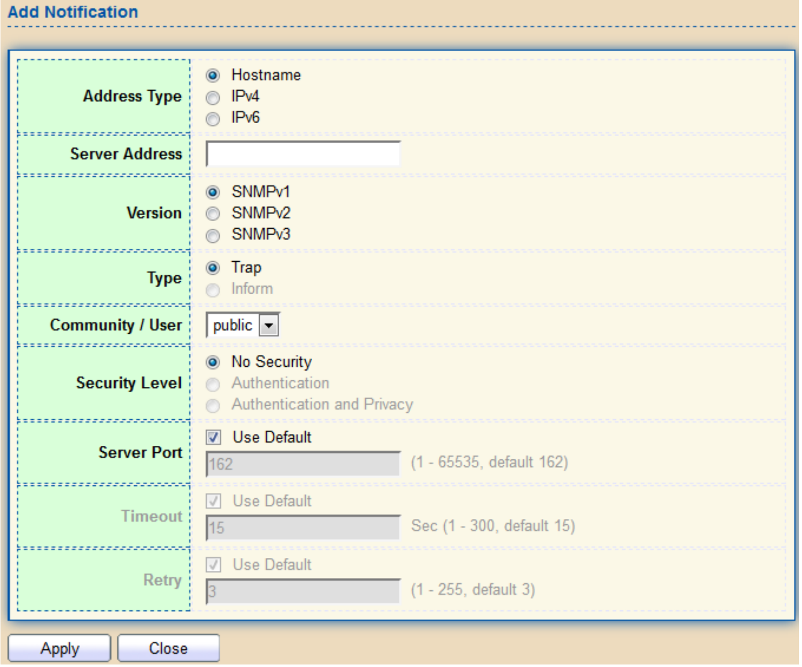
For SNMPv1,2 Notification, SNMP Community needs to be defined.
For SNMPv3 Notification, SNMP User must be created.

Figure 173 - 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.



Add Notification

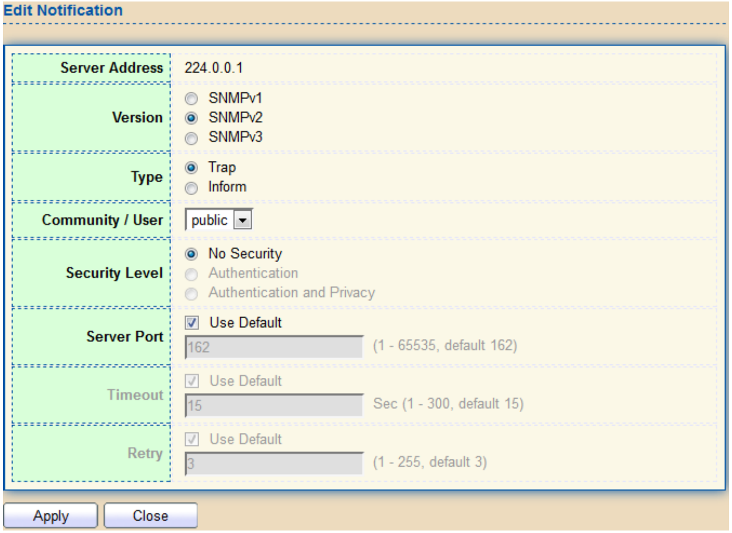
Address Type	● Hostname ○ IPv4 ○ IPv6
Server Address	
Version	● SNMPv1 ○ SNMPv2 ○ SNMPv3
Type	● Trap ○ Inform
Community / User	public
Security Level	● No Security ○ Authentication ○ Authentication and Privacy
Server Port	☑ Use Default 162 (1 - 65535, default 162)
Timeout	☑ Use Default 15 Sec (1 - 300, default 15)
Retry	☑ Use Default 3 (1 - 255, default 3)

Figure 174 - 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.



Edit Notification

Server Address	224.0.0.1
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)

Figure 175 - Management > SNMP > Notification > Edit Notification

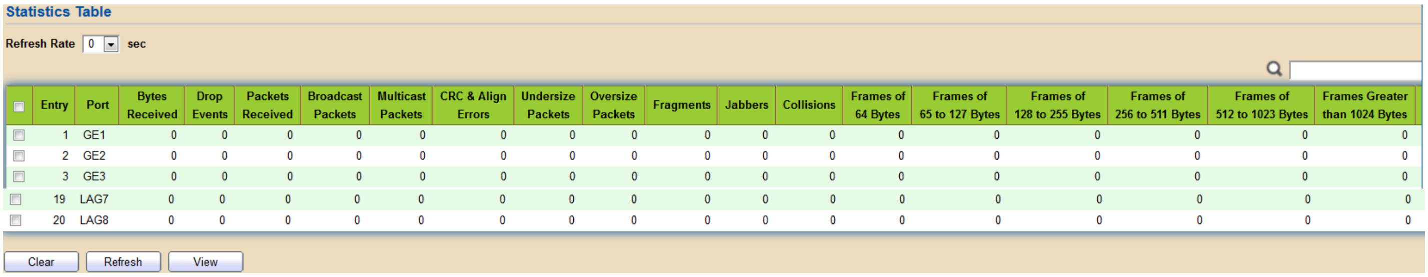
Item	Description
Server Address	Edit SNMP notify recipients address
Version	Specify SNMP notification version • SNMPv1: SNMP Version 1 notification. • SNMPv2: SNMP Version 2 notification. • SNMPv3: SNMP Version 3 notification.
Type	Notification Type • Trap: Send SNMP traps to the host. • Inform: Send 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.

