EstiNet L2/SDN Gigabit Managed Switch

USER MANUAL

EstiNet Technologies Inc

FCC Certifications

This Equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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

CE Mark Warning

This equipment complies with the requirements relating to the EMC Directive 2004/108/EC, the Low Voltage Directive 2006/95/EC, and the RoHS Directive 2011/65/EU.

Company has an on-going policy of upgrading its products and it may be possible that information in this document is not up-to-date. Please check with your local distributors for the latest information. No part of this document can be copied or reproduced in any form without written consent from the company.

Trademarks:
All trade names and trademarks are the properties of their respective companies.

EstiNet

Table of Contents

1 Introduction

1.1 General Description

The EstiNet RT188T/188P/166P/166PN are innovative switches which provide rich legacy L2 features and state-of-the-art SDN OpenFlow features. RT188T/188P are equipped with 24 gigabit RJ45 ports and 4 SFP uplink ports, support with 56Gbps forwarding capability. RT166P/166PN is equipped with 8 gigabit RJ45 ports and 2 SFP uplink ports support with 20Gbps forwarding capability. RT188P/166P/166PN are PoE switches, each RJ45 port provides 30W power. These switches are purposely designed for small to medium business customers who desire high performance, rich L2 protocols, advanced QoS, useful security features, powerful Access Control List function, power saving, easy management, and IPv6. In addition, RT188T/188P/166P/166PN provide innovative SDN functions, such as switch configuration auto-provisioning, dynamic flow-based monitoring, and abnormal traffic detection, which are new features that cannot be easily supported in legacy switches.

1.2 Key Features

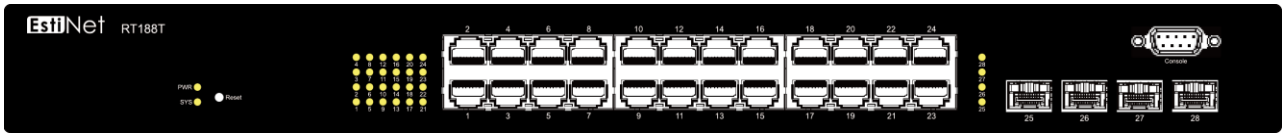
- Supports MDI/MDI-X auto crossover
- Complies with IEEE802.3, 802.3u, 802.3ab Ethernet standards
- Supports IEEE802.3x Flow Control and Back-Pressure control
- Supports Spanning Tree Protocol: STP, RSTP, MSTP, BPDU Guard
- Supports LLDP, LLDP-MED Discovery
- Supports VLAN : Port Based, MAC Based, Protocol Based, IP subnet Based, GVRP, Voice VLAN
- Supports Class of Service : 802.1p Based, DSCP Based
- Supports Security : Management Service (SSH, HTTP, HTTPS, SNMP), Protected Port, Storm Control, DoS attack prevention, Port Security, IEEE 802.1X
- Supports Storm Control (Broadcast, Unknown Multicast, Unknown Unicast)
- Supports port based Ingress/Egress rate limit
- Supports 8 queues; Strict Priority and WRR Priority
- Supports Jumbo Frame : 1518~10K Bytes
- Supports many Link Aggregation: Static, LACP types
- Support port mirroring, Cable Test
- Supports SNMP v1/v2/v3 & trap event
- Supports IGMP Snooping v2/v3
- Supports MLD Snooping v1/v2

- Supports Access Control List: MAC-based, IPv4-based, IPv6-based, management ACL
- Supports IEEE 802.3af/at (RT188P, RT166P, RT166PN)
- Supports OpenFlow v1.3

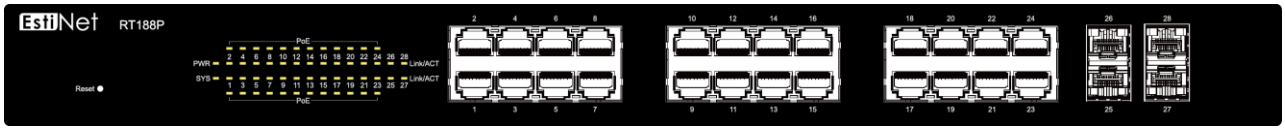
1.3 The Front Panel

The following figure shows the front panel of the switch.

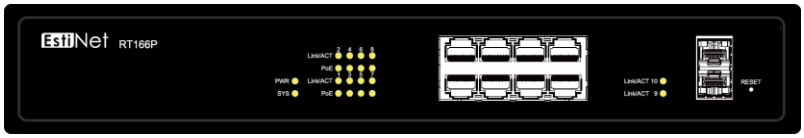
RT188T:



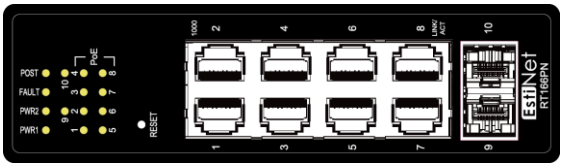
RT188P:



RT166P:



RT166PN:



1.3.1 LEDs Definition

This device provides extensive LEDs to show the activities on power, system and ports.

See the following description for RT188T/RT166P:

LED	Status	Operation
POWER	Steady Green	The switch is powered on.
	Off	The switch is powered off.
SYSTEM	Steady Green	The switch is on and functioning properly
	Blinking Green	The switch is rebooting and performing self-diagnostic tests.

	Off	The power is off or the system is not ready/malfunctioning.
Link/ACT	Steady Green	Valid port connection.
	Blinking Green	Valid port connection and there is data transmitting/receiving
	Off	Port disconnected.
PoE (for PoE switch only)	Steady Green	PoE port connection when connect to PD device.
	Off	PoE port disconnected.

See the following description for RT166PN:

LED	Status	Operation
PWR1	Steady Green	External power connect to the PWR1 slot.
PWR2	Steady Green	External power connect to the PWR2 slot.
FAULT	Steady Red	The switch is on and functioning abnormally
POST	Steady Green	The switch is on and functioning properly
	Blinking Green	The switch is rebooting and performing self-diagnostic tests.
Link/ACT	Steady Green	Valid port connection.
	Blinking Green	Valid port connection and there is data transmitting/receiving
	Off	Port disconnected.
PoE	Steady Green	PoE port connection when connect to PD device.
	Off	PoE port disconnected.

1.3.2 The Reset Button

Reset the switch to its factory default configuration via the RESET button. Press

the RESET button for two seconds more and release. The switch automatically reboots and reloads its factory configuration file. The RESET button is on the front panel of the switch.

1.4 The Rear Panel

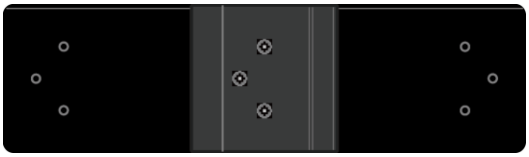
The following figure shows the rear panel of the switch:

RT188T:

RT188P:

RT166P:

RT166PN:



1.4.1 Power Receptacle

To be compatible with the electric service standards around the world, the switch is designed to afford the power supply in the range from 100 to 240 VAC, 50/60 Hz. Please make sure that your outlet standard to be within this range.

To power on the switch, please plug the female end of the power cord firmly into the receptacle of the switch, the other end into an electric service outlet.

After the switch powered on, please check if the power LED is lit for a normal power status.

1.5 Installation

1.5.1 Unpacking Information

The product package should include the following:

- One RT188T/RT188P/RT166P/RT166PN Gigabit Ethernet SDN Managed Switch
- One power cord
- Rubber foot and screws
- Rack-mount brackets
- One CD-ROM for user manual

1.5.2 Rack-mount Installation

Rack Mounting the Switch in the 19-inch rack:

- Disconnect all cables from the switch before continuing.
- Place the unit the right way up on a hard, flat surface with the front facing toward you.
- Locate a mounting bracket over the mounting holes on one side of the unit.
- Insert the screws and fully tighten with a suitable screwdriver.
- Repeat the two previous steps for the other side of the unit.
- Insert the unit into the 19" rack and secure with suitable screws (not provided).
- Reconnect all cables.

1.5.3 Installing Network Cables

To make a valid connection and obtain the optimal performance, an appropriate cable that corresponds to different transmitting/receiving speed is required. To choose a suitable cable, please refer to the following table.

Media	Speed	Wiring
Network Media(Cable)	10 Mbps	10Base-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
	100 Mbps	100Base-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)
	1000 Mbps	1000Base-T: UTP category 5e, 6 cable (maximum 100m) EIA/TIA-568 100Ω STP (maximum 100m)

1.6 安全预防措施

警告：

- 机架或机柜应妥善固定好，以防止不稳、倾斜或倾倒。安装在机架或机柜中的装置应尽可能安装在低处，最重的装置安装在下方，越轻的装置安装在越上方。

注意：

- 请确保电源电路正确接地，然后使用交换器随附的电源线连接到 AC 电源。
- 如果安装需要使用的电源线与交换器和/或电源供应器随附的电源线不同时，请确定该电源线的尺寸符合交换器的电流需求。此外，请确保使用的电源线有显示定义所在国家/地区电源线法律规定的安全机构的标记。这个标记可确保电源线能安全用于交换器和电源供应器。
- 安装交换器时，AC 插座应靠近交换器，并且在必须关闭交换器的电源时，可以容易地找到插座。
- 确保交换器不会导致电路、电线过度负载以及过电流保护。若要判断供电电路是否可能过度负载，请将与交换器安装在相同电路上的所有装置的额定安培值全部加总，然后与电路的额定总值限制比较。最大额定安培值通常会印在装置上靠近 AC 电源连接器的位置。
- 请勿将交换器安装在作业环境温度可能超过规格的环境中。
- 请确保交换器周围的空气流通不受阻碍。请预留至少 7.6 公分 (3 吋) 空间以供冷却之用。

2 Getting Started

EstiNet managed switch software provides layer 2 and SDN functionalities for enterprise networks. This guide describes how to use Web-based management interface (Web UI) to configure EstiNet managed switch software features.

The Web UI supports all frequently used web browsers listed below:

- Microsoft Internet Explorer 8 (and later versions)
- Mozilla Firefox 3.5 and (and later versions)
- Google Chrome 9.0 and (and later versions)

The Switch default URL address for Management Web UI is http://192.168.1.1. The default username is "switch" and the default password is "admin".

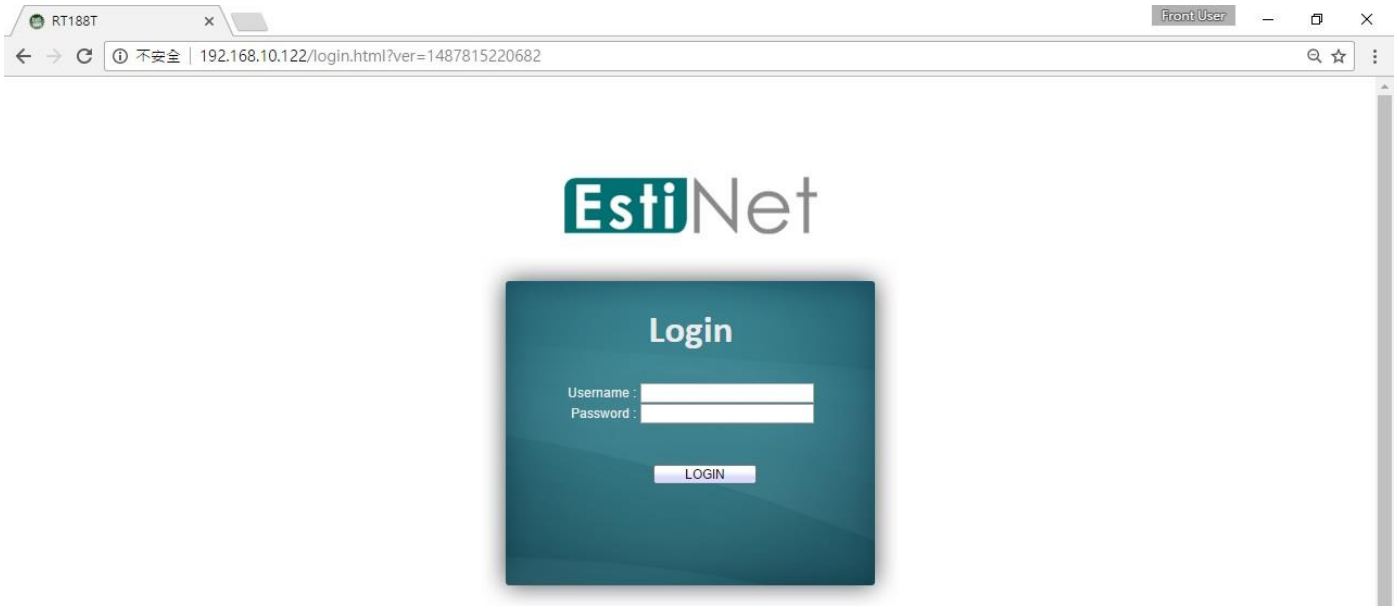


Figure 2-1 Web Login page

On the top of Web UI page, the left column shows the switch configuration menu. The switch panel shows the switch's current link status. Green squares indicate the port link is up, while black squares indicate the port link is down. Below the switch panel is the System Information table that shows basic system information of the switch.

Note: At first time setup user need to re-configure the IP address and subnet mask of the PC, in order to let PC can access to the switch.

Here is the detail procedures to re-configure the IP address, subnet mask of the PC.

a. Press "Start" > "Control Panel"; choose to view Network Connections
b. Choose "Local Area Connection", click right button then choose the "Properties"
c. Choose "Networking" tab, choose the "Internet Protocol Version 4(TCP/IPv4)", and then click "Properties". Please need to remember the original IP setting.
d. Press "General" for manually setup the IP address.
e. For the IP address field please input the IP address which is the same subnet as the switch; for example:192.168.1.2
f. Please input 255.255.255.0 to the subnet mask, then press OK.

Initiate the PC WEB browser then input the default URL http://192.168.1.1 for accessing the switch to do the configuration. Once the switch finished the configuration it can get the assigned IP address through the DHCP server. After the successful switch setting administrator need to roll back the original IP address for

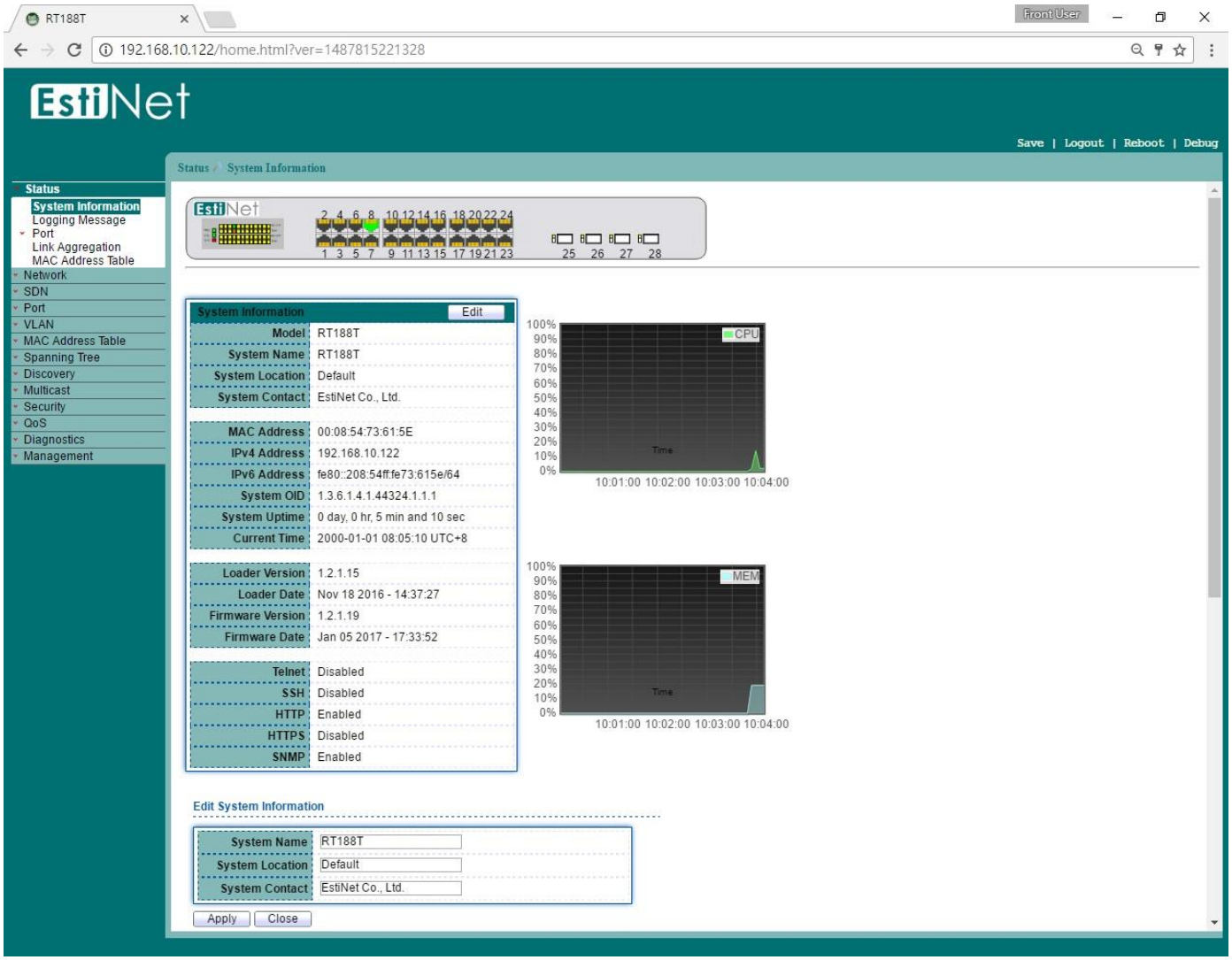


Figure 2-2 Web User Interface

3 Status

Use the Status pages to view system information and status.

3.1 System Information

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

Use this page to configure System related information and browse some system information such as MAC address, IP address, firmware version, loader version …… etc.

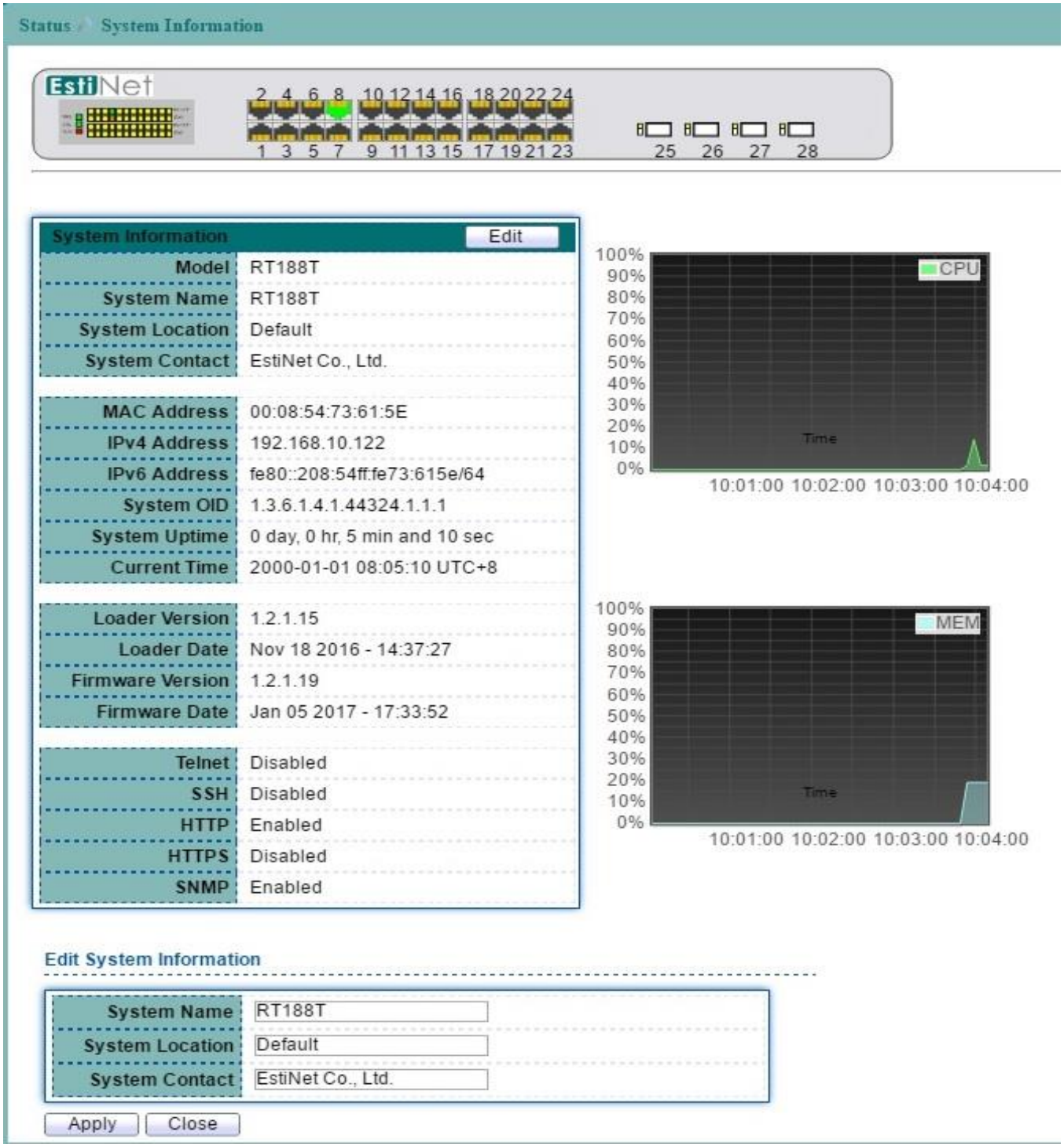


Figure 3-1 System Information page

With "Edit" button in the table，user could configure the field value.

Field	Description
System Name	System name of the switch.
System Location	System location of the switch.
System Contact	System contact of the switch

Table 3-1 System Information fields

3.2 Logging Message

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

Figure 3-2 Logging Message page

Field	Description
Viewing	View the logging information stored on switch memory. ● RAM: Show the logging messages stored on the RAM. ● Flash: Show the logging messages stored on the Flash.
Showing entries	How many entries will be showed on a single page: Possible value: ALL, 10, 30, 50, 100.

Table 3-2 Logging Message fields

3.3 Port

The Port configuration page displays port summary and status information.