4.14.5. RMON

4.14.5.1. Statistics

To display RMON Statistics, click **Management > RMON > Statistics**.



Statistics Table

Refresh Rate 0 sec

□	Entry	Port	Bytes Received	Drop Events	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Oversize Packets	Fragments	Jabbers	Collisions	Frames of 64 Bytes	Frames of 65 to 127 Bytes	Frames of 128 to 255 Bytes	Frames of 256 to 511 Bytes	Frames of 512 to 1023 Bytes	Frames Greater than 1024 Bytes
□	1	GE1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	2	GE2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	3	GE3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	19	LAG7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	20	LAG8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

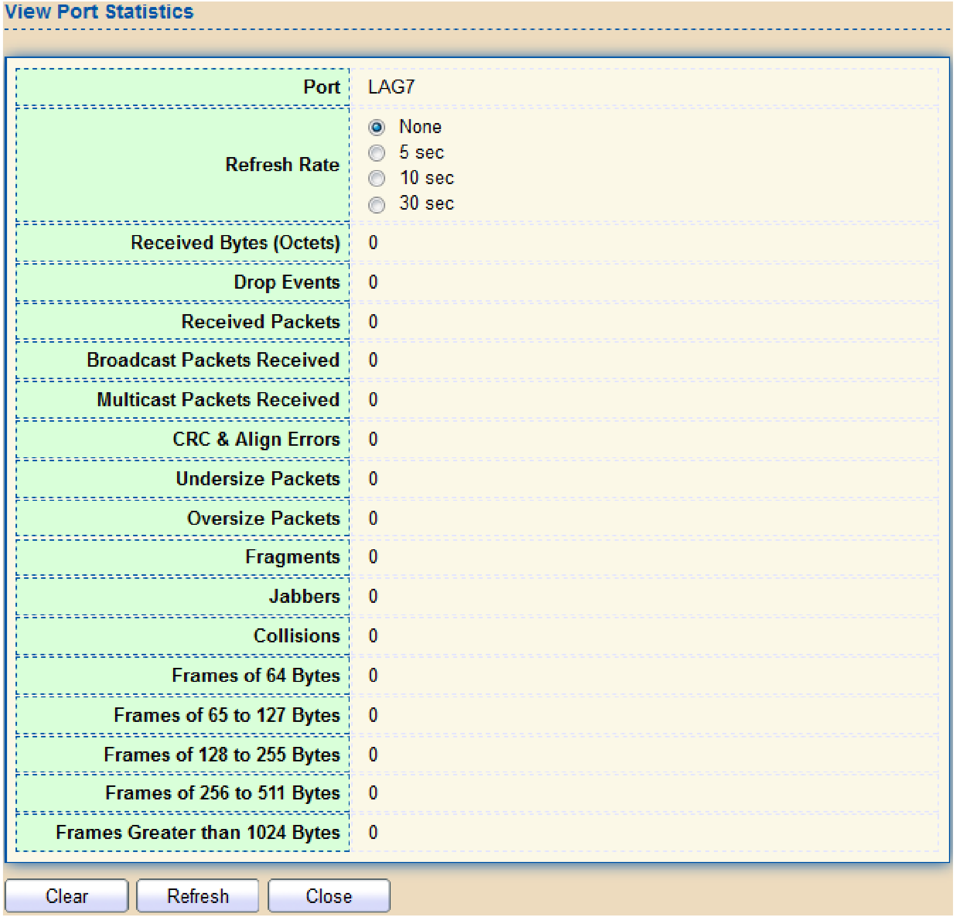
Figure 215 - Management > RMON > Statistics

Item	Description
Port	The port for the RMON statistics.
Bytes Received	Number of octets received, including bad packets and FCS octets, but excluding framing bits.

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

127 Bytes	received.
Frames of 128 to 225 Bytes	Number of frames, containing 128 to 255 bytes that were received.
Frames of 256 to 511 Bytes	Number of frames, containing 256 to 511 bytes that were received.
Frames of 512 to 1023 Bytes	Number of frames, containing 512 to 1023 bytes that were received.
Frames Greater than 1024 Bytes	Number of frames, containing 1024 to 1518 bytes that were received.
Clear	Clear the statistics for the selected ports.
View	View the statistics on the specified port.