3.3.1 Port Statistics

To display Port Counters web page, click **Status** > **Port** > **Statistics.**

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

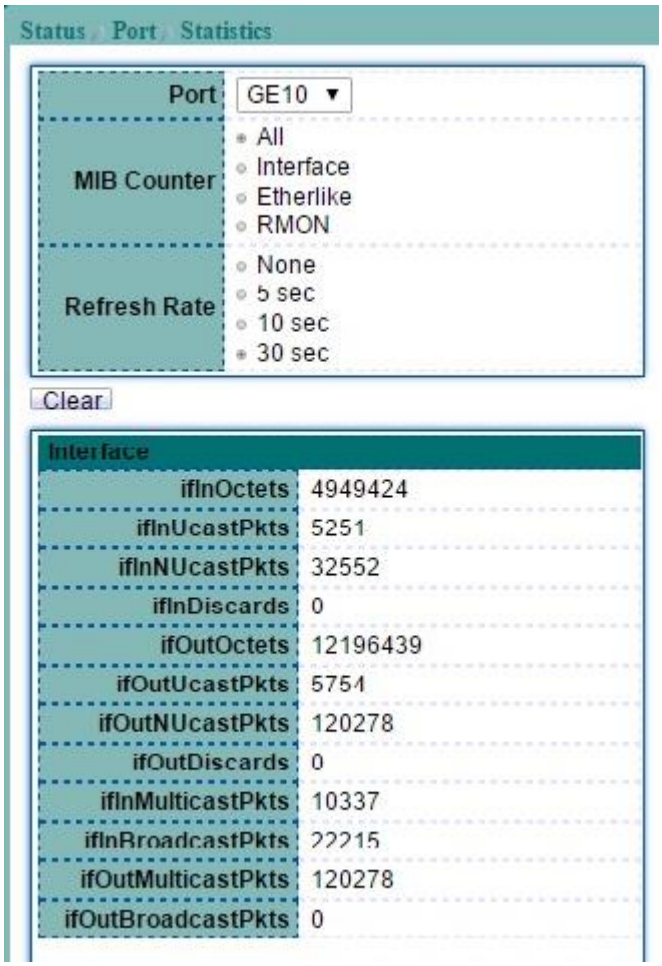


Figure 3-3 Port Statistics page

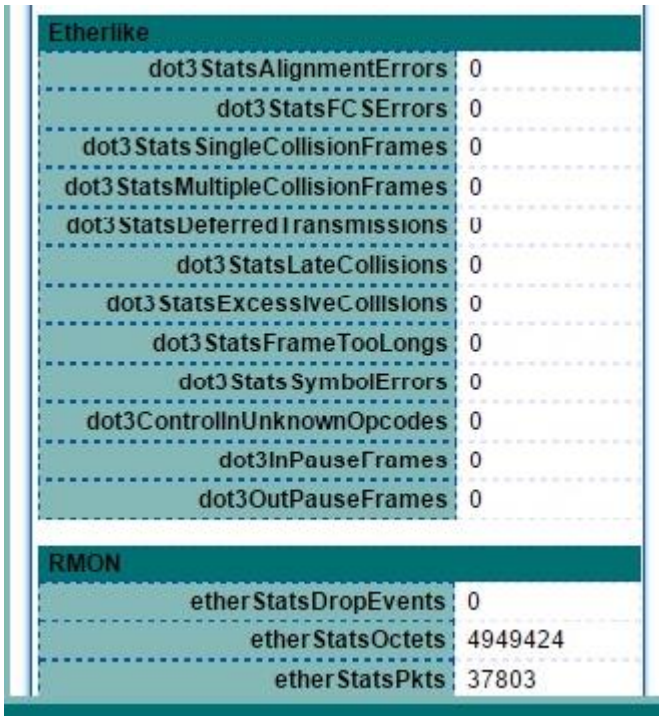


Figure 3-4 Port Statistics page

Field	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 counters. ● Etherlike: Ethernet-like related counters. ● RMON: RMON related counters.
Refresh Rate	Select refresh rate of the counter table.

Table 3-3 Port Statistics fields

3.3.2 Port Error Disabled

To display the status of port error disabled, click **Status** > **Port**> **Error Disabled.**

Figure 3-5 Port Error Disabled page

Field	Description
Port	Interface or port number.
Reason	Port will be disabled by one of the following error reason: BPDU Guard UDLD 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.

Table 3-4 Port Error Disabled fields

3.3.3 Bandwidth Utilization

To display the status of port transmit and receive rate, click **Status** > **Port**> **Bandwidth Utilization**.

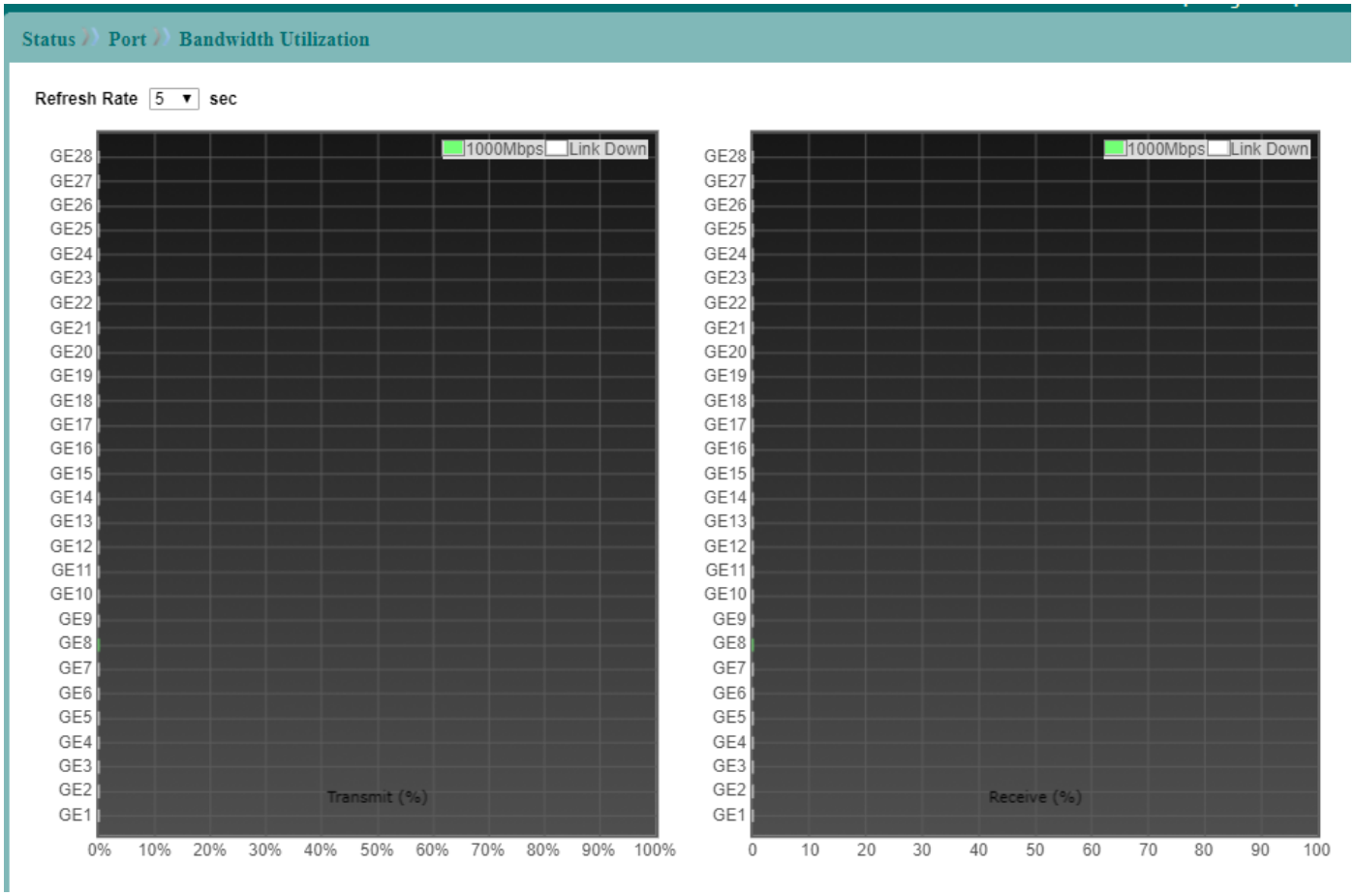


Figure 3-6 Port Bandwidth Utilization page

3.4 PoE Status

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

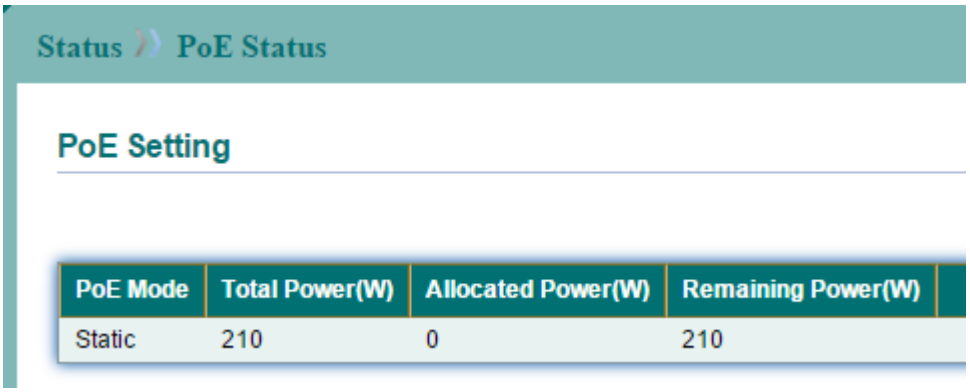


Figure 3-7 PoE Status page

Field	Description
PoE Mode	The mode of the PoE: ● Static: static mode with user configured power. ● Dynamic: automatically allocated power base on the link-up sequence of PD device.
Total Power(W)	The total power budget.
Allocated Power(W)	The used power.
Remaining Power(W)	The remaining power.

Table 3-5 PoE Status fields

3.5 Link Aggregation

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

Figure 3-8 Link Aggregation Table page

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

Table 3-6 Link Aggregation Table fields

3.6 MAC Address Table

To display MAC Address Table, click **Status** > **MAC Address Table.**

Figure 3-9 MAC Address Table page

Field	Description
Showing Entries	Select the number of entries that you would like to show on a single page.
VLAN	VLAN ID.
MAC Address	MAC address.
Type	The type of the entry: ● Management: The MAC address is used by switch. ● Dynamic: The MAC address learnt dynamically. ● Static: The MAC address is user configured.
Port	Port Number.

Table 3-7 MAC Address Table fields

4 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.

4.1 IP Address

To configure the switch IP address and DNS configuration, click **Network** > **IP Address**.

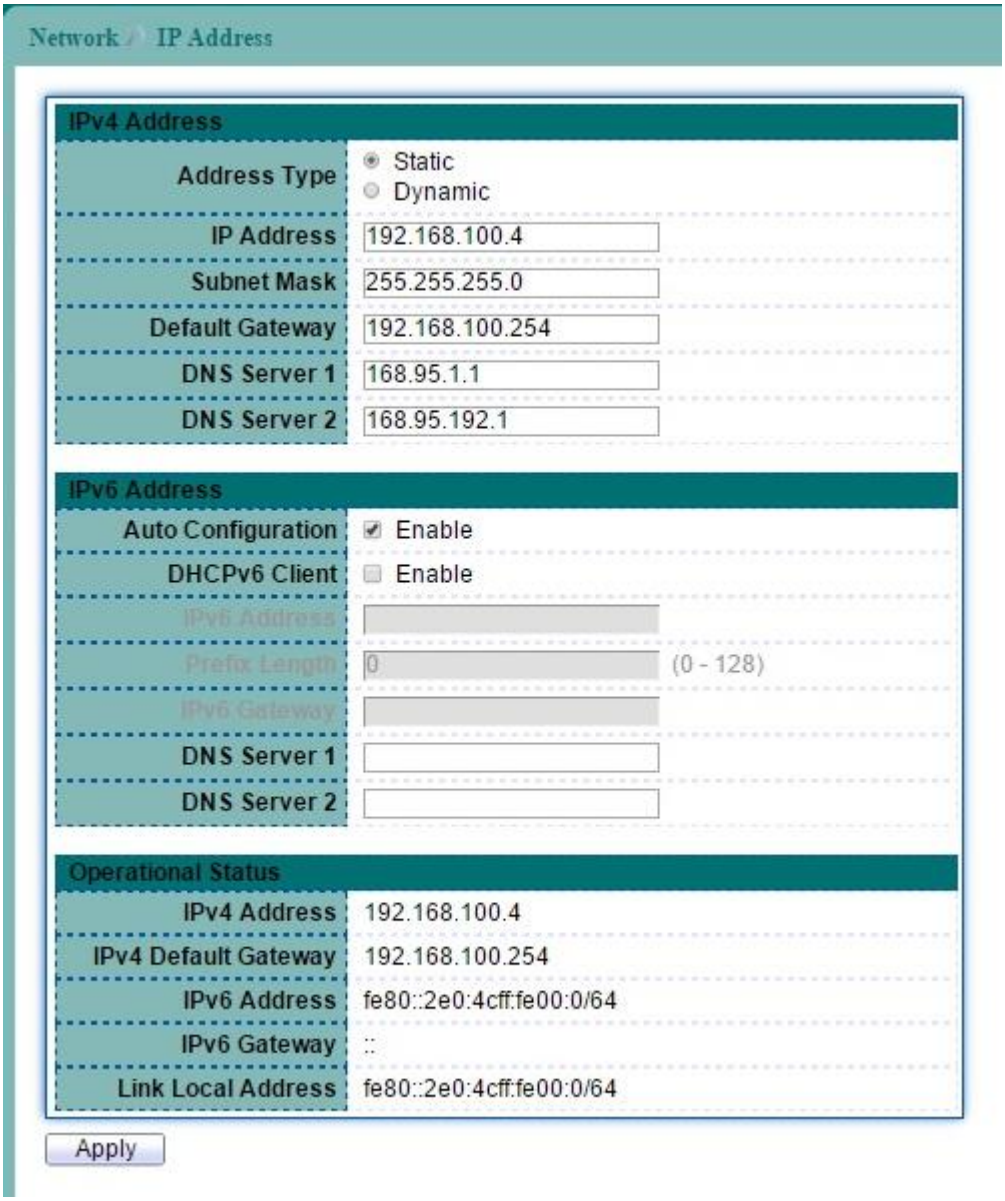


Figure 4-1 IP Address page

Field	Description
IPv4 Address	
Address Type	Type of switch IP configuration ● Static: Static IP configured by users will be used. ● DHCP: 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.
DNS Server 1	Specify the primary DNS server on the static configuration.
DNS Server 2	Specify the secondary DNS server on the static configuration.
IPv6 Address	
Auto Configuration	Enable/Disable the IPv6 auto configuration.
DHCPv6 Client	Enable/Disable the DHCPv6 client.
IPv6 Address	Specify the IPv6 address, when the IPv6 auto configuration is disabled.
Prefix Length	Specify the IPv6 prefix length.
IPv6 Gateway	Specify the IPv6 default gateway, when the IPv6 auto configuration is disabled.
DNS Server 1	Specify the primary DNS server on the static configuration.
DNS Server 2	Specify the secondary DNS server on the static configuration.

Table 4-1 IP Address fields

4.2 System Time

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

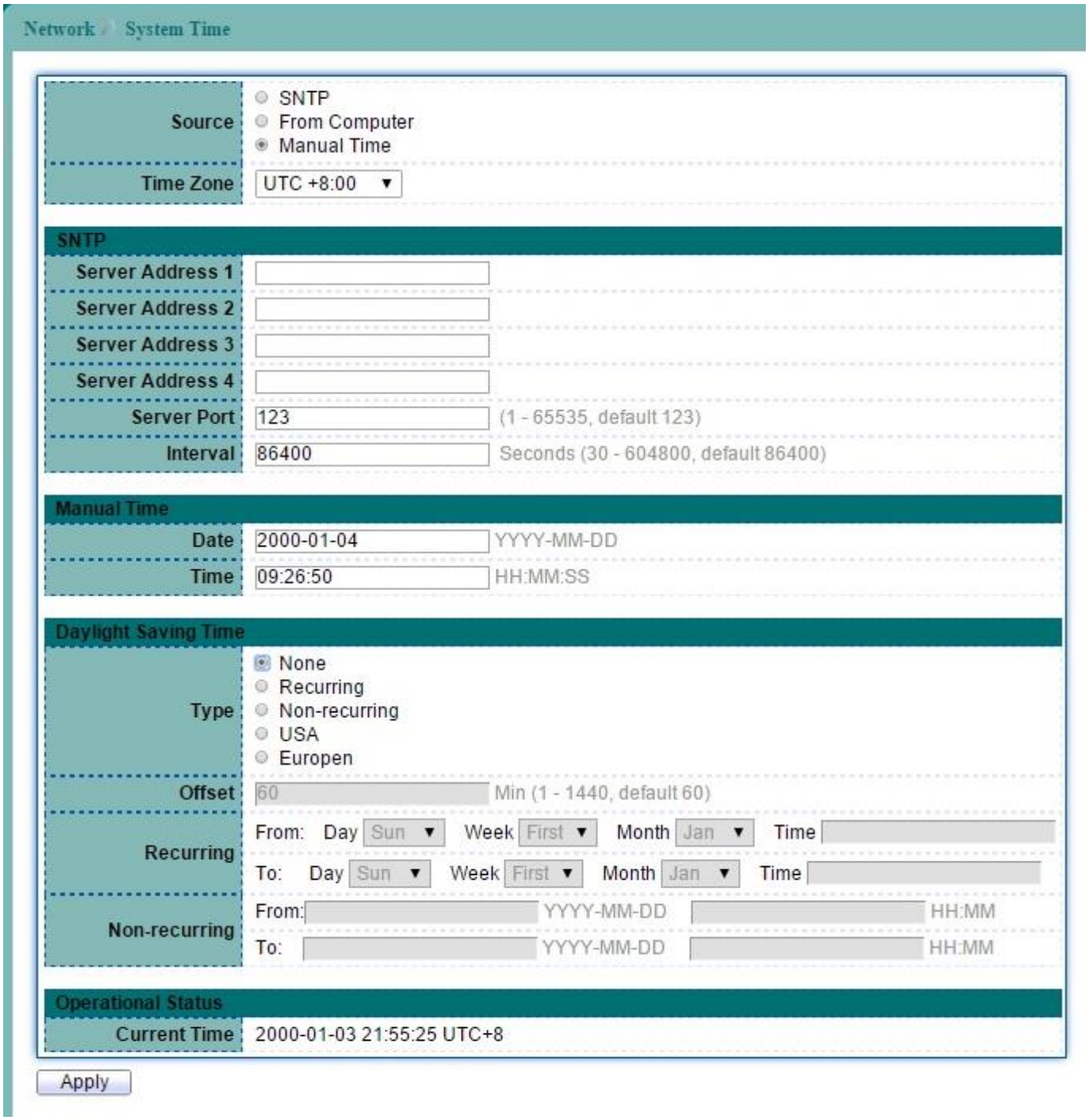


Figure 4-2 System Time page

Field	Description
Source	Select the Source of the system time. • **SNTP:** Select the radio button to enable or disable using SNTP server. • **From Computer:** Switch will synchronize its system time

	with connected management PC. • **Manual Time:** Specify static time. Static time take effect if SNTP is disabled.
Time Zone	Select a time zone from listing countries.
SNTP	
Server Address	Enter SNTP Server address.
Server Port	Enter SNTP Server Port.
Interval	Interval time.
Manual Time	
Date	Set the date (Year-Month-Day).
Time	Set the time (Hour - Minute - Second).
Daylight Saving Time	
Type	• **None:** Disable daylight saving time. • **Recurring:** Using recurring mode of daylight saving time. • **Non-Recurring:** Using non-recurring mode of daylight. • **USA:** Using daylight saving time in the United States that starts on the second Sunday of March and ends on the first Sunday of November. • **European:** Using daylight saving time in the Europe that starts on the last Sunday in March and ending on the last.
Offset	Offset of the daylight saving.
Recurring	Specify the starting and ending time of recurring daylight saving time. This field available when selecting "Recurring" mode.
Non-Recurring	Specify the starting and ending time of non-recurring daylight saving time. This field available when selecting "Non-Recurring" mode.

Table 4-2 System Time fields

5 SDN

Use the SDN pages to configure switch SDN function. When SDN enabled, a controller can control switches via uplink port or downlink ports to forward OpenFlow control frames to down-level switches.

5.1 SDN Setting

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

This page allow user to configure SDN setting on the switch.

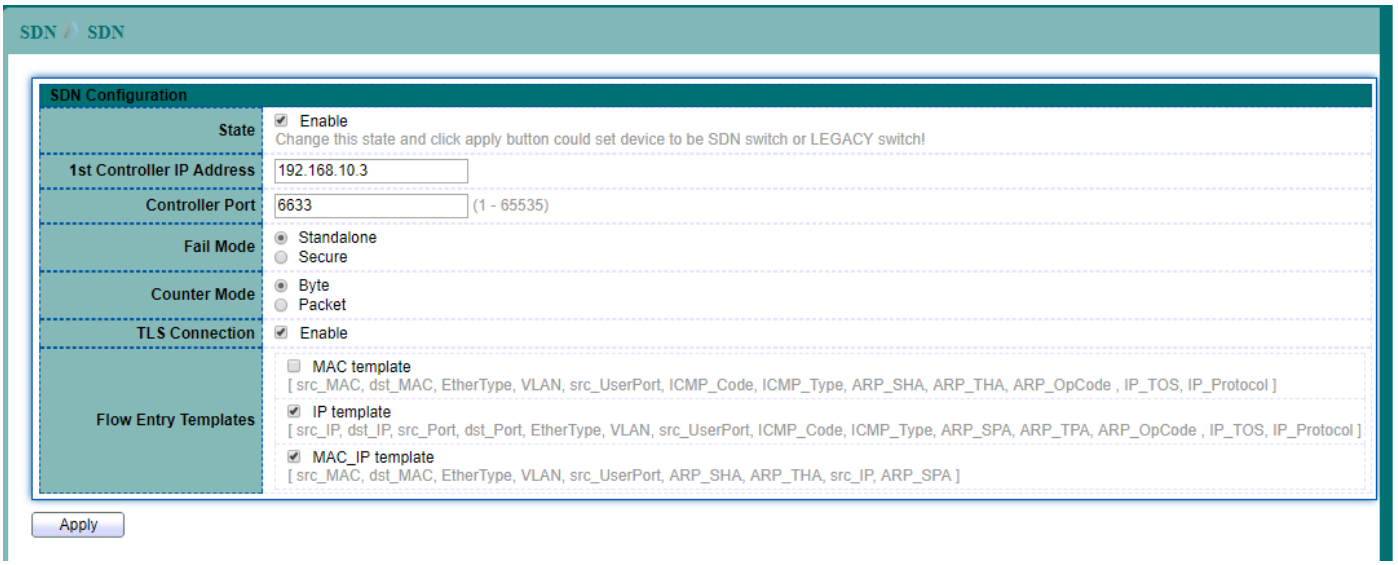


Figure 5-1 SDN page

Field	Description
State	To enable or disable Switch SDN state.
1st Controller IP Address	Enter the first Controller IP Address.
Controller Port	Controller IP Port to use for the OpenFlow management connection (1-65535).
Fail Mode	Select a Fail Mode to use when the switch loss of connectivity with the controller. • **Standalone:** The switch will reverts to using normal processing (Ethernet Switching). • **Secure:** The switch will continues operation in OpenFlow mode, until it reconnects to the server.
Counter Mode	Select a counter mode to use when bind a meter in a flow entry.
TLS Connection	To enable or disable TLS encryption for the connection with controller.
Flow Entry Templates	When creating SDN flow entries, all of its match fields must be within a template fields set. Our system provides 3 kinds of templates for SDN flow entries. Users must choose 2 templates for SDN flow entry from 3 templates (**MAC template, IP template, MAC_IP template**)

Table 5-1 SDN fields

Notice: Hybrid mode and OpenFlow Management VLAN shall be able to be configured when switch is configured as In-band mode.

6 Port

Use the Port pages to configure settings for the switch ports, trunk, layer 2 protocols and other switch features.

6.1 Port Setting

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

This page allow user to configure switch port settings and show port current status. Check the left box to select the ports then click "Edit" button to configure port setting.

Entry	Port	Type	Description	State	Link Status	Speed	Duplex	Flow Control
1	GE1	1000M Copper		Enabled	Down	Auto	Auto	Disabled
2	GE2	1000M Copper		Enabled	Down	Auto	Auto	Disabled
3	GE3	1000M Copper		Enabled	Down	Auto	Auto	Disabled
4	GE4	1000M Copper		Enabled	Down	Auto	Auto	Disabled
5	GE5	1000M Copper		Enabled	Down	Auto	Auto	Disabled
6	GE6	1000M Copper		Enabled	Down	Auto	Auto	Disabled
7	GE7	1000M Copper		Enabled	Down	Auto	Auto	Disabled
8	GE8	1000M Copper		Enabled	Down	Auto	Auto	Disabled
9	GE9	1000M Copper		Enabled	Down	Auto	Auto	Disabled
10	GE10	1000M Copper		Enabled	Up	Auto (100M)	Auto (Full)	Disabled (Disabled)
11	GE11	1000M Copper		Enabled	Down	Auto	Auto	Disabled
12	GE12	1000M Copper		Enabled	Down	Auto	Auto	Disabled
13	GE13	1000M Copper		Enabled	Down	Auto	Auto	Disabled
14	GE14	1000M Copper		Enabled	Down	Auto	Auto	Disabled
15	GE15	1000M Copper		Enabled	Down	Auto	Auto	Disabled
16	GE16	1000M Copper		Enabled	Down	Auto	Auto	Disabled
17	GE17	1000M Copper		Enabled	Down	Auto	Auto	Disabled
18	GE18	1000M Copper		Enabled	Down	Auto	Auto	Disabled
19	GE19	1000M Copper		Enabled	Down	Auto	Auto	Disabled
20	GE20	1000M Copper		Enabled	Down	10M	Auto	Disabled
21	GE21	1000M Copper		Enabled	Down	Auto	Auto	Disabled
22	GE22	1000M Copper		Enabled	Down	Auto	Auto	Disabled
23	GE23	1000M Copper		Enabled	Down	Auto	Auto	Disabled
24	GE24	1000M Copper		Enabled	Down	Auto	Auto	Disabled
25	GE25	1000M Fiber		Enabled	Down	Auto	Full	Disabled
26	GE26	1000M Fiber		Enabled	Down	Auto	Full	Disabled
27	GE27	1000M Fiber		Enabled	Down	Auto	Full	Disabled
28	GE28	1000M Fiber		Enabled	Down	1000M	Full	Disabled

Figure 6-1 Port Setting page

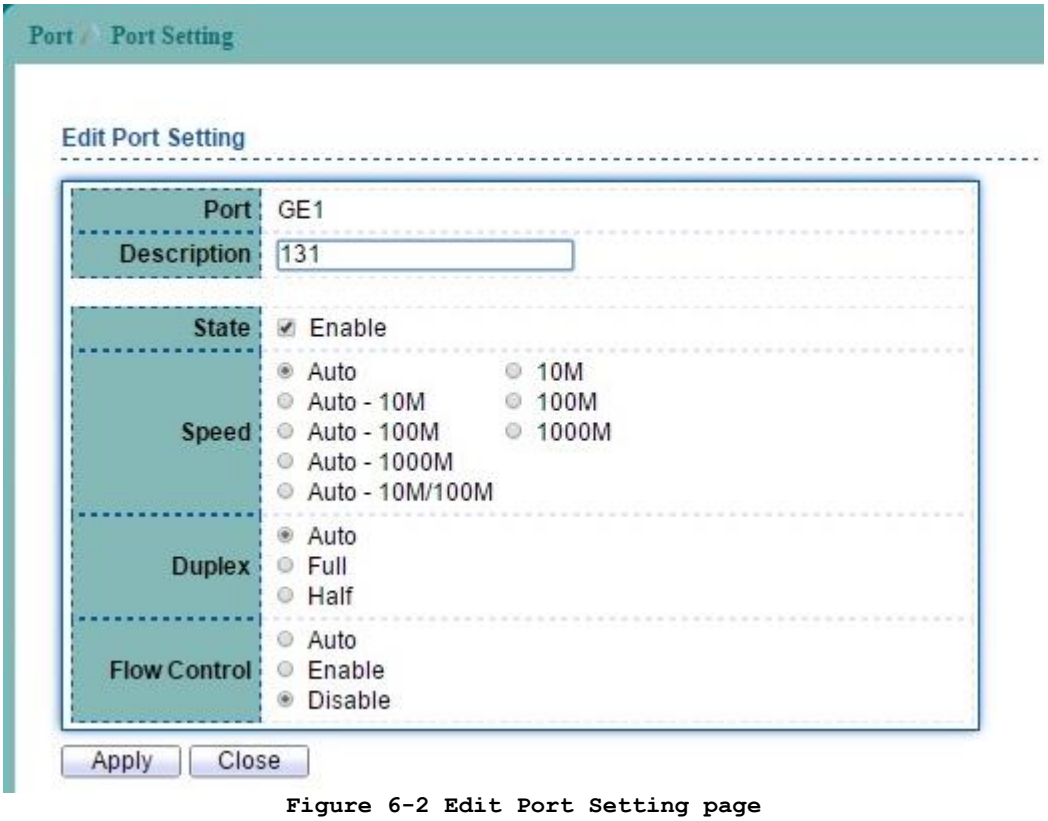


Figure 6-2 Edit Port Setting page

Field	Description
Port	Selected port number(s).
Description	Port description.
State	Port admin state. • **Enabled:** Enable 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. • **Enabled:** Enable flow control ability. • **Disabled:** Disable flow control ability.

Table 6-1 Port Setting fields

6.2 Error Disabled

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

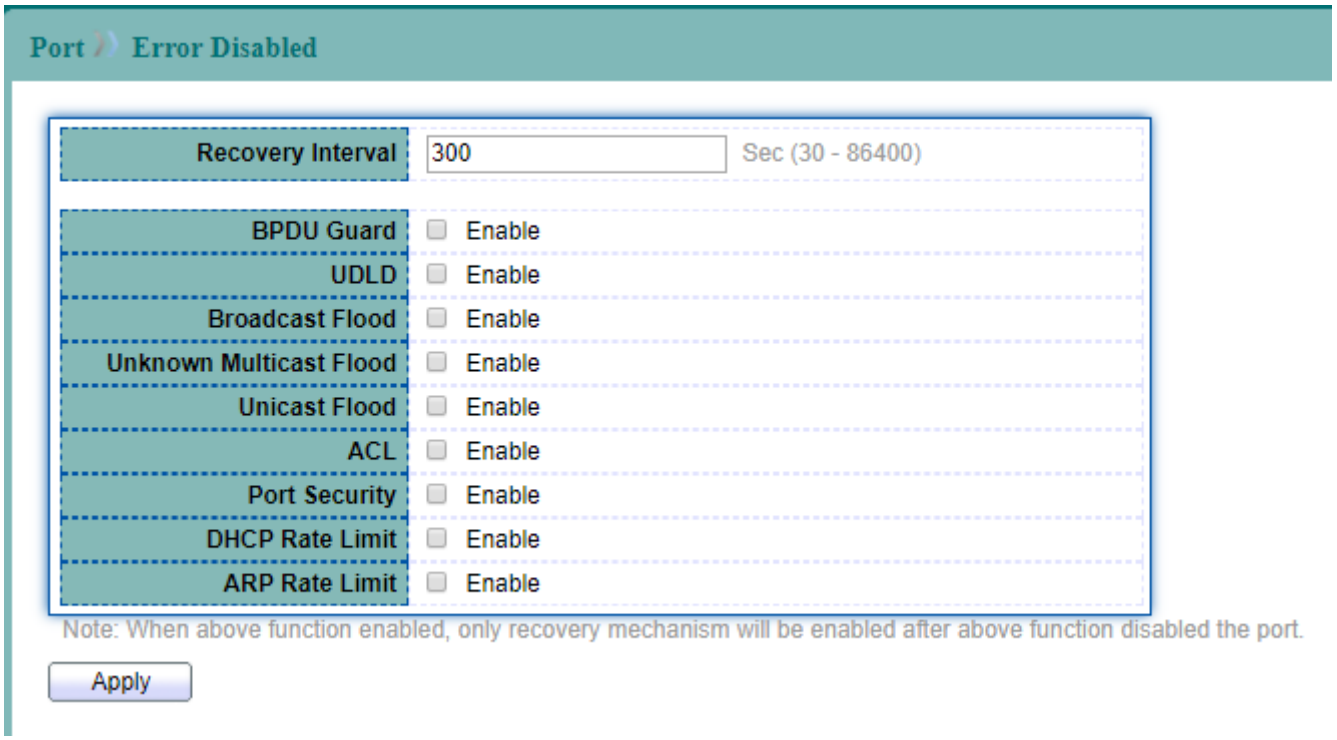


Figure 6-3 Error Disabled page

Field	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 (UniDirectional Link Detection) 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 Violation	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.

Table 6-2 Error Disabled fields

6.3 Link Aggregation

6.3.1 LAG Group

To display LAG Group Setup page, click **Port** > **Link Aggregation** > **Group**.

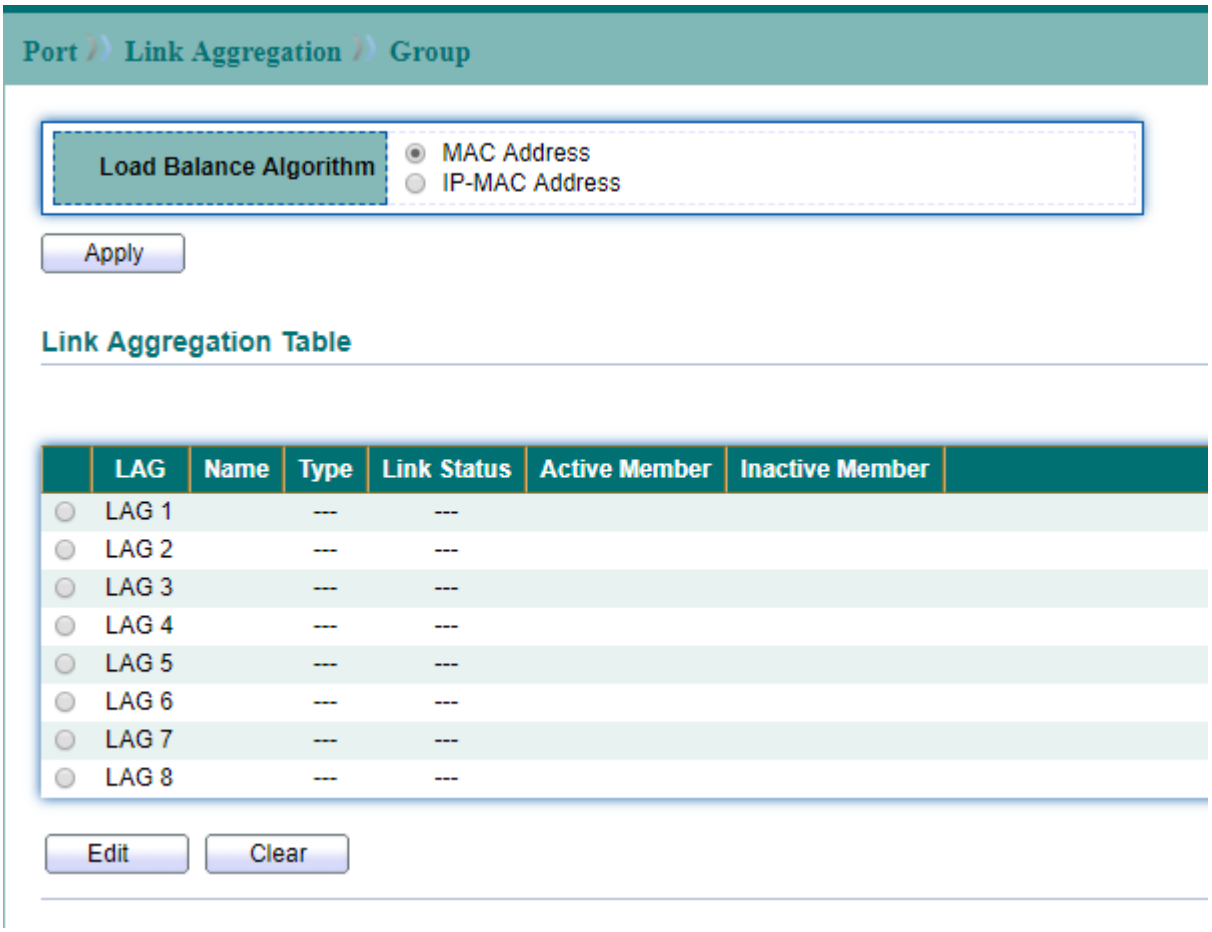


Figure 6-4 LAG Group page

Field	Description
Load Balance Algorithm	Select the LAG load balance distribution algorithm. • **MAC Address:** Based on source and destination MAC address for all packets • **IP/MAC Address:** Based on source and destination IP addresses for IP packet, and source and destination MAC address for non-IP packets.

Table 6-3 LAG Group fields

Select the LAG and click "Edit" button to configure LAG setting.

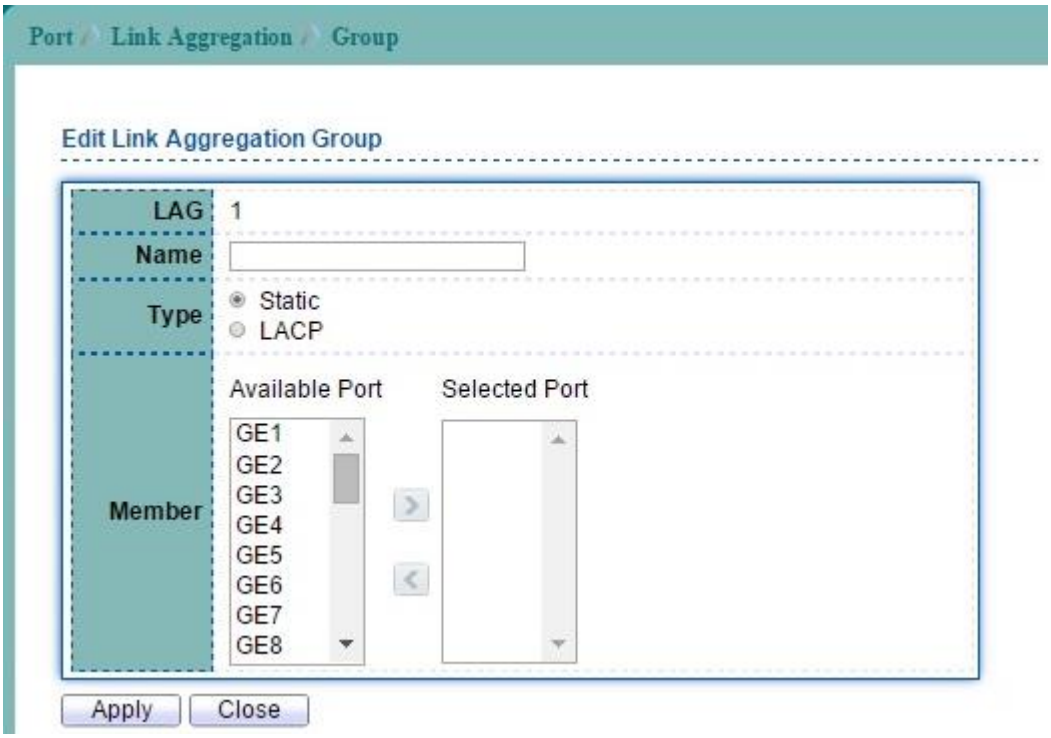


Figure 6-5 Edit LAG Group page

Field	Description
LAG	Selected LAG Group.
Name	LAG port description
Type	Select 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 the trunk member ports in this field. There are the following limitations for choosing the member ports: ● All ports in a LAG must be of the same media type. ● To add a port to the LAG, it cannot belong to any VLAN except the default VLAN. ● Ports in a LAG must not be assigned to another LAG. ● Ports in a LAG must not be a mirroring port. ● Ports in a LAG must not be a 802.1x enabled port. ● No more than eight ports are assigned to a LAG. ● When a port is added to a LAG, the configuration of the LAG is applied to the port. ● When the port is removed from the LAG, its original configuration is reapplied. ● There could be at most 8 member ports in a trunk.

Table 6-4 Edit LAG Group fields

6.3.2 LAG Port Setting

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

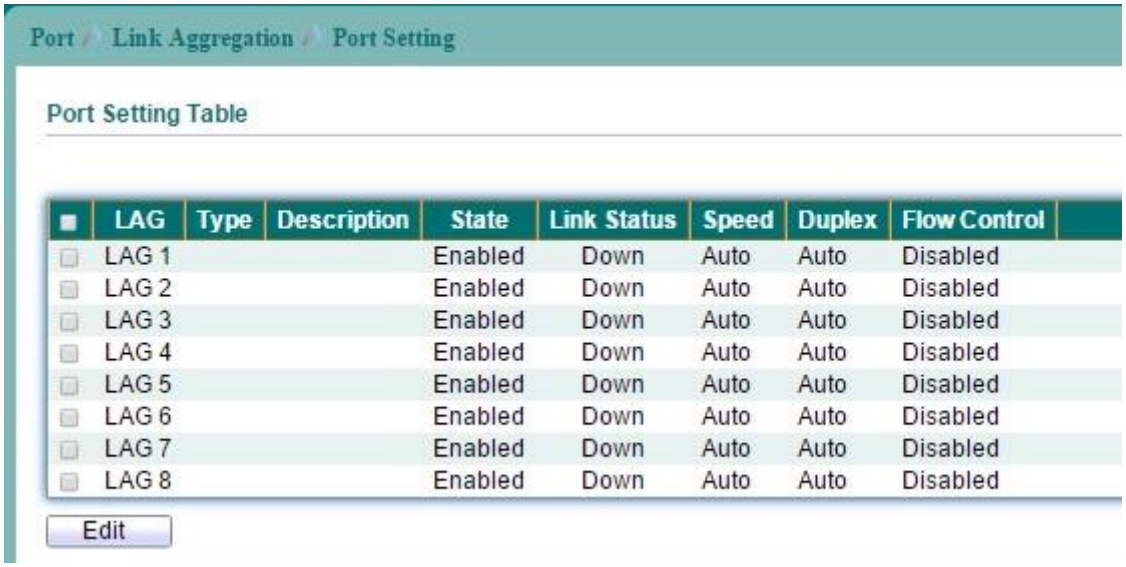


Figure 6-6 LAG Port Setting page

Field	Description
LAG	LAG Name.
Type	Member port media type.
Description	LAG port description.
Enable	LAG port admin state.
Status	LAG port link status.
Speed	Current LAG port speed.
Duplex	Current LAG port duplex.
Flow Control	Current LAG port flow control state

Table 6-5 LAG Port Setting fields

Select a LAG group then click "Edit" button to configure LAG port setting.

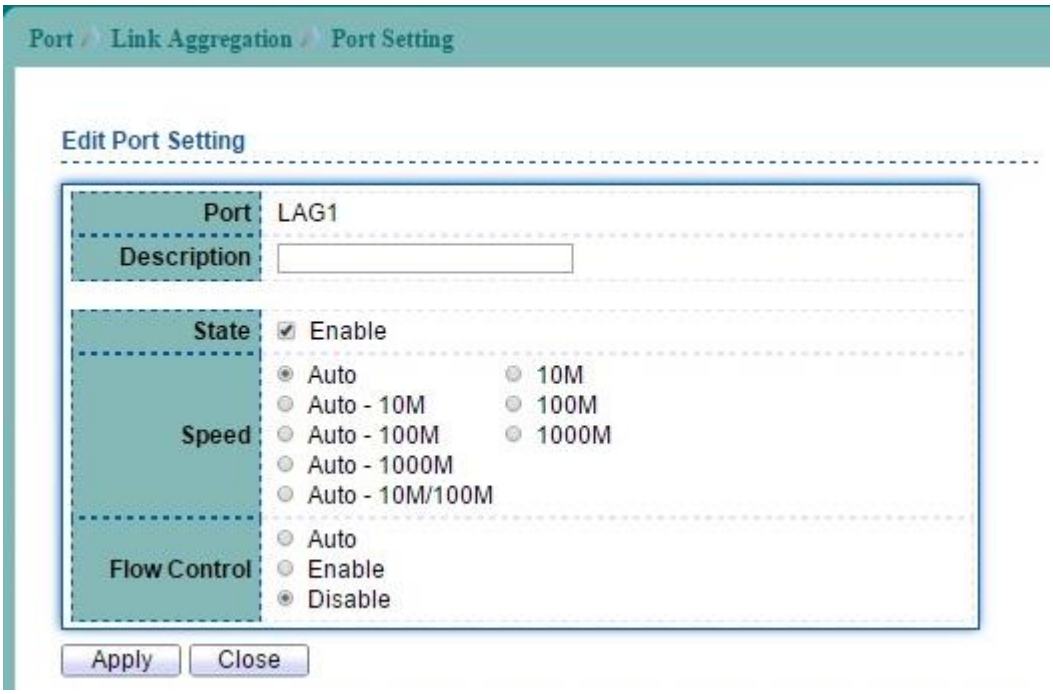


Figure 6-7 Edit LAG Port Setting page

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

Table 6-6 Edit LAG Port Setting fields

6.3.3 LACP Setting

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

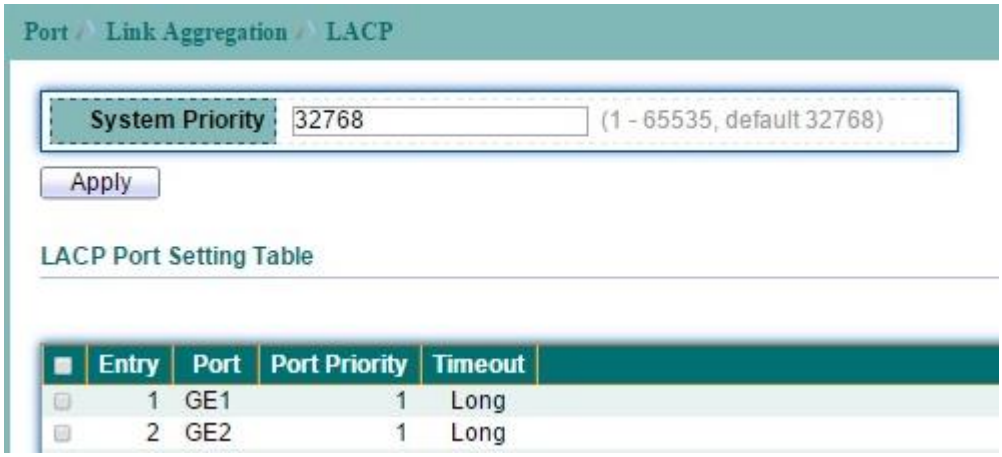


Figure 6-8 LACP page

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

Table 6-7 LACP fields

Select LACP port and click "Edit" button to configure LACP Port Setting.