Click "View" button to view the view Port Statistics menu.



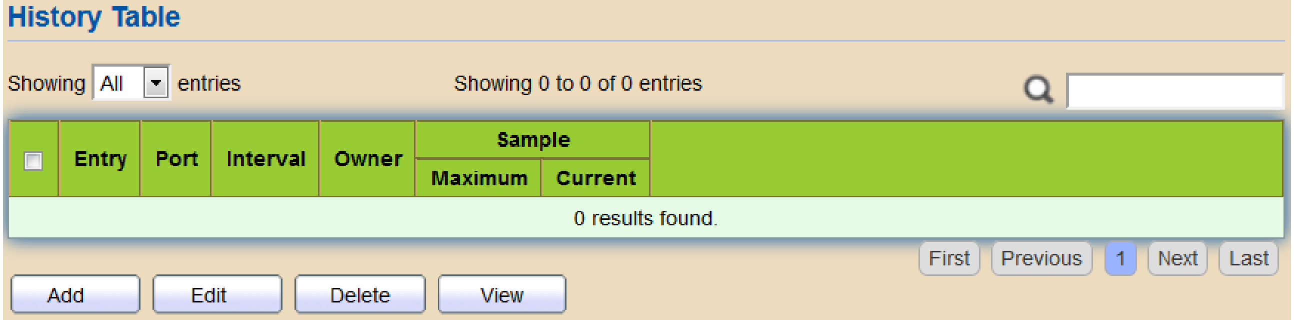
View Port Statistics

Port	LAG7
Refresh Rate	● None ○ 5 sec ○ 10 sec ○ 30 sec
Received Bytes (Octets)	0
Drop Events	0
Received Packets	0
Broadcast Packets Received	0
Multicast Packets Received	0
CRC & Align Errors	0
Undersize Packets	0
Oversize Packets	0
Fragments	0
Jabbers	0
Collisions	0
Frames of 64 Bytes	0
Frames of 65 to 127 Bytes	0
Frames of 128 to 255 Bytes	0
Frames of 256 to 511 Bytes	0
Frames Greater than 1024 Bytes	0

Figure 216 - Management > RMON > Statistics

4.14.5.2. History

For the RMON history, click **Management > RMON > History**.



History Table

Showing All entries Showing 0 to 0 of 0 entries

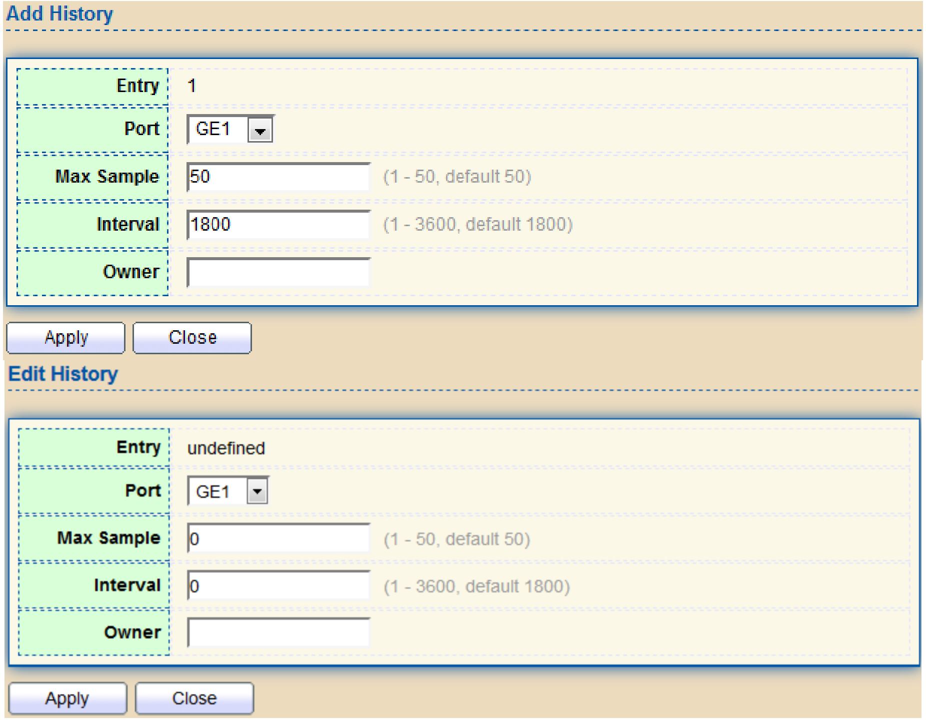
□	Entry	Port	Interval	Owner	Sample	
					Maximum	Current
0 results found.						

Figure 217 - Management > RMON > History

Item	Description

Port	The port for the RMON history.
Interval	The number of seconds for each sample.
Owner	The owner name of event (0~31 characters).
Sample Maximum	The maximum number of buckets.
Sample Current	The current number of buckets.
Add	Add the new RMON history entries
Edit	Edit the RMON history
Delete	Delete the RMON histories
View	View the history log.

Click "Add/Edit" button to Add/Edit the History menu.



Add History

Entry	1	
Port	GE1 ▾	
Max Sample	50	(1 - 50, default 50)
Interval	1800	(1 - 3600, default 1800)
Owner		

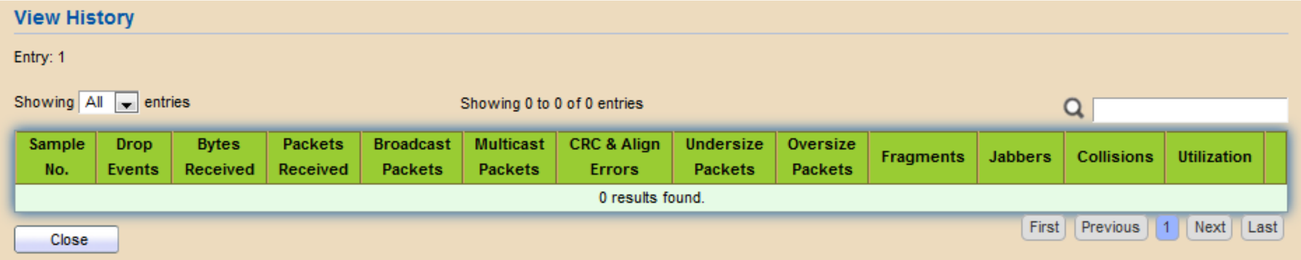
Edit History

Entry	undefined	
Port	GE1 ▾	
Max Sample	0	(1 - 50, default 50)
Interval	0	(1 - 3600, default 1800)
Owner		

Figure 218 - Management > RMON > Add /Edit History

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

Click "View" button to view the History menu.



View History

Entry: 1

Showing All entries

Showing 0 to 0 of 0 entries

Sample No.	Drop Events	Bytes Received	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Oversize Packets	Fragments	Jabbers	Collisions	Utilization

0 results found.

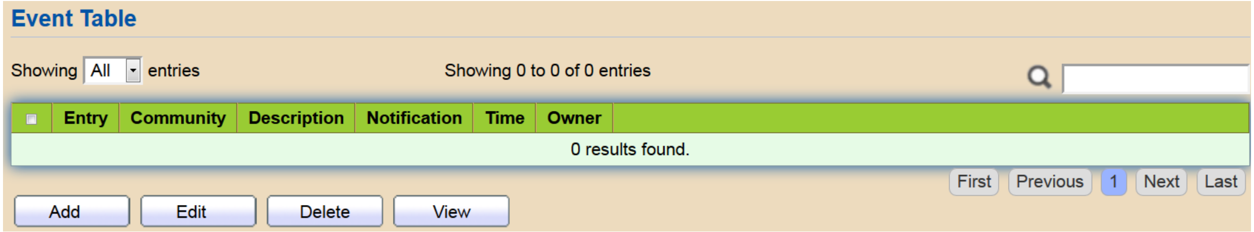
Figure 219 - Management > RMON > View History

Item	Description
Port	The port for the RMON statistics.
Bytes Received	Number of octets received, including bad packets and FCS. octets, but excluding framing bits
Drop Events	Number of packets that were dropped.
Packets Received	Number of packets received, including bad packets, Multicast packets, and Broadcast packets.
Broadcast Packets	Number of good Broadcast packets received. This number does not include Multicast packets.
Multicast Packets	Number of good Multicast packets received.
CRC & Align Errors	Number of CRC and Align errors that have occurred.
Undersize	Number of undersized packets (less than 64 octets)

Packages	received.
Oversize Packages	Number of oversized packets (over 1518 octets) received.
Fragments	Number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received.
Jabbers	Number of received packets that were longer than 1632 octets. This number excludes frame bits, but includes FCS octets that had either a bad FCS (Frame Check Sequence) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. A Jabber packet is defined as an Ethernet frame that satisfies the following criteria: □ ● Packet data length is greater than MRU. ● Packet has an invalid CRC. ● RX error event has not been detected.
Collision	Number of collisions received. If Jumbo Frames are enabled, the threshold of Jabber Frames is raised to the maximum. size of Jumbo Frames.
Utilization	Percentage of current interface traffic compared to the maximum traffic that the interface can handle.

4.14.5.3. Event

For the RMON event, click **Management > RMON > Event**.