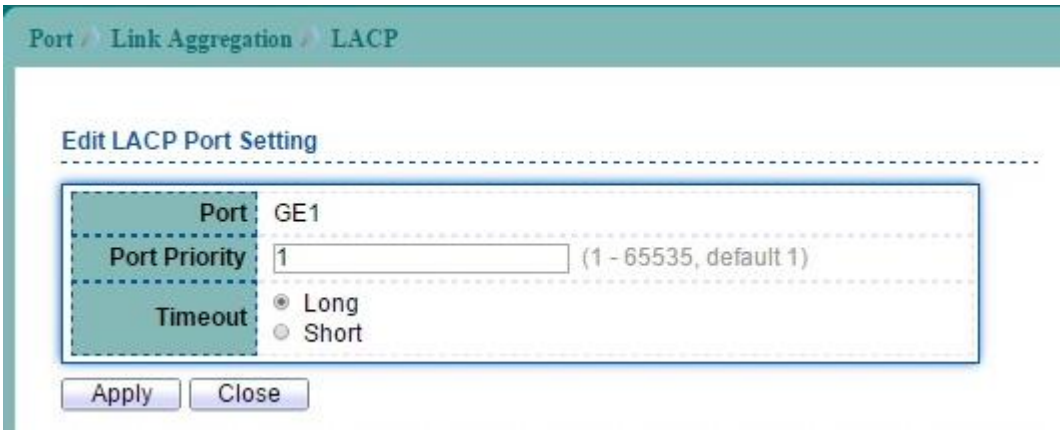


Figure 6-9 Edit LACP page

Field	Description
Port Select	Select one or multiple ports to configure
Priority	Enter the LACP priority value of the port
Timeout	Select the periodic transmissions type of LACP PDUs. ● **Long:** Transmit LACP PDU with slow periodic (30s). ● **Short:** Transmit LACPP DU with fast periodic (1s).

Table 6-8 Edit LACP fields

6.4 EEE

To configure and display the status of switch green feature, click **Port** > **EEE**.

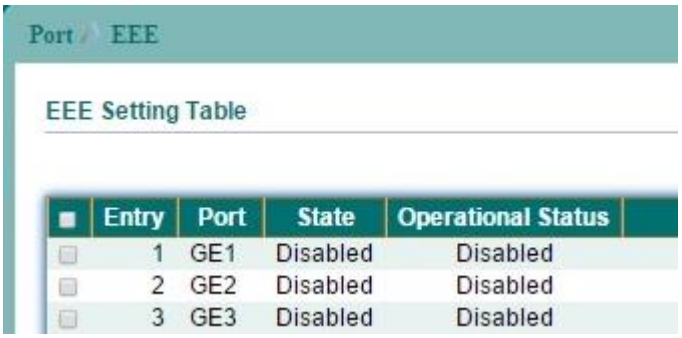


Figure 6-10 EEE page

Select Entry number and click "Edit" button to configure EEE Setting.

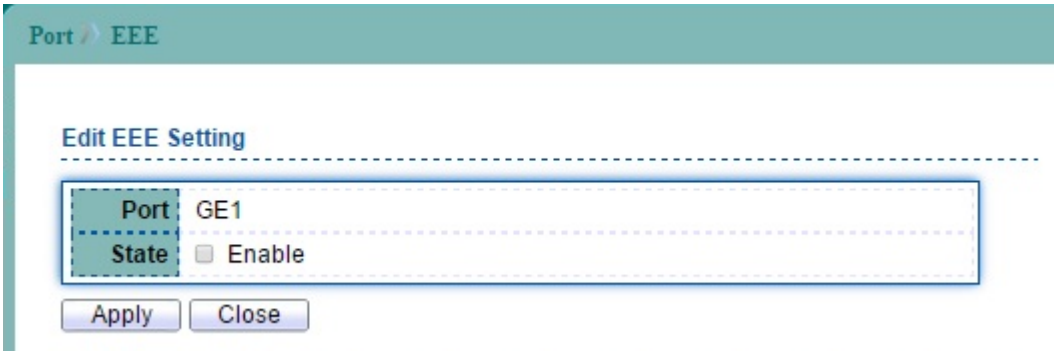


Figure 6-11 Edit EEE page

Field	Description
Port	Selected EEE Port.
State	Specify the EEE status.

Table 6-9 EEE fields

6.5 Jumbo Frame

To modify the jumbo frame configuration, click **Port** > **Jumbo Frame.**

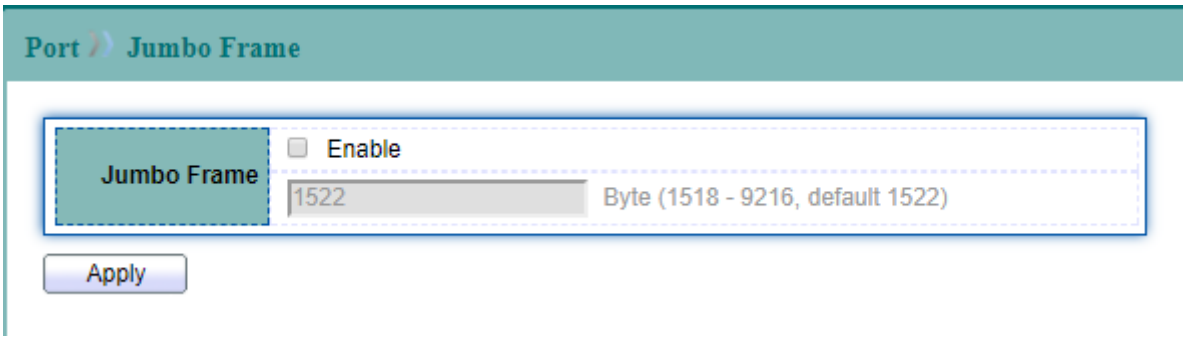


Figure 6-12 Jumbo Frame page

Field	Description
Enable	Enable Jumbo Frame.
Jumbo Frame (Bytes)	Specify the size of jumbo frame. The valid range is from 1518 to 9216.

Table 6-10 Jumbo Frame fields

6.6 PoE

6.6.1 PoE Port Status

To display PoE Port Status page, click **Port** > **PoE** > **PoE Port Status**.

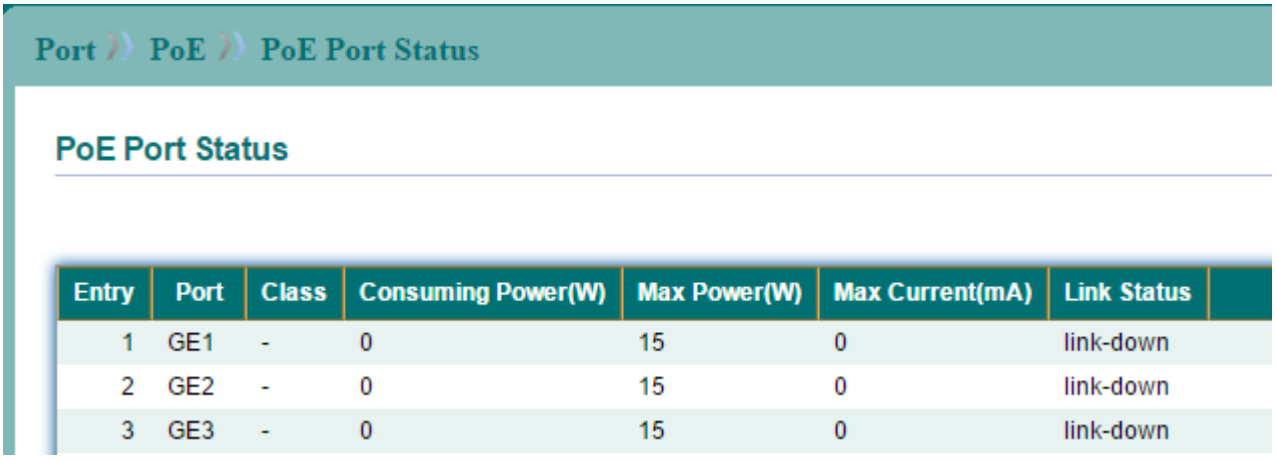


Figure 6-13 PoE Port Status page

Field	Description
Port	The switch port.
Class	PoE Class. ● - : normal status. ● Over: The used power is over the allocated power.
Consuming Power(W)	The used power.
Max Power(W)	Maximum power can be used.
Max Current(mA)	Maximum current can be used.
Link Status	The link status with PD device.

Table 6-11 PoE Port Status fields

Click "Refresh" button to update PoE Port Status.

6.6.2 PoE Setting

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

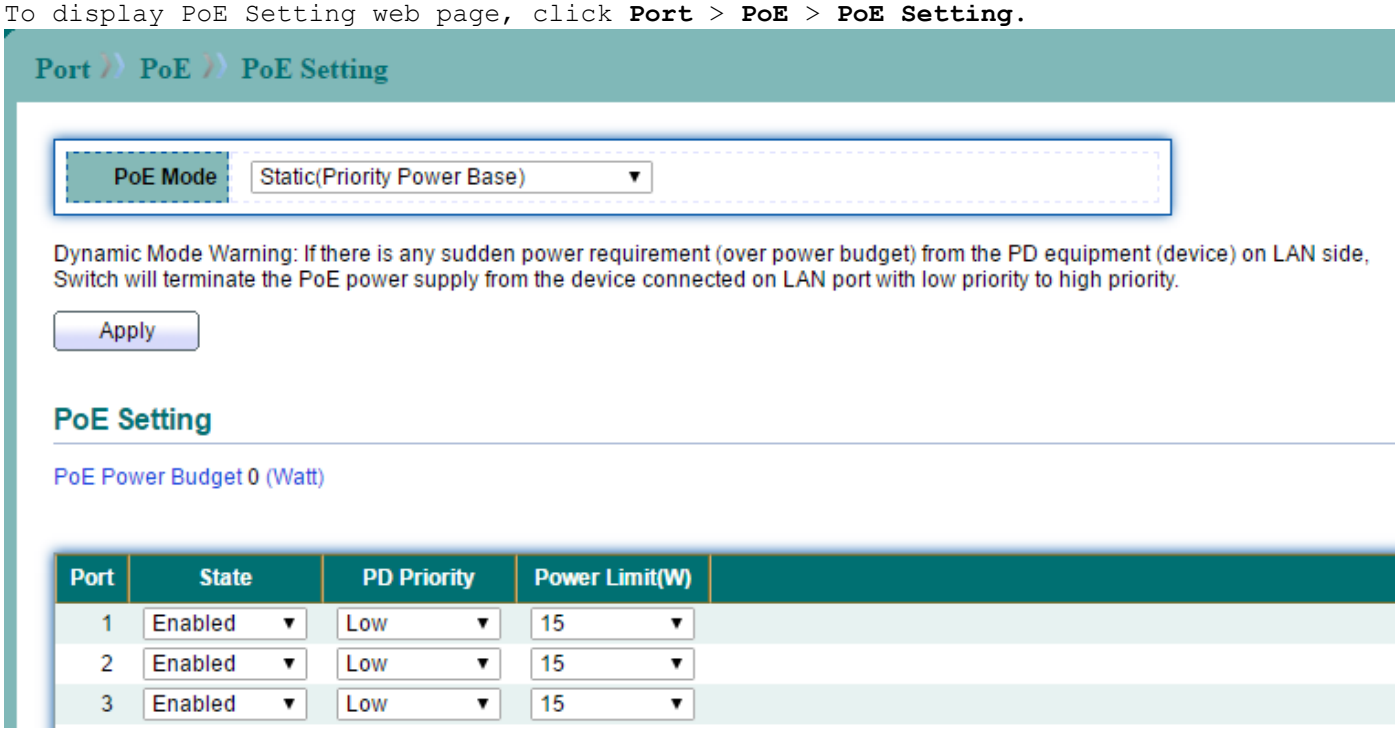


Figure 6-14 PoE Setting page

Field	Description
PoE Mode	The PoE mode : ● Static (Priority Power Base): static mode with user configured power. ● Dynamic (Priority Class Base): automatically allocated power base on the link-up sequence of PD device.
Port	The switch port.
State	Enabled or disabled state of PoE for the port
PD Priority	The priority of PD device : ● Low: the lowest priority. ● High: the medium priority. ● Critical: the highest priority.
Power Limit(W)	The power limit for PD device.

Table 6-12 PoE Setting fields

7 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.

7.1 VLAN

7.1.1 Create VLAN

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

This page allow user to configure add, edit or delete VLAN entries.

Figure 7-1 Create VLAN page

Field	Description
Available VLAN	VLAN that available for create.
Created VLAN	VLAN that has been created.

Table 7-1 Create VLAN fields

Select an available VLAN then click "Apply" button to create. User can edit VLAN name by select VLAN from VLAN Table then click "Edit" button.

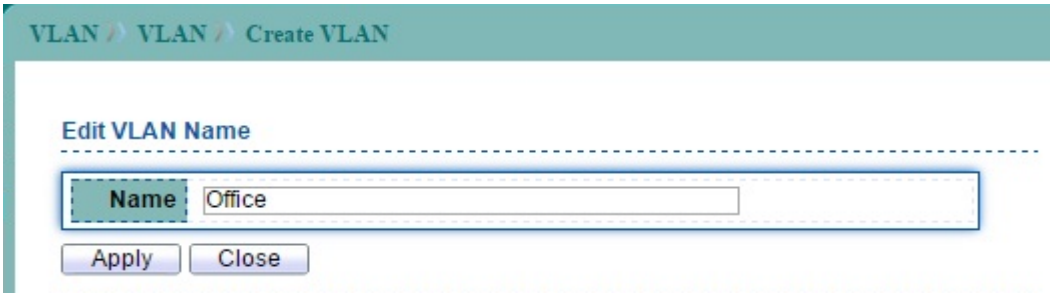


Figure 7-2 Edit VLAN Name page

7.1.2 VLAN Configuration

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

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

Figure 7-3 VLAN Configuration Table page

Field	Description
Entry	Port entry.
Port	Display the interface of this port entry.
Mode	Display the LAN mode of this port. • **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.
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	Check this checkbox to select the VLAN ID to be the port-based VLAN ID for this port. In access mode, PVID equals access VLAN.

Table 7-2 VLAN Configuration Table fields

7.1.3 VLAN Membership

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

This page allow user to view membership information for each port and edit membership for all existed.

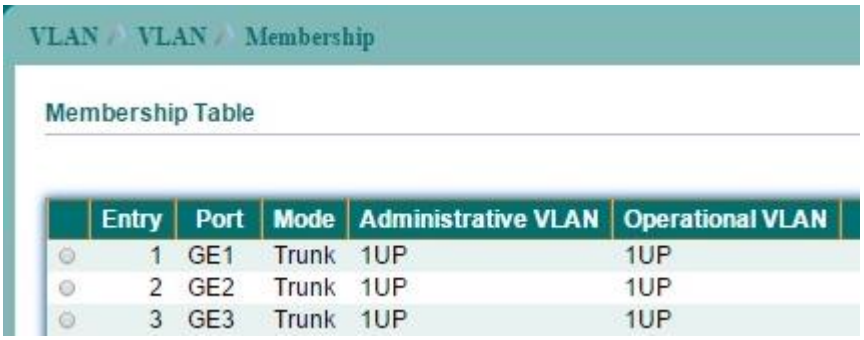


Figure 7-4 VLAN Membership Table page

Field	Description
Entry	Port entry.
Port	Display the interface of this port entry.
Mode	Display the VLAN mode of this port.
Administrative VLANs	Display the administrative VLAN list of this port.
Operational VLANs	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.
Modify	Click the `Edit` Button to edit the VLAN membership of this port.

Table 7-3 VLAN Membership Table fields

Select entry and click "Edit" button to configure Port VLAN membership.

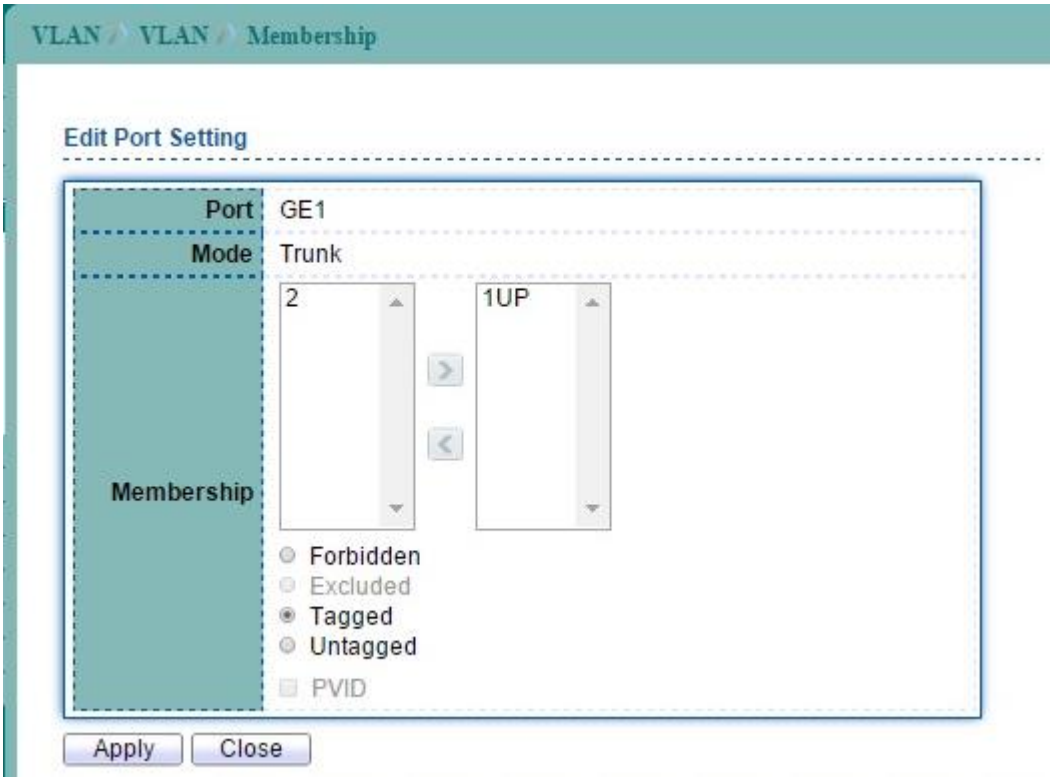


Figure 7-5 Edit VLAN Membership Port Setting page

Field	Description
Port	Selected Switch port.
Mode	Display the VLAN mode of this port.
Select VLAN	Select the left available VLANs to add or the right used VLANs to delete for this port.
Tagging	Select the VLAN membership of the specified left VLANs for this port. Tagging mode may not choose in differ VLAN port mode.
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.

Table 7-4 Edit VLAN Membership Port Setting fields

7.1.4 Port Setting

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

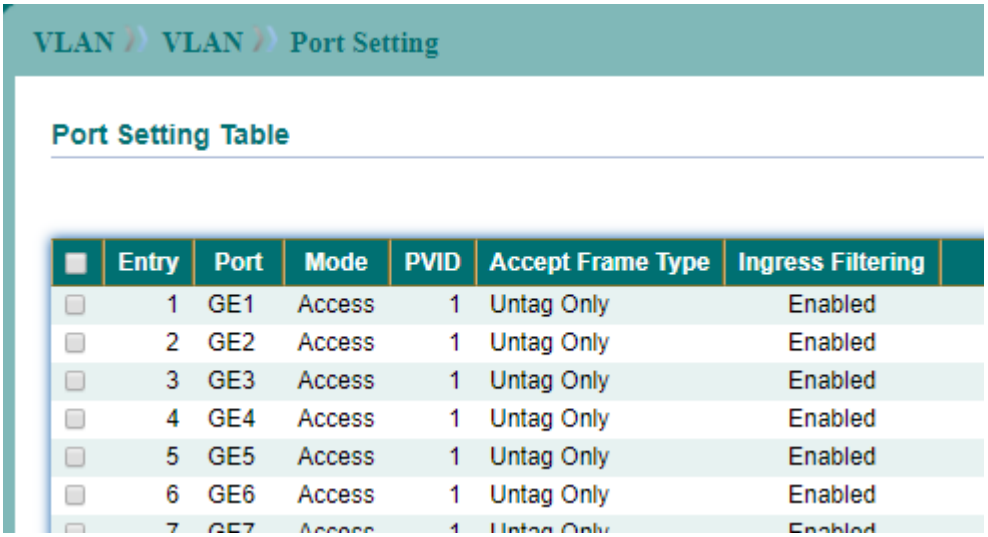


Figure 7-6 VLAN Port Setting page

Select entry and click "Edit" button to configure Port Setting.

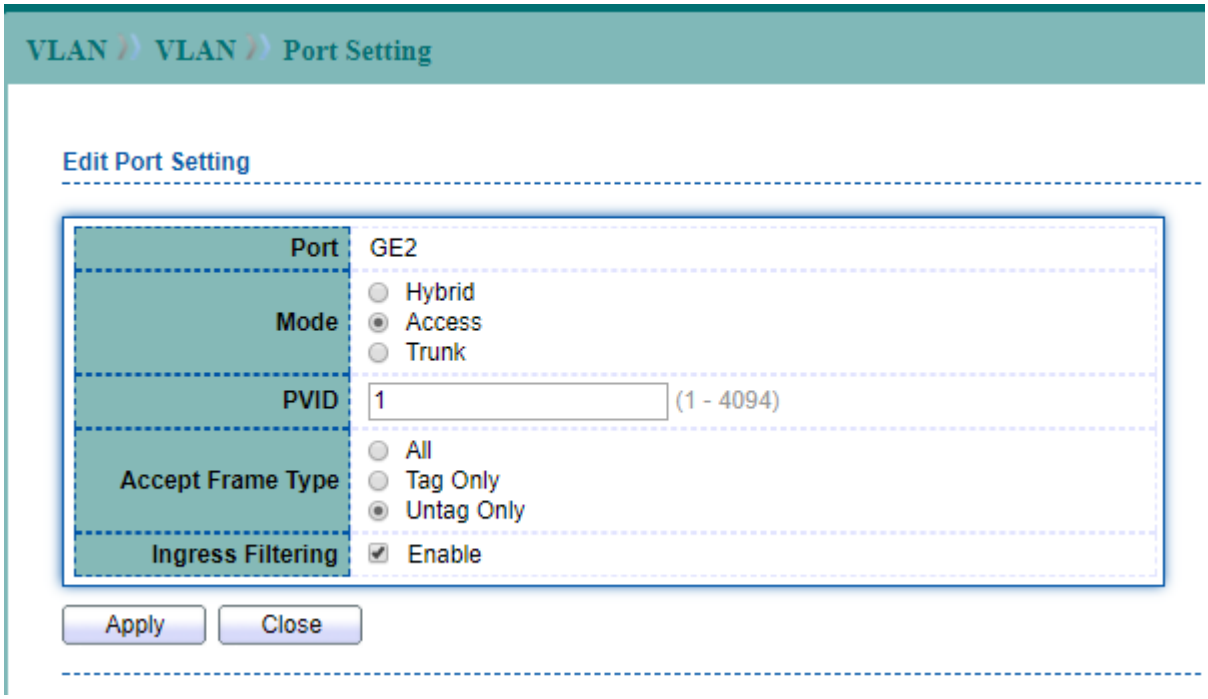


Figure 7-7 Edit VLAN Port Setting page

Field	Description
Port	Selected Switch port.
Mode	Select the VLAN port mode of the interface. • **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 Frame Type	Specify the acceptable-frame-type of the specified interfaces. It's only available with Hybrid mode.
Ingress Filtering	Specify the status of ingress filtering. It's only available with Hybrid mode.

Table 7-5 Edit VLAN Port Setting fields

7.2 Voice VLAN

A Voice VLAN processes IP voice traffic on a specific VLAN.

7.2.1 Voice VLAN Property

To display Voice VLAN Global and Port Setting web page, click **VLAN** > **Voice VLAN** > **Property**.

This page allow user to configure Voice VLAN global settings.

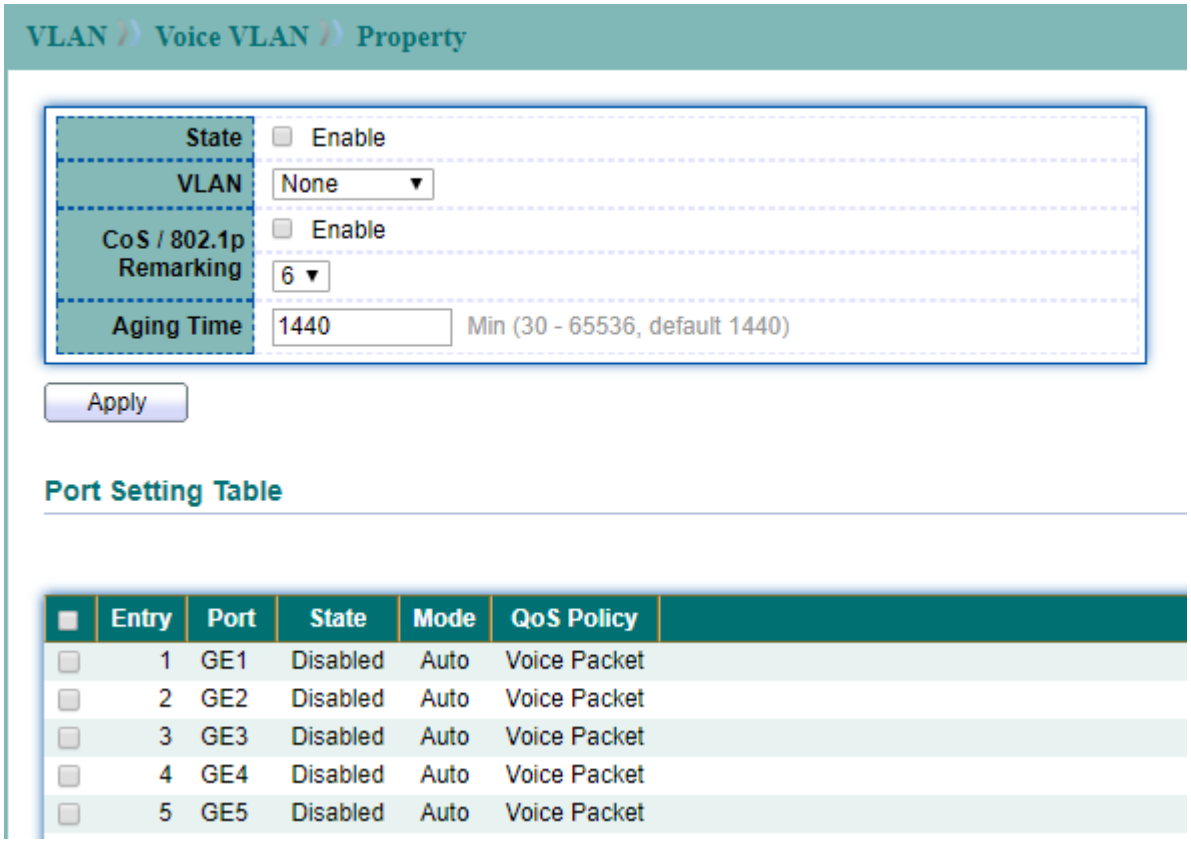


Figure 7-8 Voice VLAN Property page

Select port number from Port Setting Table to enter Voice VLAN Port Setting configure page. This page allow user to set per port settings of Voice VLAN function.

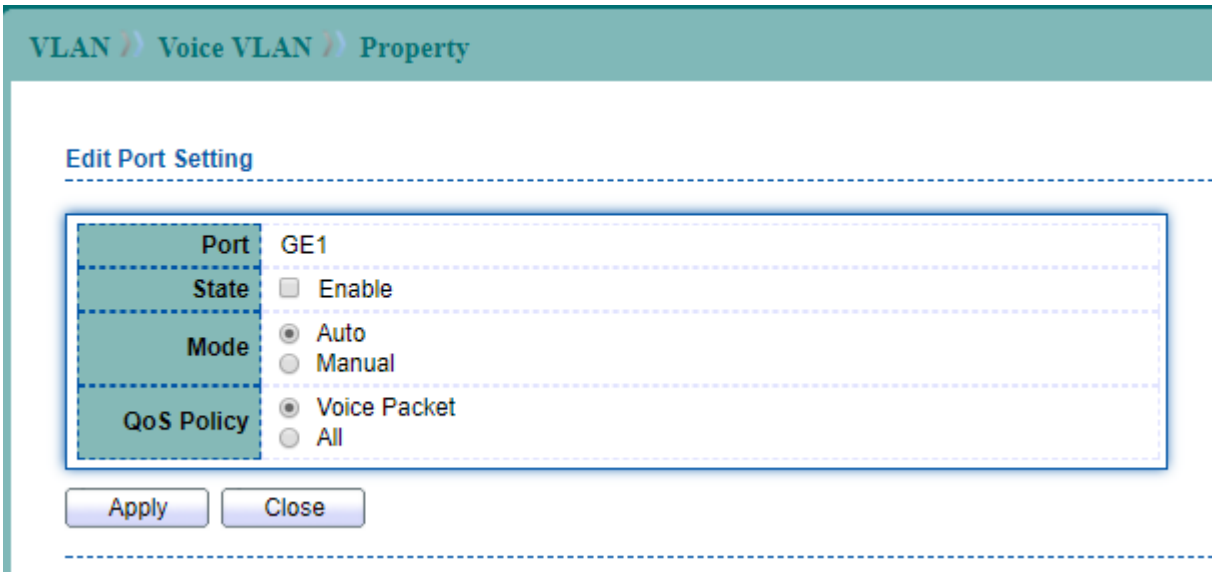


Figure 7-9 Edit Voice VLAN Port Setting page

Field	Description
State	Enable or disable voice VLAN function
VLAN	Select Voice VLAN ID. Voice VLAN ID cannot be default VLAN.
CoS/802.1p Remarking	Enable or disable 1p remarking and select a value of VPT that will be advertised by LLDP-MED.
Aging Time	Select value of aging time.

Table 7-6 Voice VLAN global setting fields

Field	Description
Port	Specified port number
State	Enable or disable voice VLAN function for specified port number.
Mode	Specify port mode Auto : The specified port will add to voice VLAN automatically Manual : The specified port need to manually add to the voice VLAN
QoS Policy	Specify QoS policy target Voice Packet : Only for voice packet All : For all packets

Table 7-7 Voice VLAN port setting fields

7.2.2 Voice OUI

To display Voice OUI Setting web page, click **VLAN** > **Voice VLAN** > **Voice OUI.**

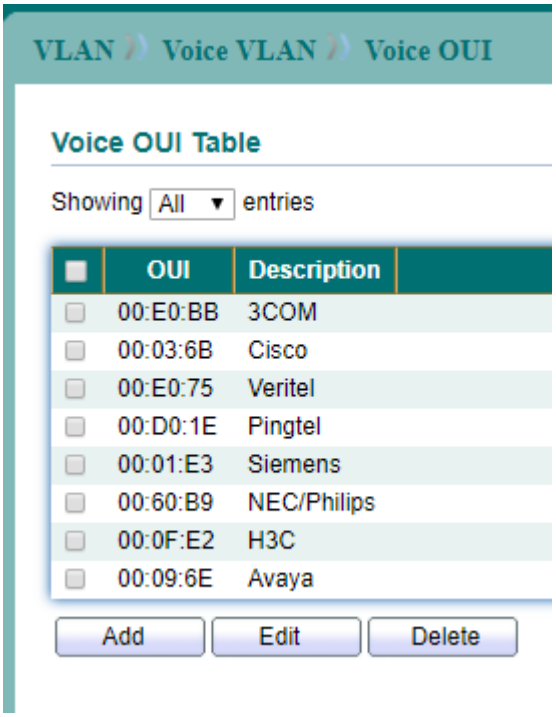


Figure 7-10 Voice OUI page

Click "Add" button to add Voice OUI. Select and click "Edit" button to configure voice OUI.

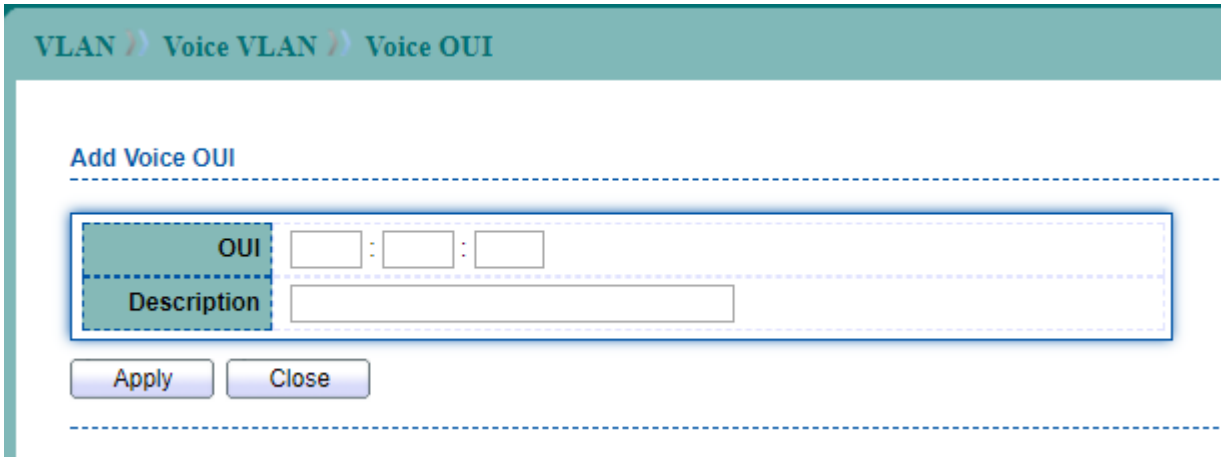


Figure 7-11 Add Voice OUI page

Field	Description
OUI	Enter OUI MAC address
Description	The description of the specified MAC address to the voice VLAN OUI table

Table 7-8 Add voice OUI fields

7.3 Protocol VLAN

A Protocol VLAN processes network traffic based on network protocol. Users can create a protocol VLAN to define filtering criteria for untagged packets.

7.3.1 Protocol Group

To display Protocol VLAN Group Setting web page, click **VLAN** > **Protocol VLAN** > **Protocol Group**.

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

Figure 7-12 Protocol VLAN Protocol Group page

Click "Add" button to add Protocol Group. Select Group and click "Edit" button to configure Protocol Group.

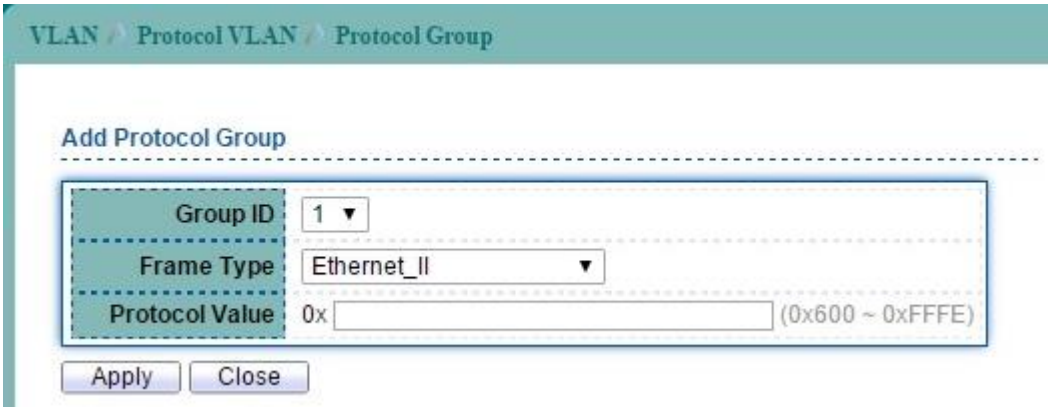


Figure 7-13 Add Protocol VLAN Protocol Group page

Field	Description
Group ID(1-8)	Enter an ID number of the group, between 1 and 8.
Frame Type	This function maps packets to protocol-defined VLANs by examining the type octet within the packet header to discover the type of protocol associated with it. ● **Ethernet_II:** packet type is Ethernet version 2. ● **IEEE802.3 LLC Other:** packet type is 802.3 packet with LLC other header. ● **RFC_1042:** packet type is RFC 1042 packet.
Protocol Value (0-FFFF)	Enter the Ether-type of the target protocol.

Table 7-9 Add Protocol VLAN Protocol Group fields

7.3.2 Protocol VLAN Group Binding

To display Protocol VLAN Group Binding Setting web page, click **VLAN** > **Protocol VLAN** > **Group Binding.**

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

Figure 7-14 Protocol VLAN Group Binding page

Click "Add" button to create a new Group Binding entry.

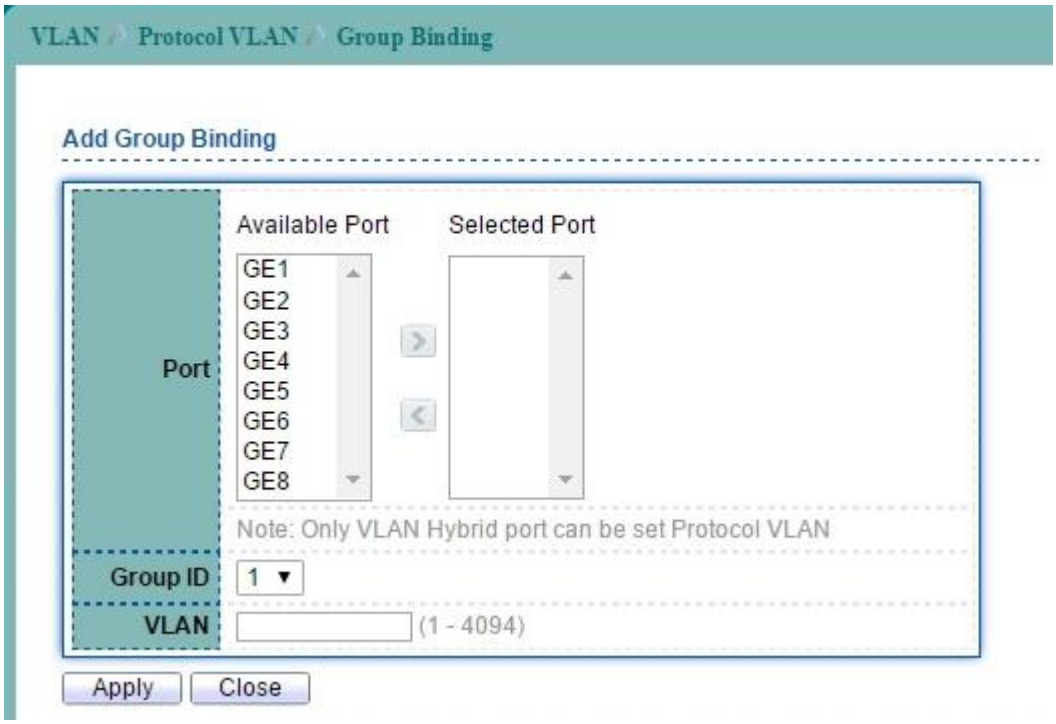


Figure 7-15 Add Protocol VLAN Group Binging page

Field	Description
Port	Select the specified ports you wish to configure by selecting the port in this list.
Group ID	Click the corresponding radio button to select a previously configured Group ID.
VLAN	Enter the VLAN ID.

Table 7-10 Add Protocol VLAN Group Binging fields

7.4 MAC VLAN

7.4.1 MAC Group

To display MAC VLAN Group Table web page, click **VLAN** > **MAC VLAN** > **MAC Group.**

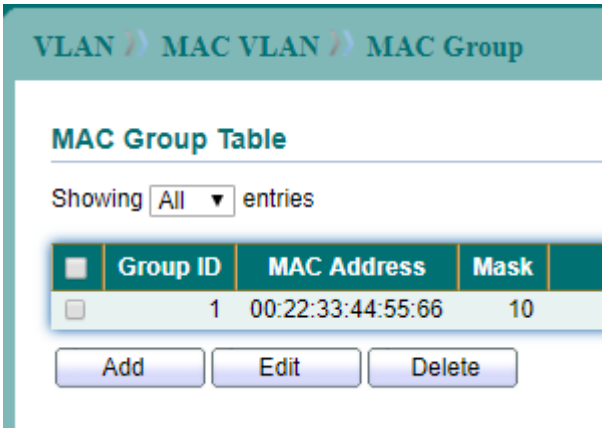


Figure 7-16 MAC Group Table page

Click "Add" button to create a new MAC Group entry.

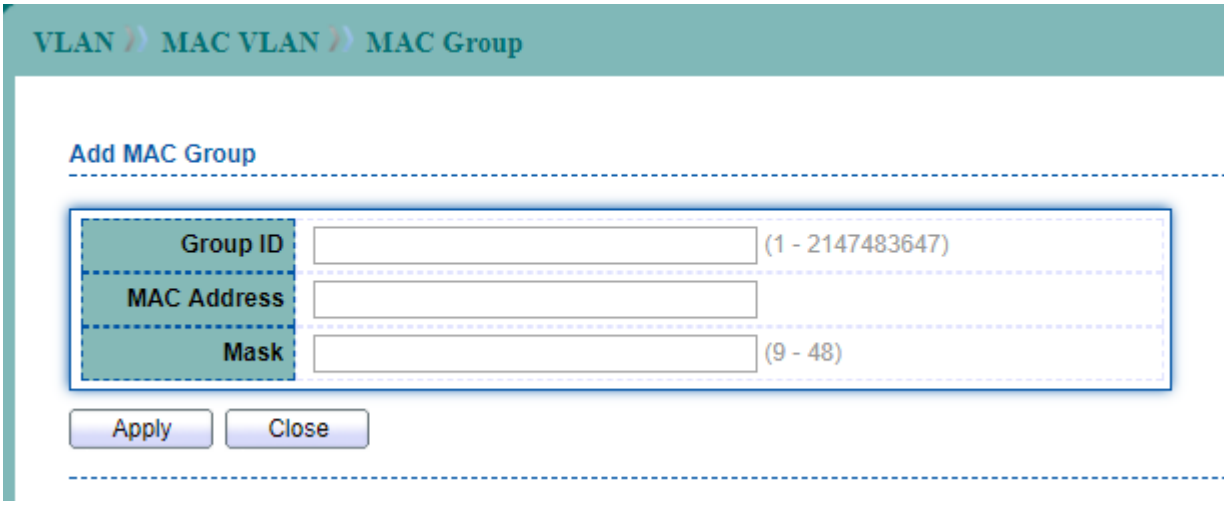


Figure 7-17 Add MAC Group page

Field	Description
Group ID	Specify the Group ID
MAC Address	Specify MAC Address
Mask	Specify Mask length for MAC address

Table 7-11 Add MAC Group Table fields

7.4.2 Group Binding

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

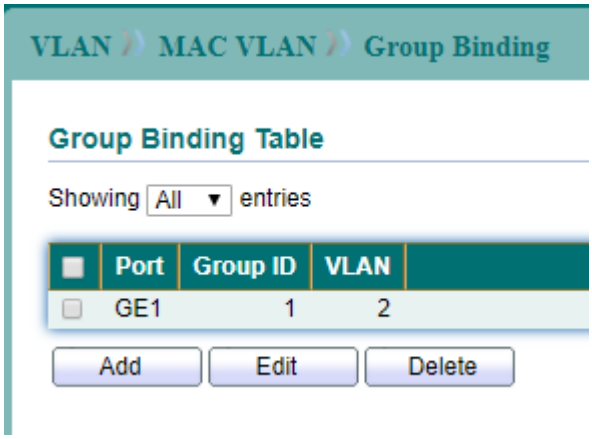


Figure 7-18 Group Binding Table page

Click "Add" button to create a new Group Binding entry.

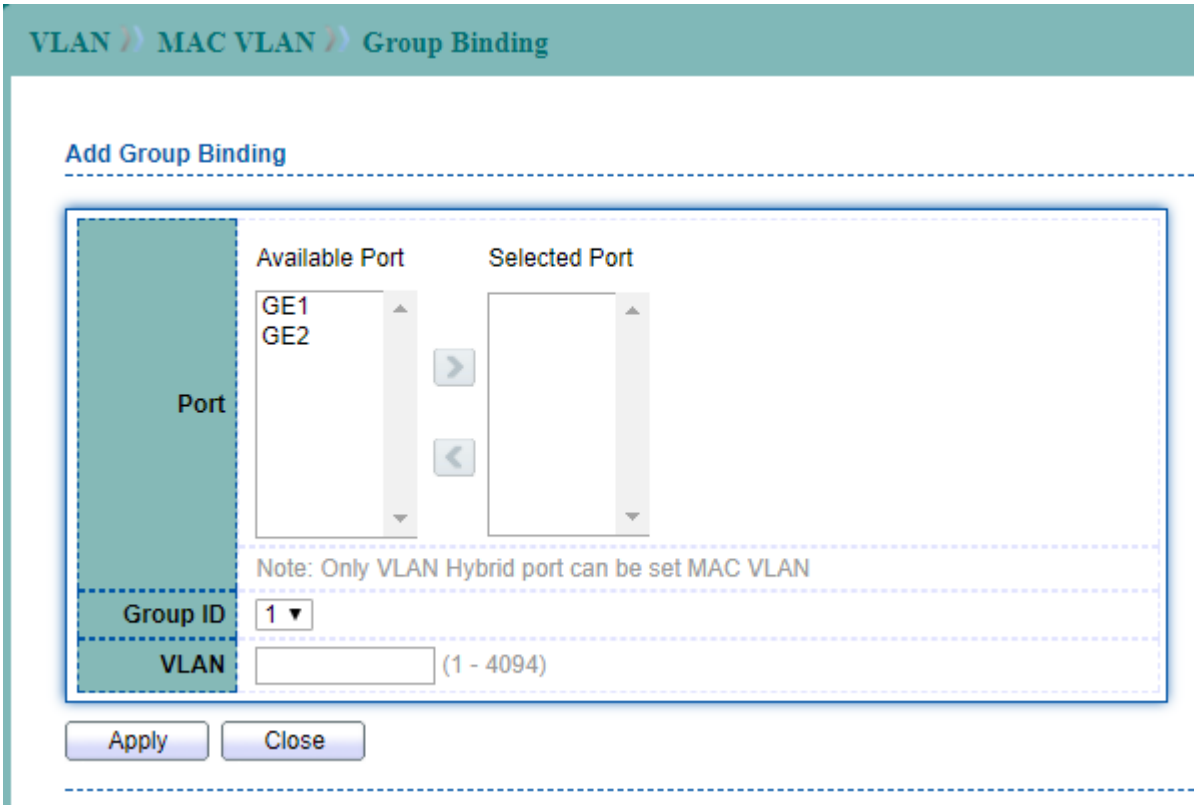


Figure 7-19 Add Group Binding page

Field	Description
Port	Specify the port number
Group ID	Specify MAC Group ID
VLAN	Specify VLAN ID

Table 7-12 Add Group Binding Table fields

7.5 GVRP

7.5.1 GVRP Property

To display GVRP Global Setting web page, click **VLAN** > **GVRP** > **Property**.