Event Table

Showing All entries

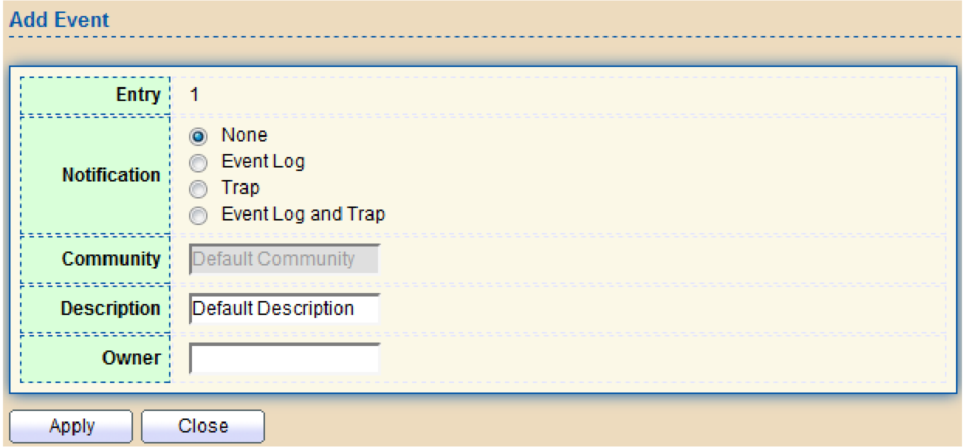
Showing 0 to 0 of 0 entries

□	Entry	Community	Description	Notification	Time	Owner
0 results found.						

Figure 220 - Management > RMON > Event

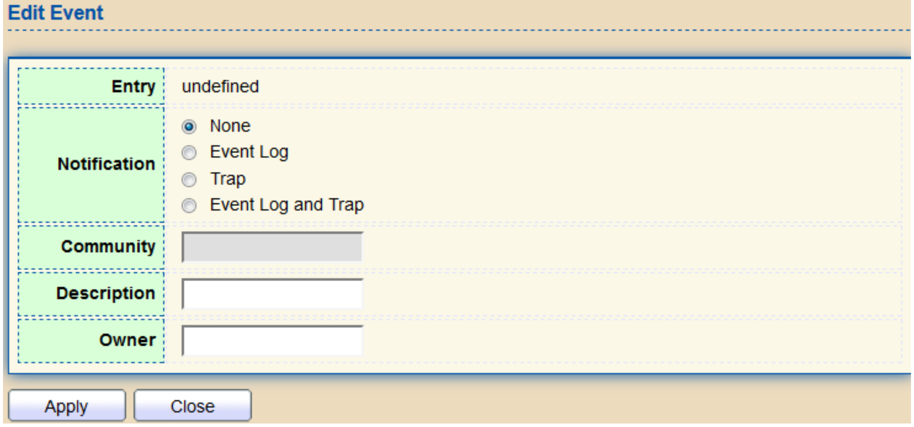
Item	Description
Community	The SNMP community when the notification type is specified as trap
Description	The description for the event
Notification	The notification type for the event, and the possible value are: ● None: Nothing for notification. ● Event Log: Logging the event in the RMON Event Log table. ● Trap: Send a SNMP trap. · ● Event Log and Trap: Logging the event and send the SNMP. trap.
Time	The time that the event was triggered.
Owner	The owner for the event.

Click "Add/Edit" button to view the Add/Edit Event menu.



Add Event

Entry	1
Notification	● None ○ Event Log ○ Trap ○ Event Log and Trap
Community	Default Community
Description	Default Description
Owner	



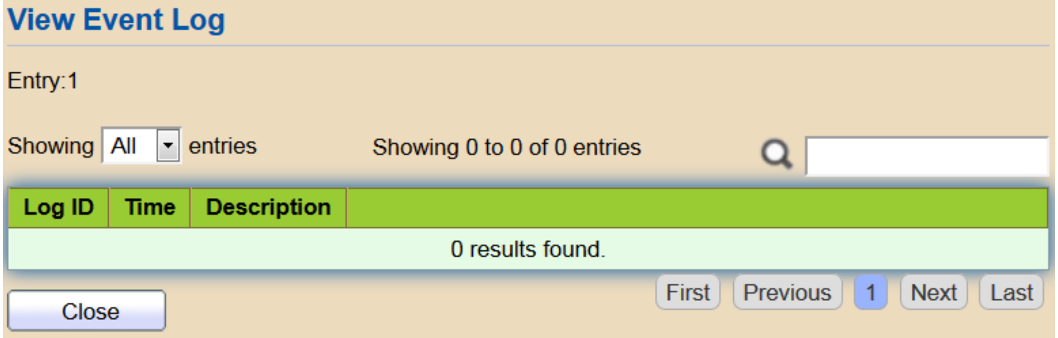
Edit Event

Entry	undefined
Notification	● None ○ Event Log ○ Trap ○ Event Log and Trap
Community	
Description	
Owner	

Figure 221 - Management > RMON > Add/Edit Event

Item	Description
Notification	Specify the notification type for the event, and the possible value are: ・ ● None: Nothing for notification. ・ ● Event Log: Logging the event in the RMON Event Log table ● Trap: Send a SNMP trap. ・ ● Event Log and Trap: Logging the event and send the SNMP trap
Community	Specify the SNMP community when the notification type is specified as “Trap” pr “Event Log and Trap”
Description	Specify the description for the event.
Owner	Specify owner for the event.

Click "View" button to view the View Event Log menu.



View Event Log

Entry:1

Showing All entries Showing 0 to 0 of 0 entries

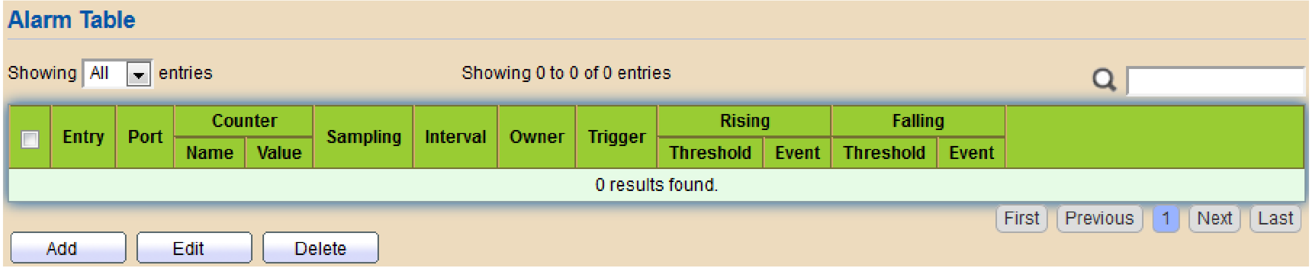
Log ID	Time	Description
0 results found.		

Figure 222 - Management > RMON > View Event Log

Item	Description
Log ID	The log identifier.
Time	The time that the event was triggered.
Description	The description for the event.

4.14.5.4. Alarm

For the RMON Alarm menu, click **Management > RMON > Alarm**.



Alarm Table

Showing All entries Showing 0 to 0 of 0 entries

□	Entry	Port	Counter		Sampling	Interval	Owner	Trigger	Rising		Falling	
			Name	Value					Threshold	Event	Threshold	Event
0 results found.												

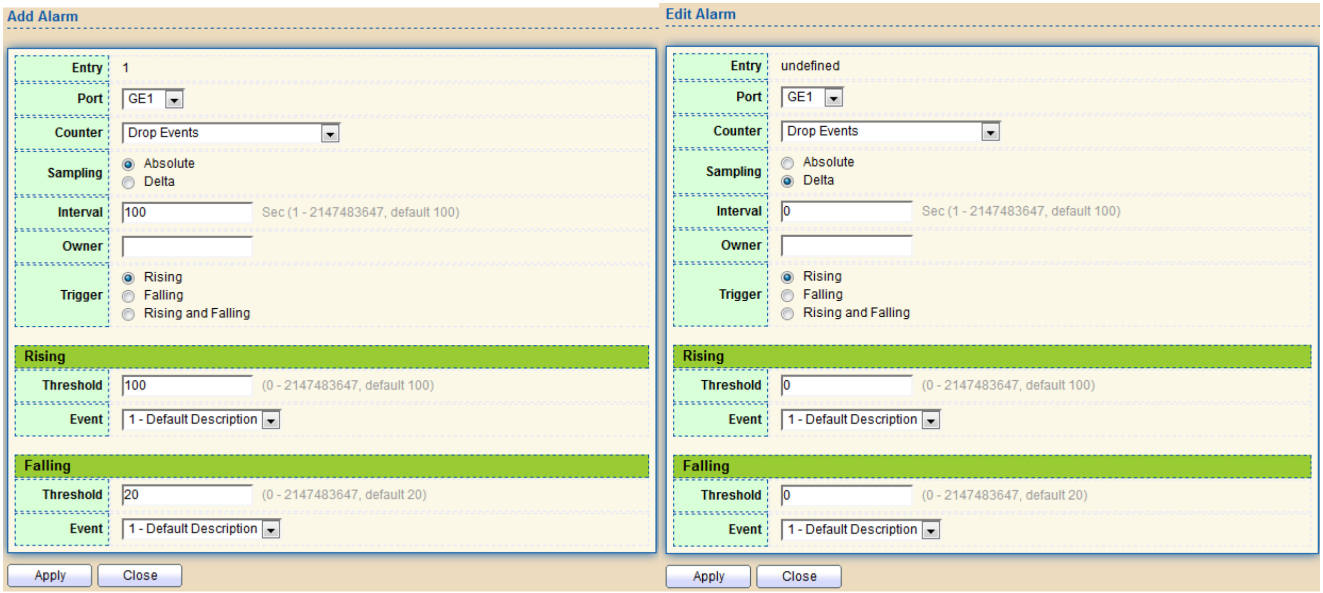
Figure 223 - Management > RMON > Alarm

Item	Description
Port	The port configuration for the RMON alarm.
Counter	The counter for sampling ・ ● DropEvents (Drop Event): Total number of events