This page allow user to enable or disable GVRP function.

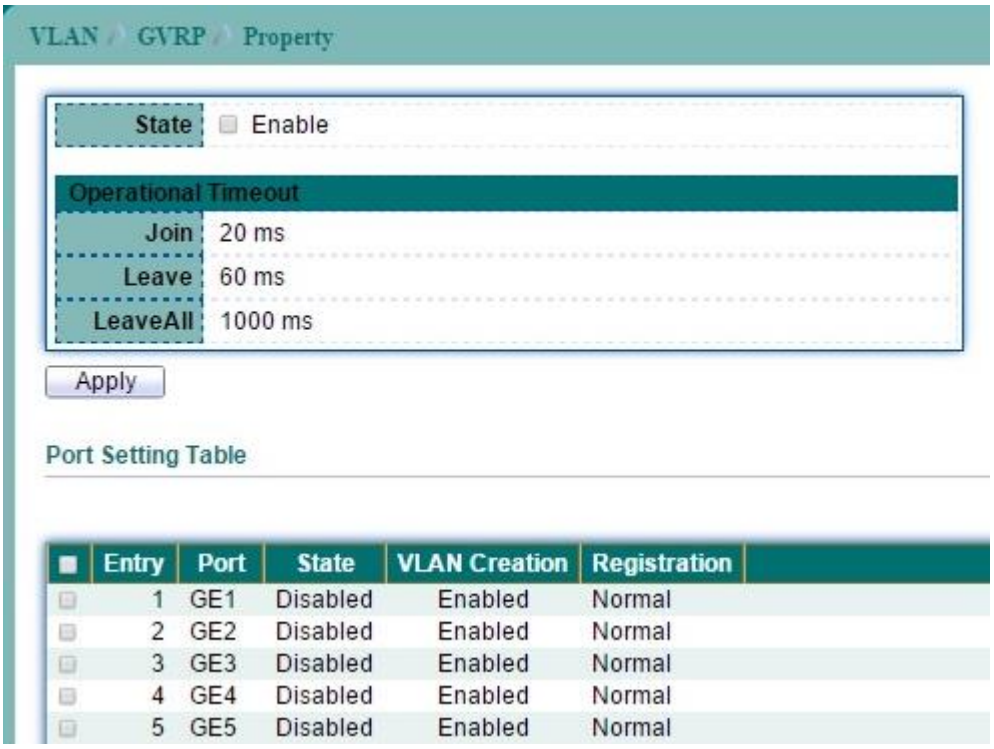


Figure 7-20 GVRP Property page

Field	Description
State	Set the enabling status of GVRP functionality Enable: Enable GVRP.
GVRP Status	GVRP Global status.
Operational Timeout	
Join TimeOut	GVRP Join time out.
Leave TimeOut	GVRP leave time out.
Leave All TimeOut	GVRP leave all time out.

Table 7-13 Property fields

Select port number from Port Setting Table to enter GVRP Port Setting configure page.
This page allow user to set per port settings of GVRP function.

Figure 7-21 Edit GVRP Property Port Setting page

Field	Description
Port	Selected Port or multiple ports.
State	Set the enabling status of GVRP port. ● **Enable**: Enable port of GVRP.
VLAN Creation	Set the enabling status of GVRP port create VLAN ● **Enable**: port can create dynamic VLAN.
Registration	Set the register mode of GVRP port. ● **Normal**: Normal mode. ● **Fixed**: The port will not learn any dynamic VLAN. Only send static VLAN information to neighbor and allow static VLAN packet pass. ● **Forbidden**: The port will not learn any dynamic VLAN and only allow default VLAN packet pass.

Table 7-14 Edit GVRP Property Port Setting fields

7.5.2 GVRP Membership

To display GVRP VLAN database web page, click **VLAN** > **GVRP** > **Membership.**

This page allow user to browser all VLAN member settings that learned by GVRP protocol.

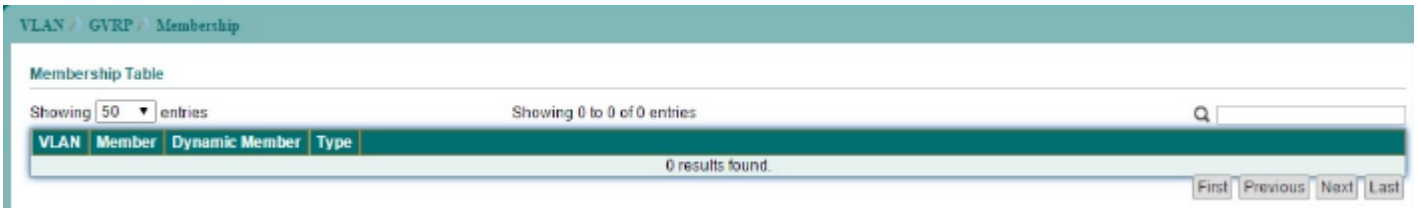


Figure 7-22 GVRP Membership page

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

Table 7-15 GVRP Membership fields

7.5.3 GVRP Statistics

To display GVRP statistics web page, click **VLAN** > **GVRP** > **Statistics.**

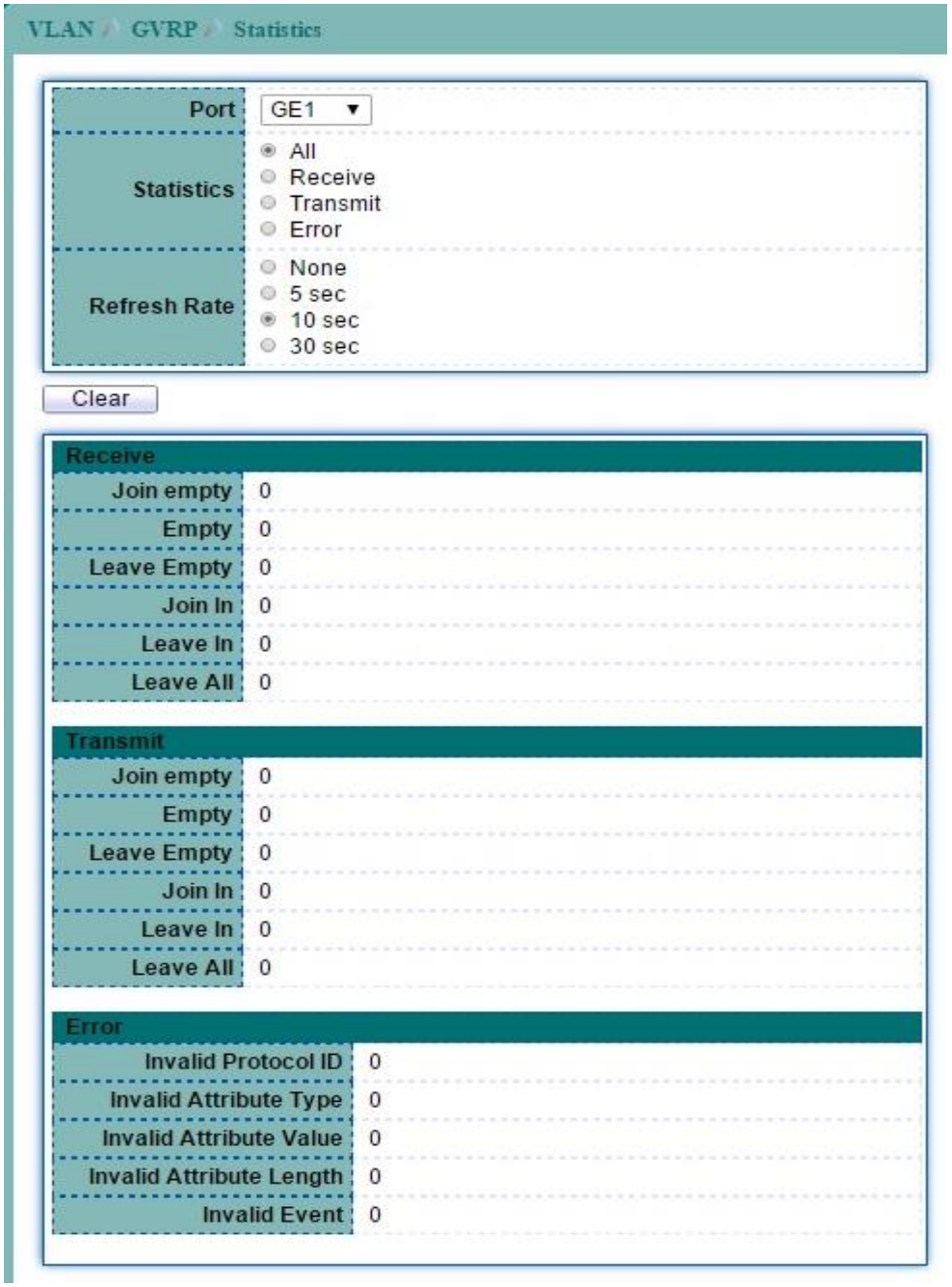


Figure 7-23 GVRP Statistics page

Field	Description
Port	Port Number
Statistics	Type of Statistics
Refresh Rate	The interval of refresh statistics

Table 7-16 GVRP Membership fields

8 MAC Address Table

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

8.1 Dynamic Address

To configure the aging time of the dynamic address and to display the dynamic learned address, click **MAC Address Table** > **Dynamic Address**.

Select the dynamic address entry and click "Add Static Address" button to configure the entry to be static.

Figure 8-1 Dynamic Address page

Field	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.
VLAN	The VLAN ID that dynamic MAC address learned on.
MAC Address	The dynamic learned MAC addresses.
Port	The port number that dynamic MAC address learned on.

Table 8-1 Dynamic Address fields

8.2 Static MAC Setting

To display the static MAC address, click **MAC Address Table** > **Static Address**.

Figure 8-2 Static Address Table page

Click "Add" button to configure new static address entry.

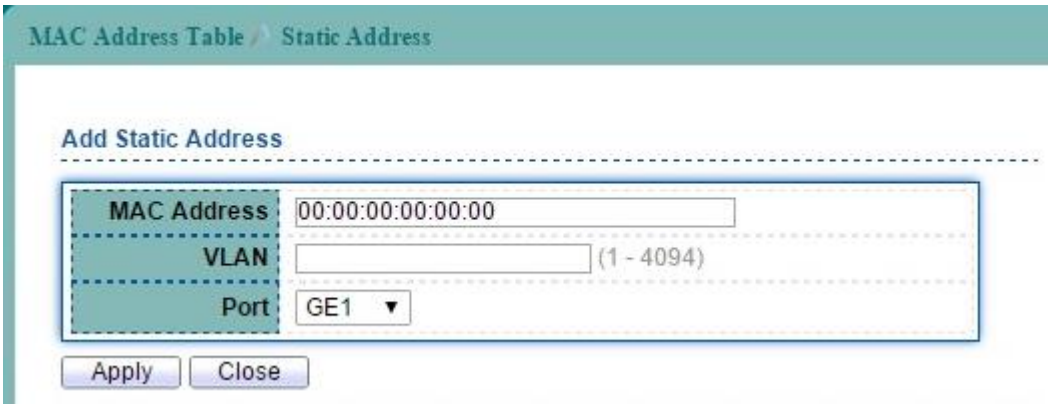


Figure 8-3 Add Static Address page

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

Table 8-2 Add Static Address fields

8.3 MAC Filtering Address

To configure and display the MAC filtering settings, click **MAC Address Table** > **Filtering Address.**

Figure 8-4 Filtering Address page

Field	Description
VLAN	Specify the VLAN to show or clear MAC entries.
MAC Address	The MAC address to which packets will be statically forwarded.
Add	Add Filtering Address.

Table 8-3 Filtering Address fields

Click "Add" button to configure new filtering address entry.

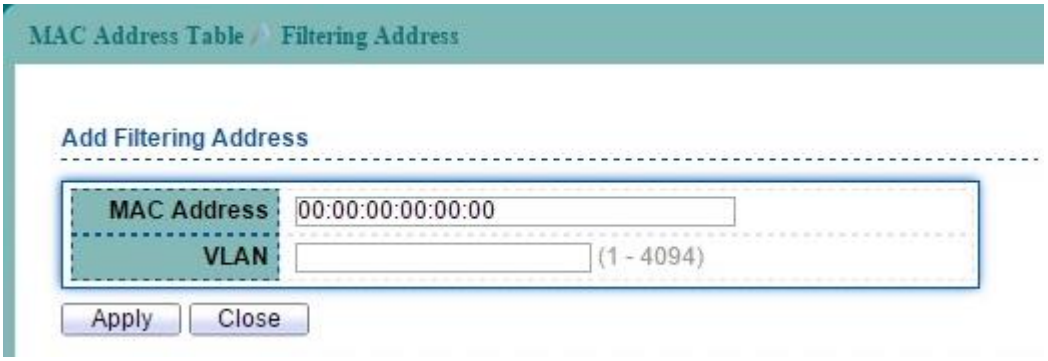


Figure 8-5 Add Filtering Address page

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

Table 8-4 Add Filtering Address fields

9 Spanning Tree Protocol

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

9.1 STP Property

To configure and display STP configuration, click **Spanning Tree** > **Property**.

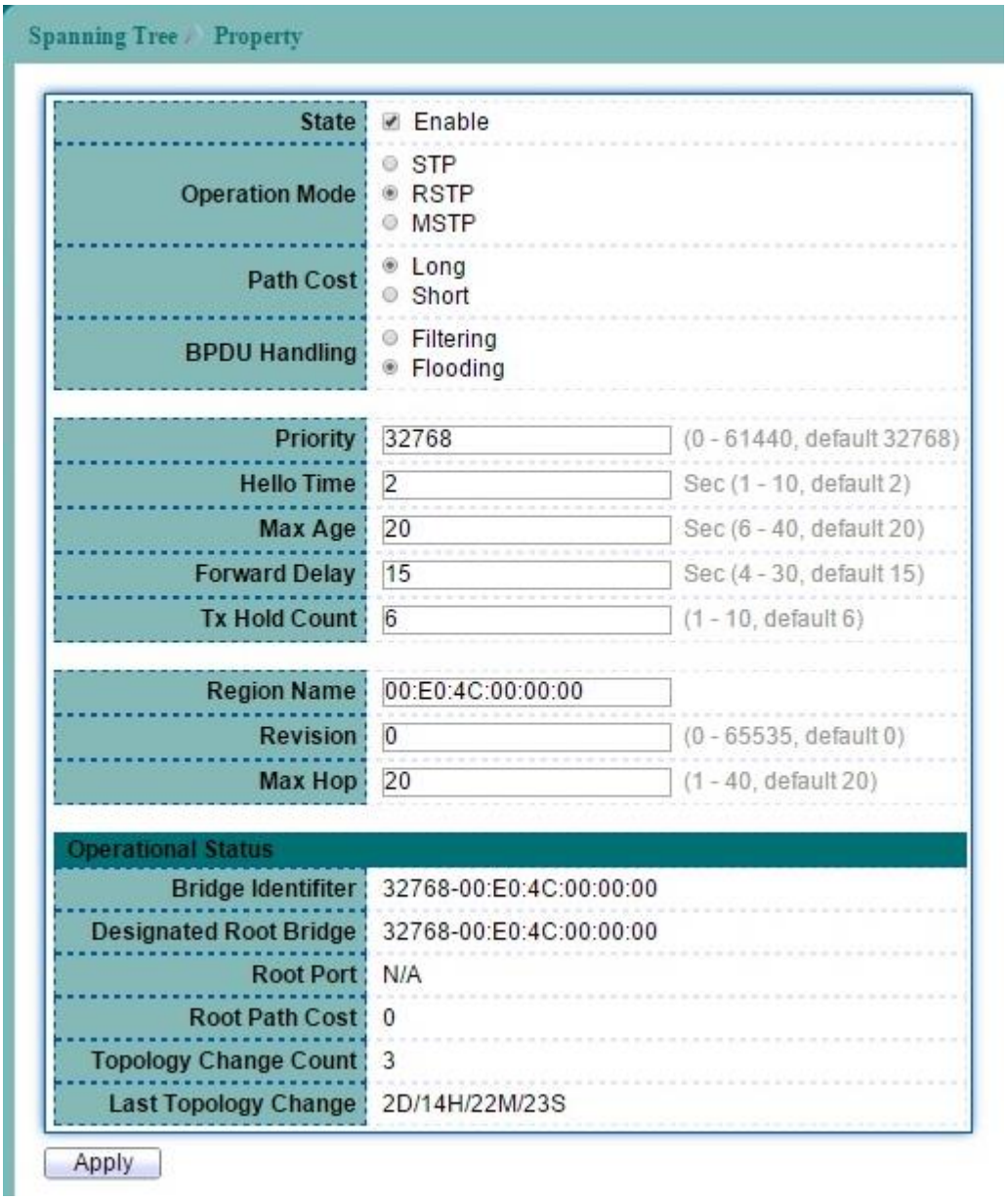


Figure 9-1 STP Property page

Field	Description
State	Enable/Disable the STP on the switch.
Operation Mode	Specify the STP operation mode. • **STP-Compatible:** Enable the Spanning Tree (STP) operation. • **RSTP-Operation:** Enable the Rapid Spanning Tree (RSTP) operation. • **MSTP-Operation:** Enable the Multiple Spanning Tree (MSTP) operation.
Path Cost	Specify the path cost method.

	• **long**: Flood the BPDU when STP is disabled. • **short**: Filter the BPDU when STP is disabled.
BPDU Handling	Specify the BPDU forward method when the STP is disabled. • **flooding**: Flood the BPDU when STP is disabled. • **filtering**: Filter the BPDU when STP is disabled.
Priority	Specify the CIST bridge priority. The valid range is from 0 to 61440. 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.
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 Hops	Specify the number of hops in an MSTP region before the BPDU is discarded. The valid range is 1 to 40.

Table 9-1 STP Property fields

9.2 STP Port Setting

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

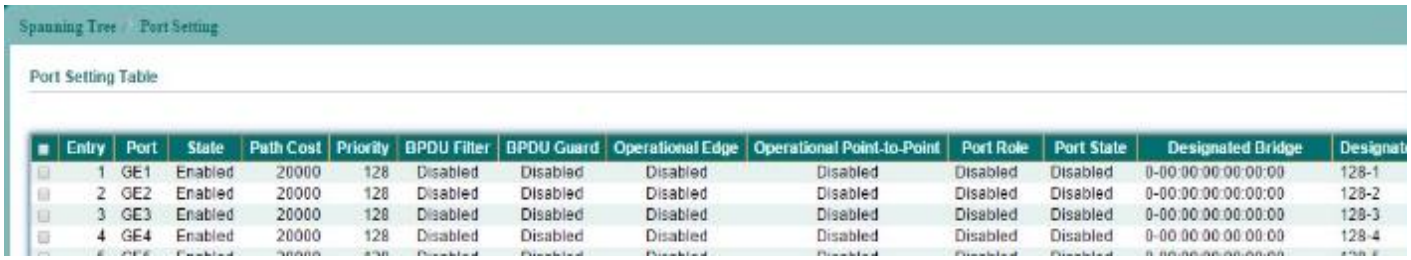


Figure 9-2 STP Port Setting page

Select entry and click "Edit" button to configure STP port setting.

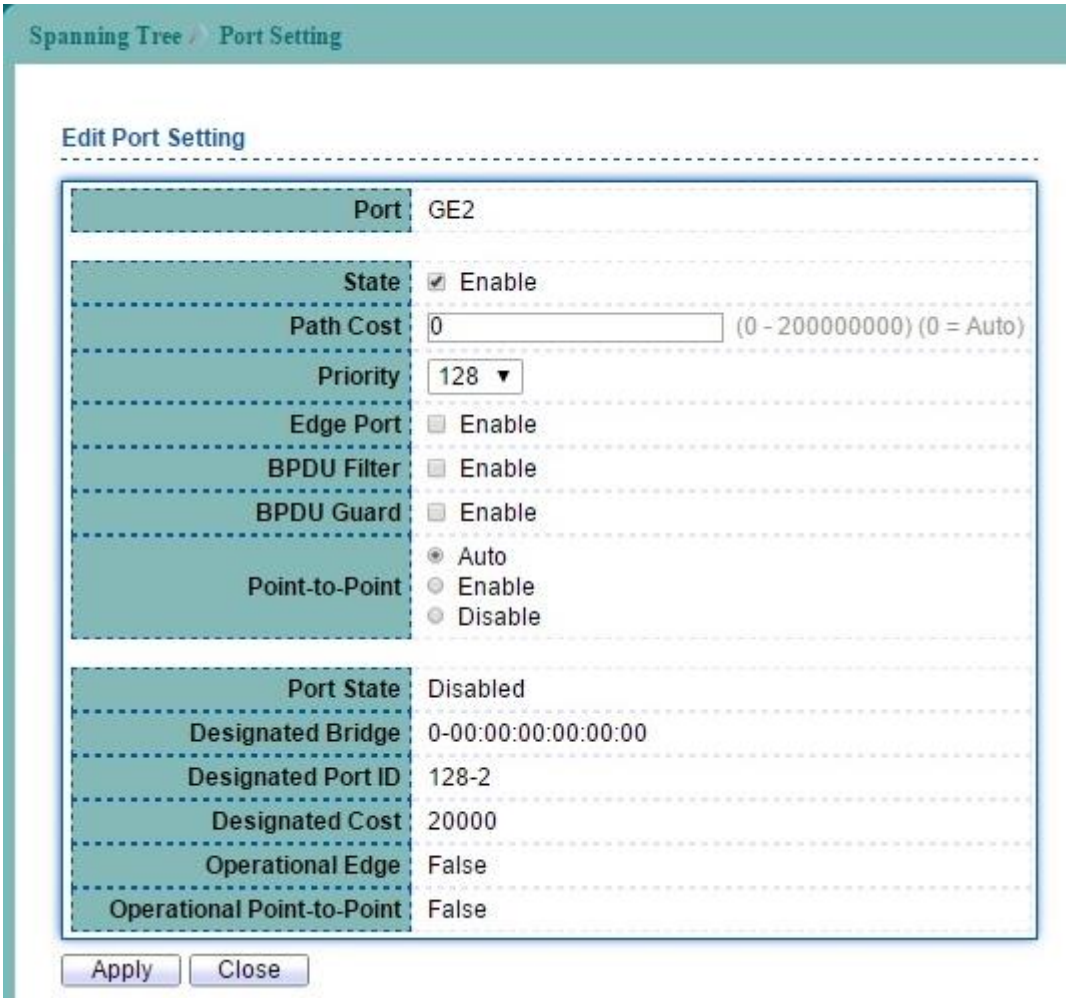


Figure 9-3 Edit STP Port Setting page

Field	Description
Port	Specify the port ID or the list of port IDs.
Path Cost	The port path cost. For the long path cost method, its valid range is from 0 to 200000000; and the valid range is from 0 to 65535 for the short path cost method. The value 0 indicates AUTO, which the port path cost is determined by the port speed and the path cost method.
Edge Port	Enable the edge mode. 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.
Priority	Specify the interface port priority of the CIST
BPDU Filter	Enable the BPDU Filter configuration avoid receiving/transmitting BPDU from the specified ports.
BPDU Guard	Enable the BPDU Guard configuration to drop the received BPDU directly.
Point-to-Point	Specify the Point-to-Point port configuration. Auto: Auto detect mode. Enable: Enable Point-to-Point. Disable: Disable Point-to-Point.