	received in which the packets were dropped. · ● Octets (Received Bytes): Octets. · ● Pkts (Received Packets): Number of packets.
	● BroadcastPkts (Broadcast Packets Received): Broadcast packets. · ● MulticastPkts (Multicast Packets Received): Multicast packets. · ● CRCAlignError (CRC and Align Error): CRC alignment error. · ● UndersizePkts (Undersize Packets): Number of undersized packets. · ● OversizePkts (Oversize Packets): Number of oversized packets. · ● Fragments (Fragments): Total number of packet fragment. · ● Jabbers (Jabbers): Total number of packet jabber. ● Collisions (Collisions): Collision. · ● Pkts64Octetes (Frames of 64 Bytes): Number of packets size 64 octets. · ● Pkts65to127Octetes (Frames of 65 to 127 Bytes): Number of packets size 65 to 127 octets. ● Pkts128to255Octetes (Frames of 128 to 255 Bytes): Number of packets size 128 to 255 octets. ● Pkts256to511Octetes (Frames of 256 to 511 Bytes): Number of packets size 256 to 511 octets. ● Pkts512to1023Octetes (Frames of 512 to 1023 Bytes):

	Number of packets size 512 to 1023 octets. ● Pkts1024to1518Octets (Frames Greater than 1024 Bytes): Number of packets size 1024 to 1518 octets.
Sampling	The sampling type including: ・ ● Absolute: The selected variable value is compared directly with the thresholds at the end of the sampling interval. ・ ● Delta: The selected variable value of the last sample is subtracted from the current value and the difference is compared with the thresholds.
Interval	The number of seconds for each sample.
Owner	The owner for the alarm entry.
Trigger	The type of event triggering.
Rising Threshold	The threshold for firing rising event.
Rising Event	The rising event when alarm was fired.
Falling Threshold	The threshold for firing falling event.
Falling Event	The falling event when alarm was fired.

Click "Add/Edit" button to view the Add/Edit menu.



Add Alarm

Entry	1
Port	GE1
Counter	Drop Events
Sampling	● Absolute ○ Delta
Interval	100 Sec (1 - 2147483647, default 100)
Owner	
Trigger	● Rising ○ Falling ○ Rising and Falling
Rising	
Threshold	100 (0 - 2147483647, default 100)
Event	1 - Default Description
Falling	
Threshold	20 (0 - 2147483647, default 20)
Event	1 - Default Description

Edit Alarm

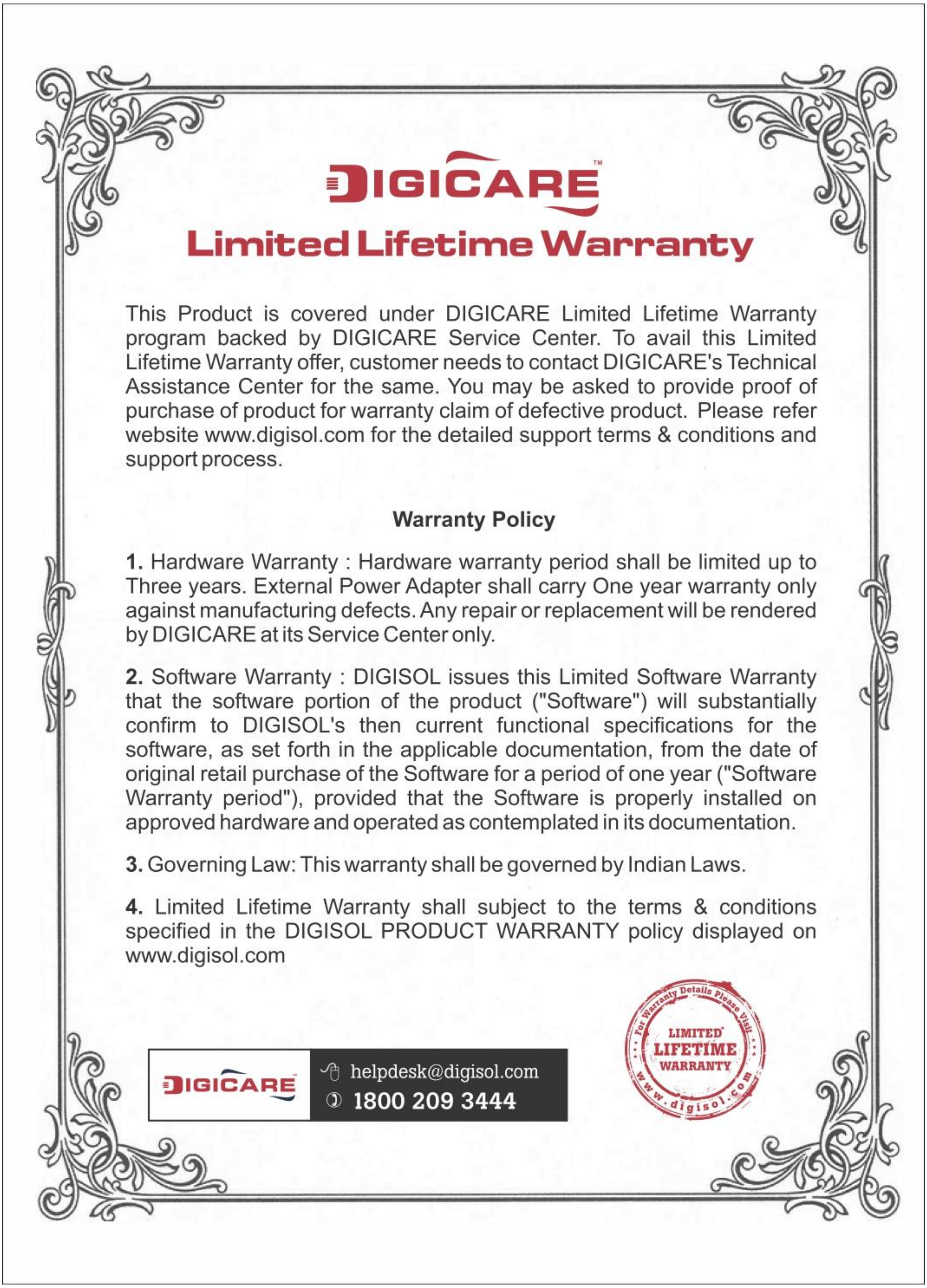
Entry	undefined
Port	GE1
Counter	Drop Events
Sampling	○ Absolute ● Delta
Interval	0 Sec (1 - 2147483647, default 100)
Owner	
Trigger	● Rising ○ Falling ○ Rising and Falling
Rising	
Threshold	0 (0 - 2147483647, default 100)
Event	1 - Default Description
Falling	
Threshold	0 (0 - 2147483647, default 20)
Event	1 - Default Description