Table 9-2 STP Port Setting fields

9.3 MST Instance Setting

To configure and display the configuration for MST instance, click **Spanning Tree** > **MST Instance**.

Figure 9-4 MST Instance page

Select MSTI entry and click "Edit" button to configure MST Instance entry.

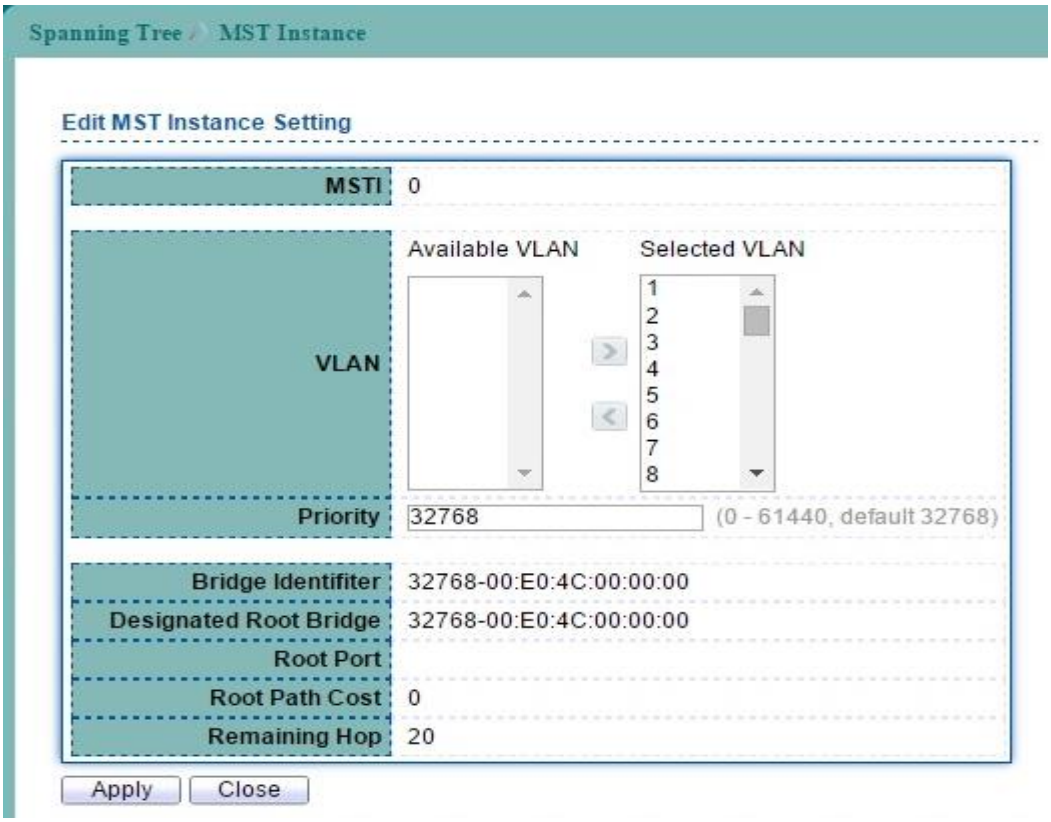


Figure 9-5 Edit MST Instance Setting page

Field	Description
MSTI ID	Specify the MST instance ID.
VLAN List	Specify the VLAN list to the specific instance.
Priority	Specify the bridge priority on the specific instance. The valid range is from 0 to 61440. 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.

Table 9-3 MST Instance fields

9.4 MST Port Setting

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

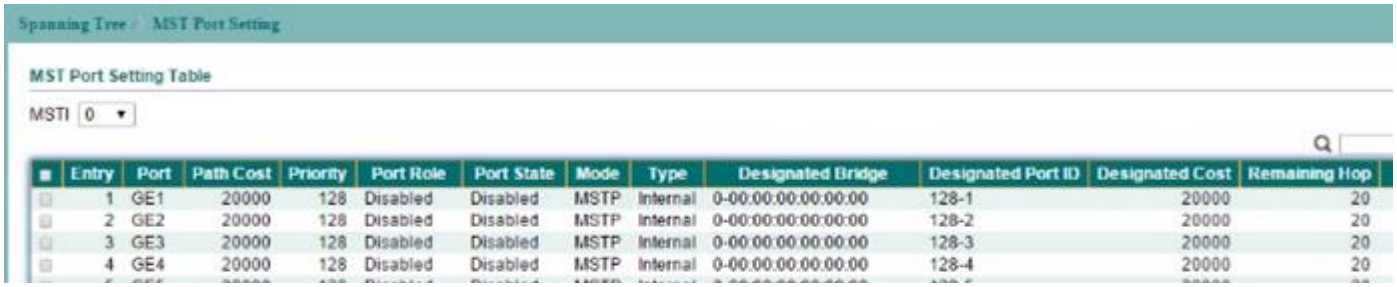


Figure 9-6 MST Port Setting page

Select entry and click "Edit" button to configure MST Port Setting entry.

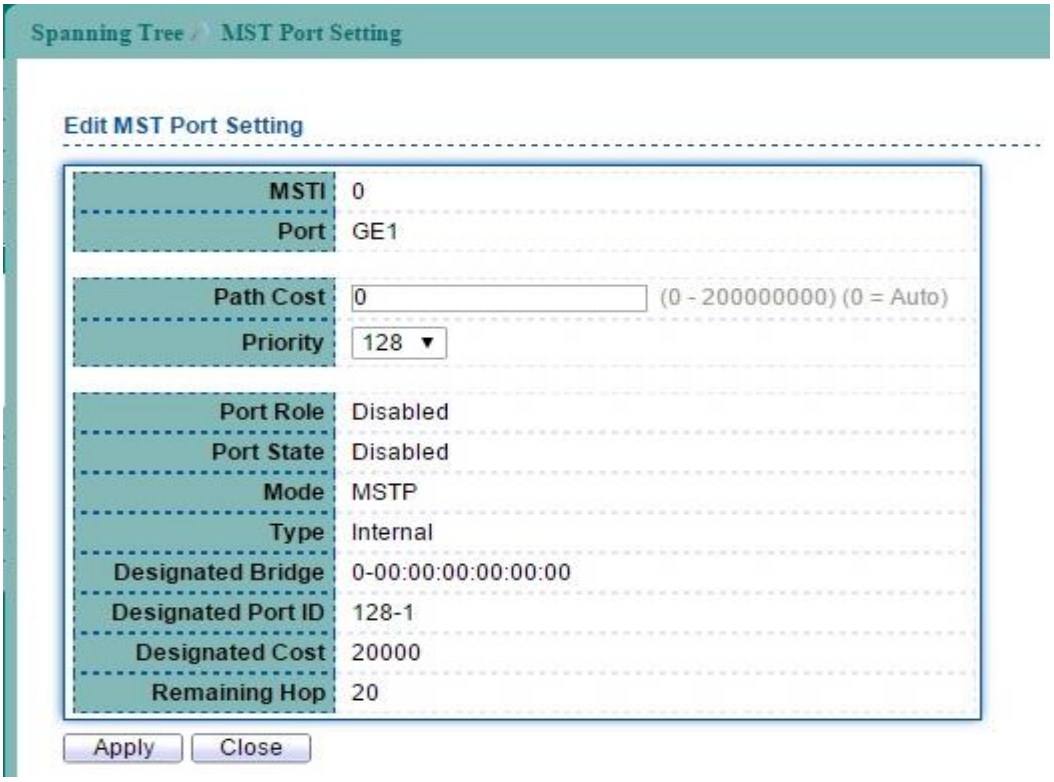


Figure 9-7 Edit MST Port Setting page

Field	Description
MSTI ID	Specify the MST instance ID.
Port	Specify the port or the list of ports on the MST instance.
Priority	Specify the interface priority on the specific instance.
Internal Path Cost	Specify the path cost for the interfaces on the specific MSTP instance. For the long path cost method, its valid range is from 0 to 200000000; and the valid range is from 0 to 65535 for the short path cost method. The value 0 indicates AUTO, which the port path cost is determined by the port speed and the path cost method.

Table 9-4 MST Port Setting fields

9.5 STP Statistics

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

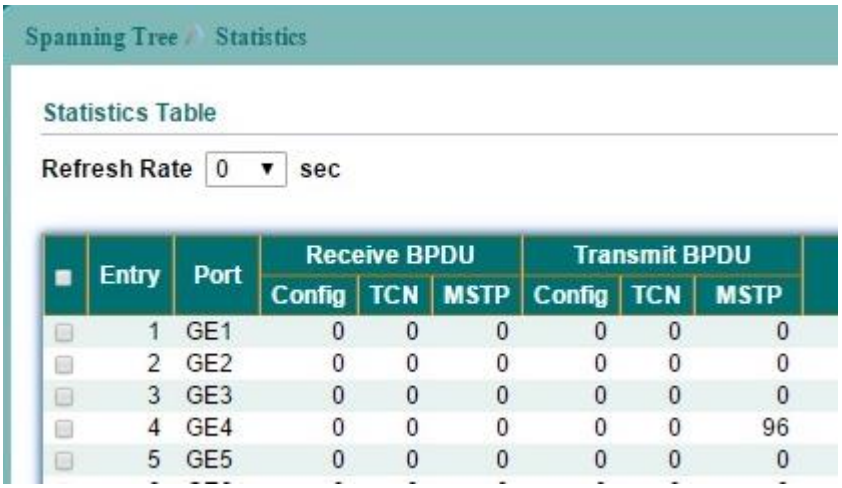


Figure 9-8 STP Statistics page

Field	Description
Port	The switch port number.
Receive BPDU	
Config	The number of configuration BDPUs received.
TCN	The number of TCN BDPUs received.
MSTP	The number of Multiple Spanning Tree Protocol BDPUs received.
Transmit BPDU	
Config	The number of configuration BDPUs transmitted.
TCN	The number of TCN BDPUs transmitted.
MSTP	The number of Multiple Spanning Tree Protocol BDPUs transmitted.

Table 9-5 STP Statistics fields

10 Discovery

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.

10.1 LLDP Property

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

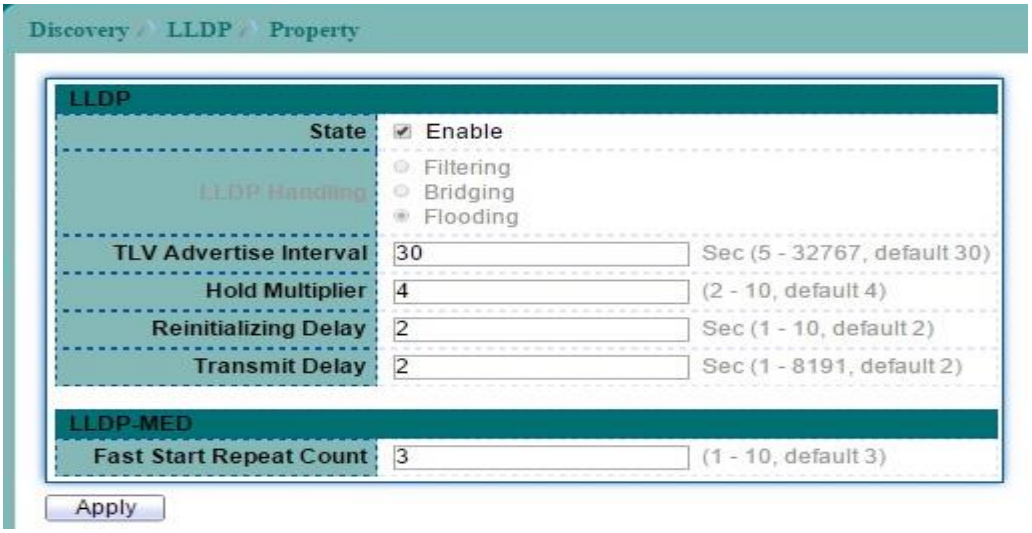


Figure 10-1 LLDP Property page

Field	Description
LLDP	
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 5-32768 seconds.
Hold Multiplier	Select the multiplier on the transmit interval to assign to TTL (range 2-10, default = 4).
Re-initializing 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 1-8192 seconds, default = 3).
LLDP-MED	
Fast Start Repeat Count	Enter LLDP-MED fast start repeat count value (1-10).

Table 10-1 LLDP Property fields

10.2 LLDP Port Setting

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

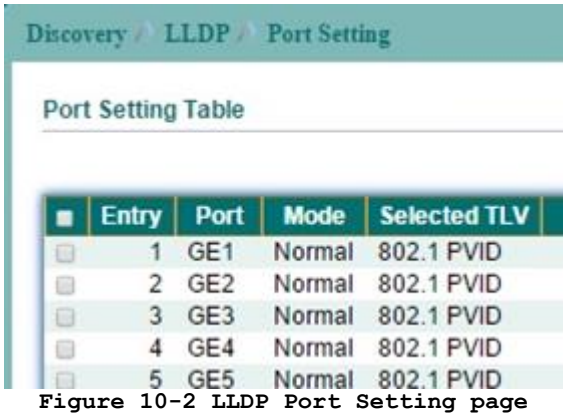


Figure 10-2 LLDP Port Setting page

Select entry and click "Edit" button to configure LLDP Port Setting entry.

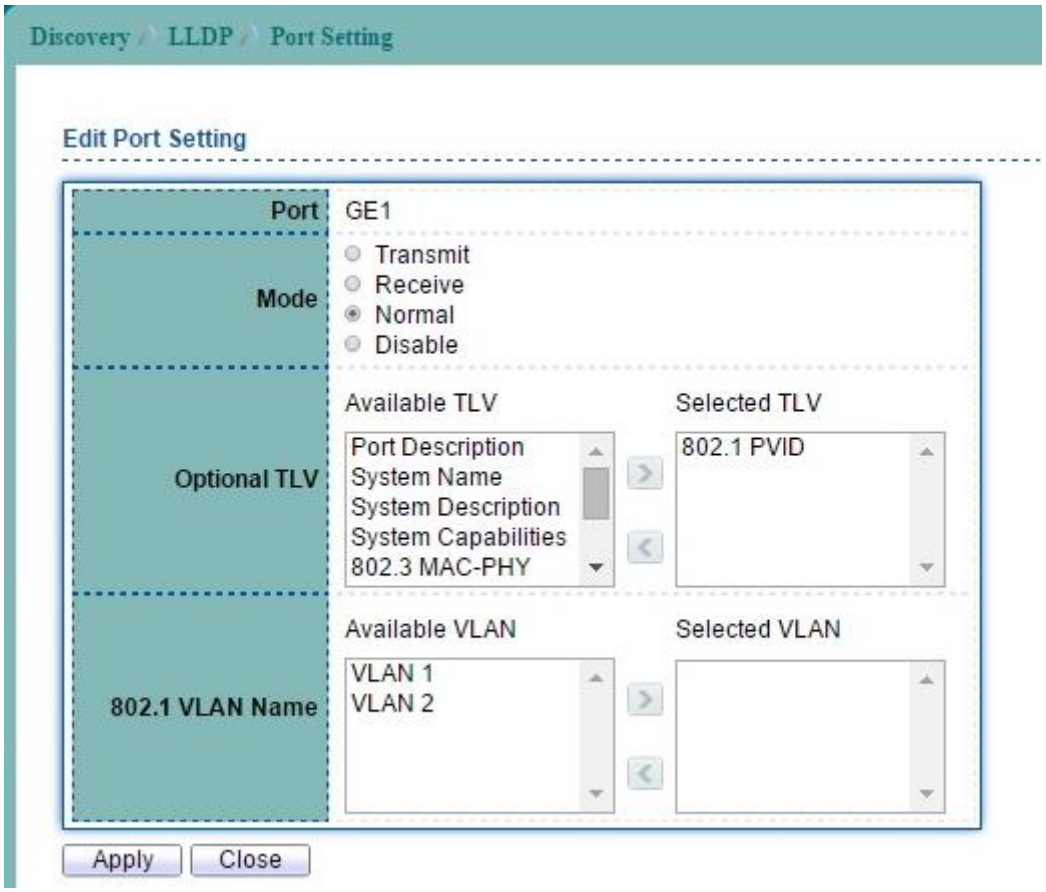


Figure 10-3 Edit LLDP Port Setting page

Field	Description
Port	Selected port(s).
Mode	Select the transmission state of LLDP port interface. ● **Transmit:** Transmit LLDP PDUs only. ● **Receive:** Receive LLDP PDUs only. ● **Normal:** Transmit and receive LLDP PDUs both. ● **Disable:** Disable the transmission of LLDP PDUs.
Optional TLV	Select the LLDP optional TLVs to be carried (multiple selection

Select	is allowed). • **System Name** • **Port Description** • **System Description** • **System Capability** • **802.3 MAC-PHY** • **802.3 Link Aggregation** • **802.3 Maximum Frame Size** • **Management IP Address** • **802.1 PVID**
802.1 VLAN Name	Select the VLAN Name ID to be carried (multiple selection is allowed).

Table 10-2 LLDP Port Setting fields

10.3 LLDP MED Network Policy Setting

To display LLDP MED Network Policy Setting, click **Discovery**> **LLDP** > **MED Network Policy**.

Figure 10-4 LLDP MED Network Policy page

Click "Add" button to configure new LLDP MED Network Policy entry.

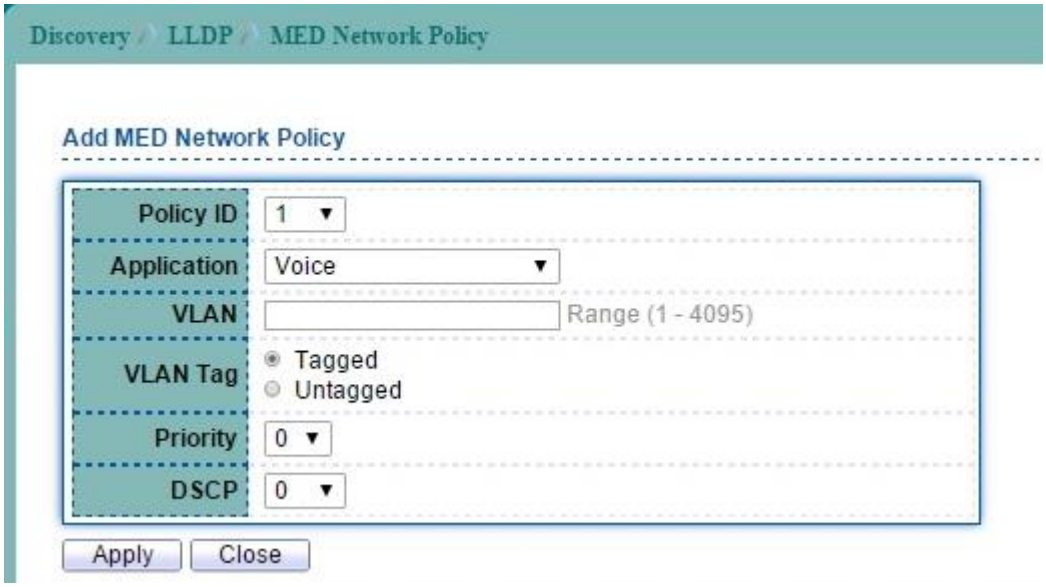


Figure 10-5 Add LLDP MED Network Policy page

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

Table 10-3 LLDP MED Network Policy fields

10.4 LLDP MED Port Setting

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

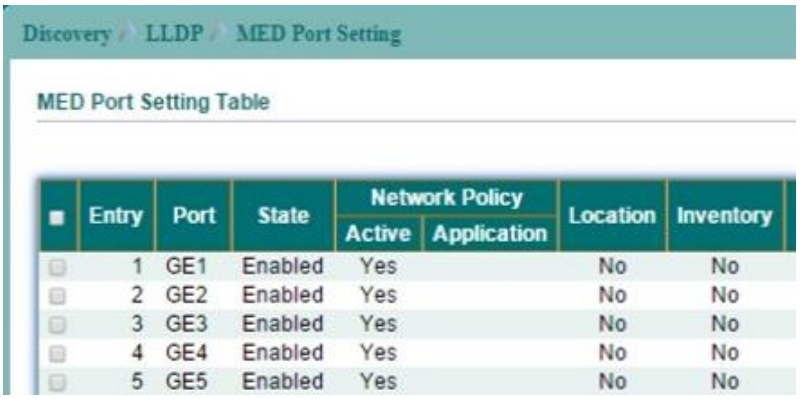


Figure 10-6 LLDP MED Port Setting page

Select entry and click "Edit" button to configure LLDP MED Port Setting entry.

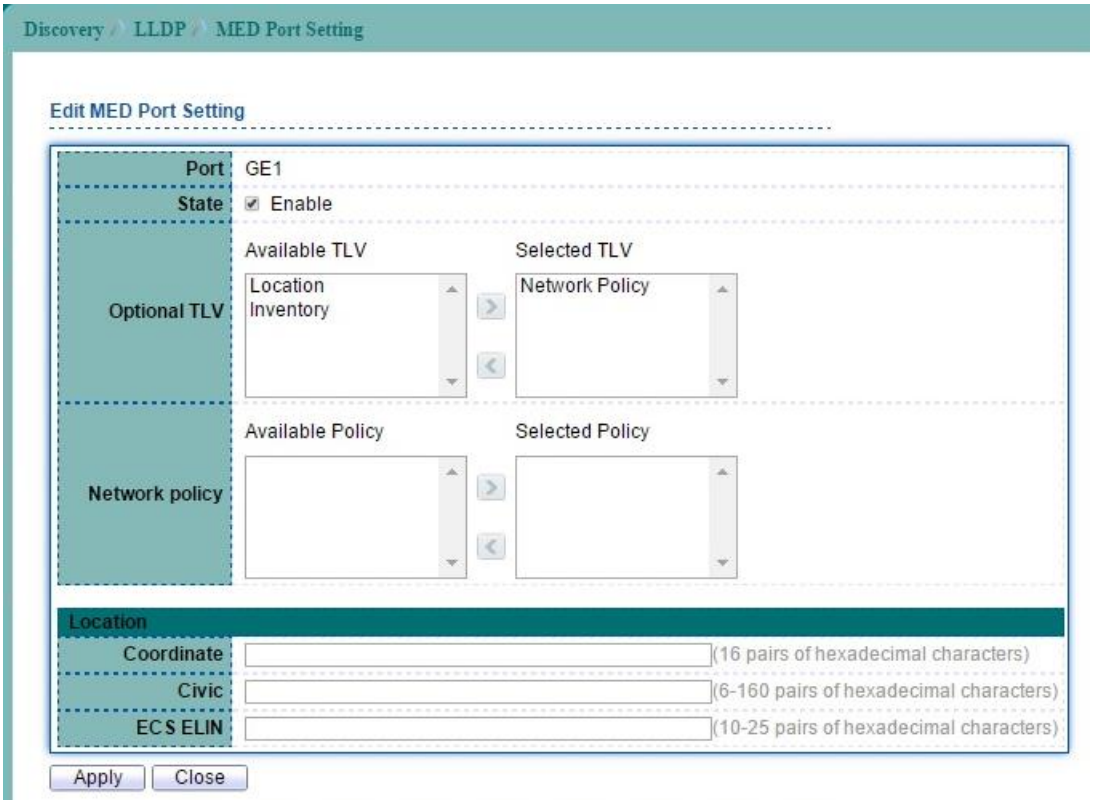


Figure 10-7 Edit LLDP MED Port Setting page

Field	Description
Port	Select specified port or all ports to configure LLDP MED.
State	Select LLDP MED enable status.
Optional TLVs	Select LLDP MED optional TLVs (multiple selection is allowed) • **Network Policy** • **Location** • **Inventory**
Network Policy	Select the network policy IDs to be bound to ports. The network policy should be created in MED Network Policy

	page at first.