Figure 224 - Management > RMON > Add/Edit Alarm

Item	Description
Port	Specify the port for sampling
Counter	Specify the counter for sampling ． ● Drop Event: Total number of events received in which the packets were dropped. ． ● Received Bytes (Octets): Octets. ● Received Packets: Number of packets. ● Broadcast Packets Received: Broadcast packets. ● Multicast Packets Received: Multicast packets. ● CRC and Align Error: CRC alignment error. ． ● Undersize Packets: Number of undersized packets.
	● Oversize Packets: Number of oversized packets. ● Fragments: Total number of packet fragment.

	● Jabbers: Total number of packet jabber. ・ ● Collisions: Collision. ・ ● Frames of 64 Bytes: Number of packets size 64 octets. ● Frames of 65 to 127 Bytes: Number of packets size 65 to 127 octets. ・ ● Frames of 128 to 255 Bytes: Number of packets size 128 to 255 octets. ・ ● Frames of 256 to 511 Bytes: Number of packets size 256 to 511 octets. ・ ● Frames of 512 to 1023 Bytes: Number of packets size 512 to 1023 octets. ・ ● Frames Greater than 1024 Bytes: Number of packets size 1024 to 1518 octets.
Sampling	Specify the sampling type. ・ ● Absolute: The selected variable value is compared directly with the thresholds at the end of the sampling interval. ・ ● Delta: The selected variable value of the last sample is subtracted from the current value and the difference is compared with the thresholds.
Interval	Specify the sampling interval.
Owner	Specify the owner for the sampling.
Trigger	Specify the type for the alarm trigger.
RISING	
Threshold	Specify the threshold for firing rising event.
Event	Specify the index of rising event when alarm was fired.

Falling	
Threshold	Specify the threshold for firing falling event.
Event	Specify the index of falling event when alarm was fired.



DIGICARE™

Limited Lifetime Warranty

This Product is covered under DIGICARE Limited Lifetime Warranty program backed by DIGICARE Service Center. To avail this Limited Lifetime Warranty offer, customer needs to contact DIGICARE's Technical Assistance Center for the same. You may be asked to provide proof of purchase of product for warranty claim of defective product. Please refer website www.digisol.com for the detailed support terms & conditions and support process.

Warranty Policy

1. Hardware Warranty : Hardware warranty period shall be limited up to Three years. External Power Adapter shall carry One year warranty only against manufacturing defects. Any repair or replacement will be rendered by DIGICARE at its Service Center only.

2. Software Warranty : DIGISOL issues this Limited Software Warranty that the software portion of the product ("Software") will substantially confirm to DIGISOL's then current functional specifications for the software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of one year ("Software Warranty period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation.

3. Governing Law: This warranty shall be governed by Indian Laws.

4. Limited Lifetime Warranty shall subject to the terms & conditions specified in the DIGISOL PRODUCT WARRANTY policy displayed on www.digisol.com

DIGICARE
helpdesk@digisol.com
1800 209 3444

For Warranty Details Please Visit
LIMITED LIFETIME WARRANTY
www.digisol.com