Table 10-4 LLDP MED Port Setting fields

10.5 LLDP Packet View

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

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

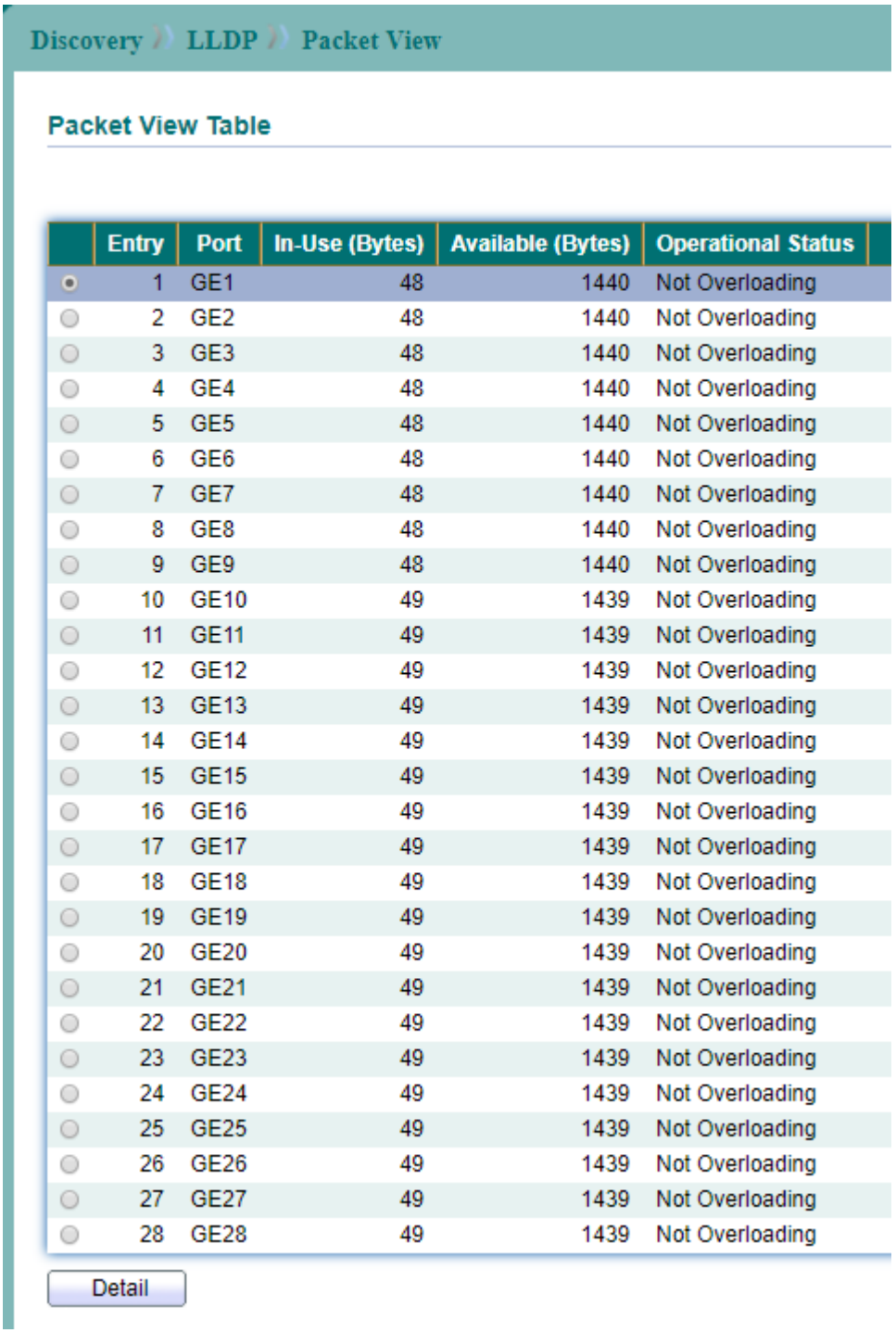


Figure 10-8 LLDP Packet View page

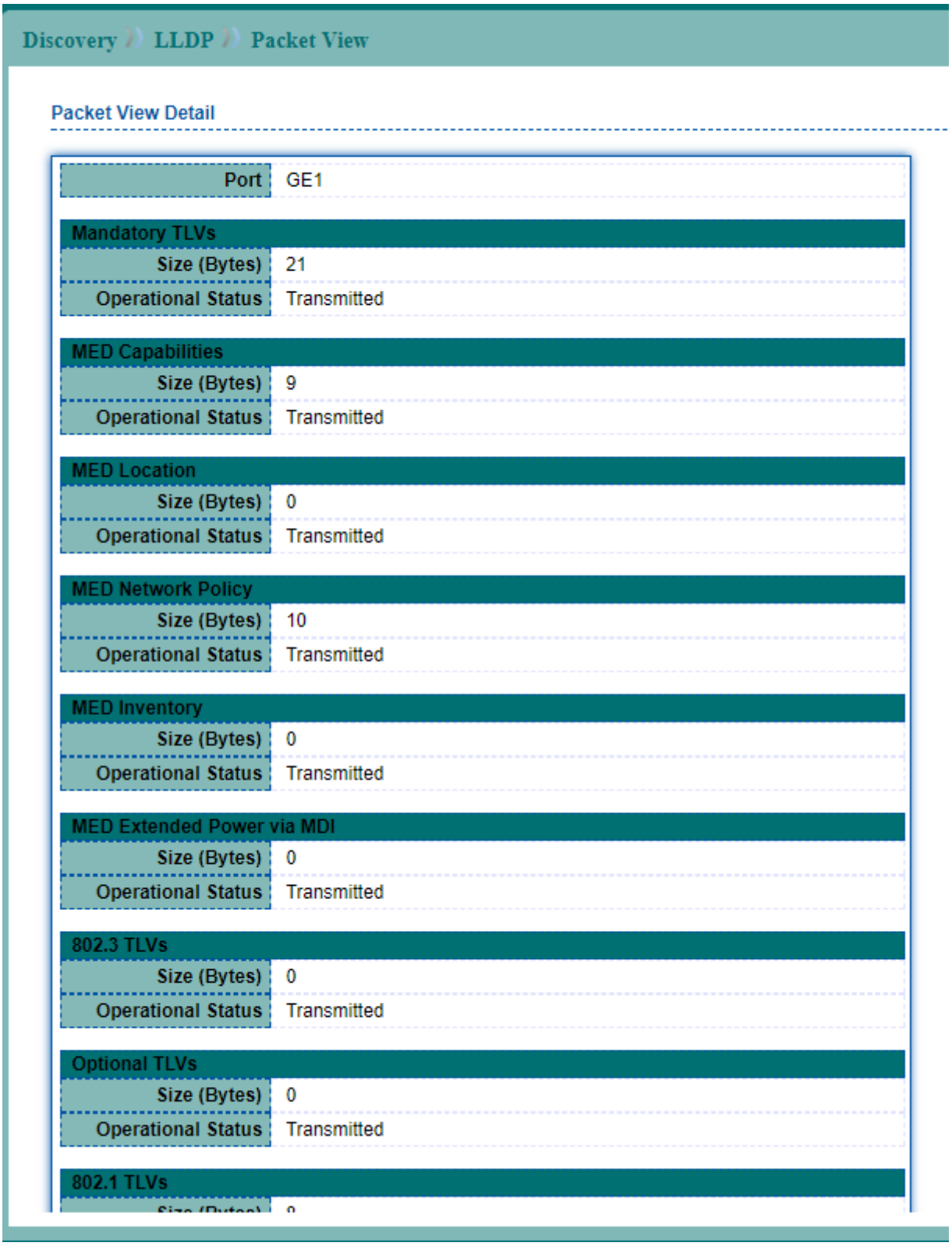


Figure 10-9 Detail LLDP Packet View page

Field	Description
In-Use(Bytes)	Total in-used size
Available(Bytes)	Remain available size
Operational Status	Indicate if over loading is happen

Table 10-5 LLDP Local Information fields

10.6 LLDP Local Information

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

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

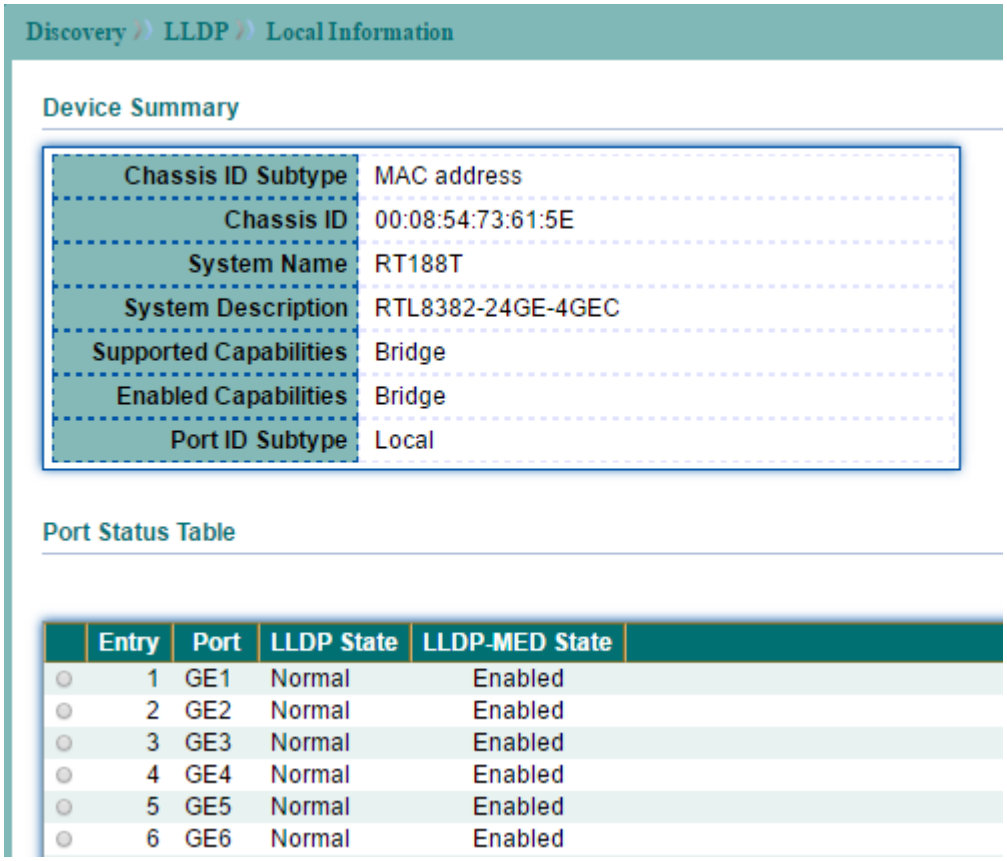


Figure 10-10 LLDP Local Information page

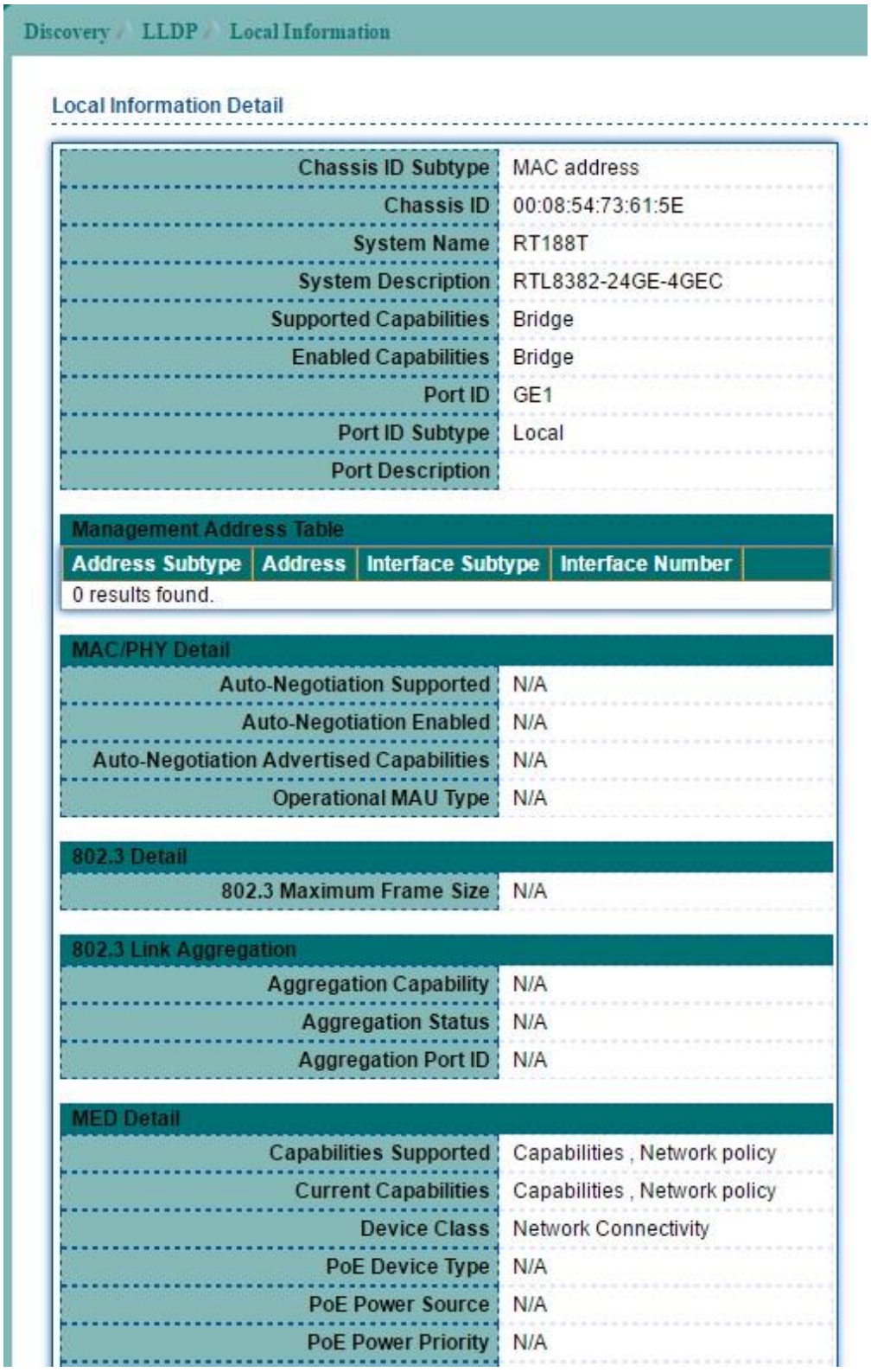


Figure 10-11 LLDP Local Information Detail page

Field	Description
Chassis ID Subtype	Type of chassis ID, such as the MAC address.
Chassis ID	Identifier of chassis. Where the chassis ID subtype is a MAC address, the MAC address of the switch is displayed.
System Name	Name of switch.
System Description	Description of the switch.

Supported Capabilities	Primary functions of the device, such as Bridge, WLAN AP, or Router.
Enabled Capabilities	Primary enabled functions of the device.
Port ID Subtype	Type of the port identifier that is shown.
LLDP State	LLDP Tx and Rx abilities.
LLDP Med State	LLDP MED enable state.

Table 10-6 LLDP Local Information fields

10.7 LLDP Neighbor

To display LLDP Neighbor Devices, click **Discovery** > **LLDP** > **Neighbor.**

Click "Detail" to view selected neighbor detail information.

Figure 10-12 LLDP Neighbor page

Field	Description
Local Port	Number of the local port to which the neighbor is connected.
Chassis ID Subtype	Type of chassis ID (for example, MAC address).
Chassis ID	Identifier of the 802 LAN neighboring device's chassis.
Port ID Subtype	Type of the port identifier that is shown.
Port ID	Identifier of port.
System Name	Published name of the switch.
Time to Live	Time interval in seconds after which the information for this neighbor is deleted.

Table 10-7 LLDP Neighbor fields

10.8 LLDP Statistics

To display LLDP Statistics, click **Discovery** > **LLDP** > **Statistics.**

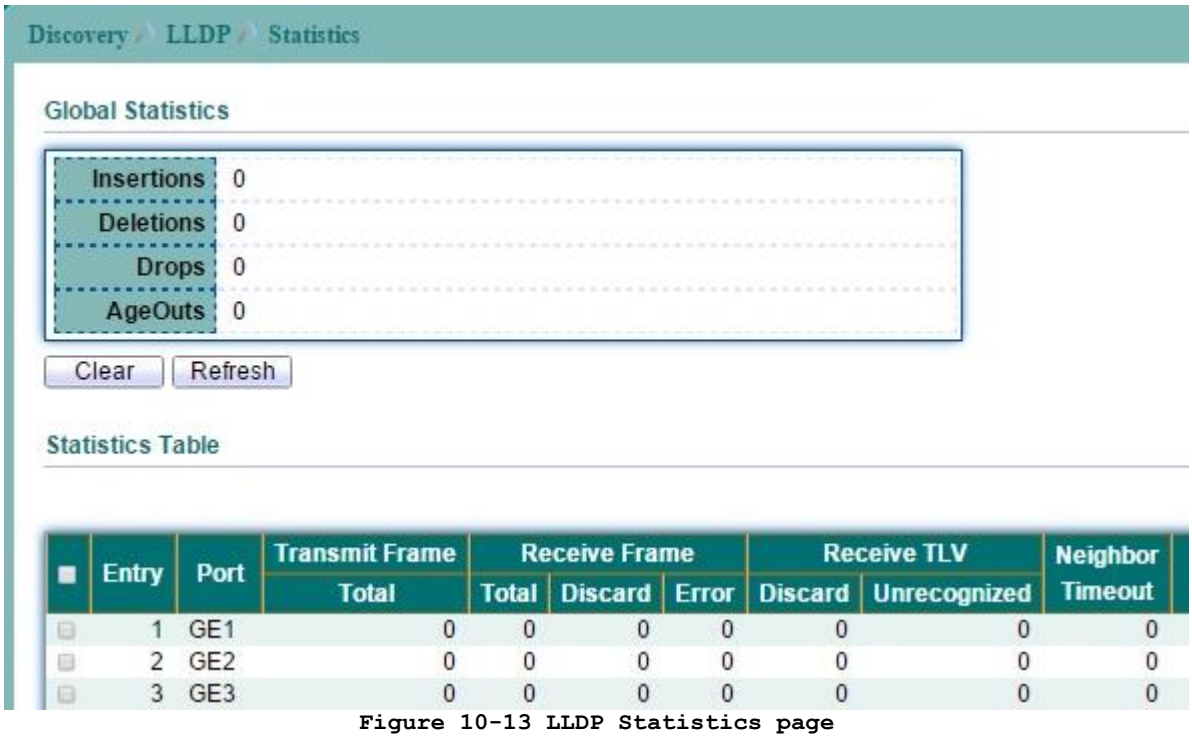


Figure 10-13 LLDP Statistics page

Field	Description
Insertions	Total number of neighbors that already insert per system
Deletions	Total number of neighbors that already delete per system
Drops	Total number of neighbors that already drop per system
AgeOuts	Total number of neighbors that already timeout per system
Port	Port number.
Transmit Frame Total	Total number of transmitted LLDP frame.
Receive Frame Total	Total number of received LLDP frame.
Receive Frame Discard	Total number of discard LLDP frame ever received.
Receive Frame Error	Total number of error LLDP frame ever received.
Receive TLV Discard	Total number of discard TLVs in received LLDP frame.
Receive TLV Unrecognized	Total number of unrecognized TLVs in received LLDP frame.
Neighbor Timeout	Total number of neighbors that already timeout per port

Table 10-8 LLDP Statistics fields

11 Multicast

11.1 General

11.1.1 Multicast Property

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

This page allow user to set multicast forwarding method and unknown multicast action.

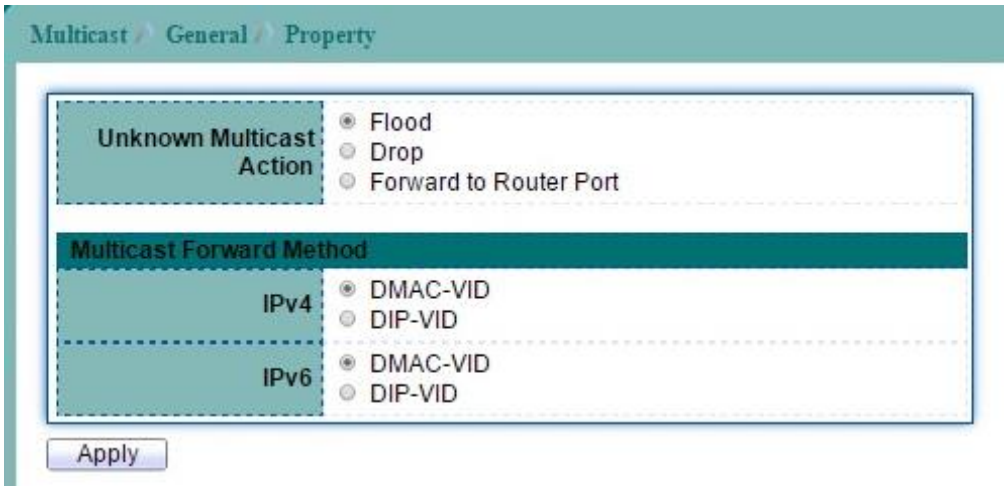


Figure 11-1 Multicast Property page

Field	Description
Unknown Multicast Action	Set the unknown multicast action ● **Flood:** flood the unknown multicast data. ● **Drop:** drop the unknown multicast data. ● **Forward Router port:** forward the unknown multicast data to router port.
Multicast Forward Method	
IPv4	Set the ipv4 multicast forward method. ● **DMA-VID (MAC):** forward method dmac+vid. ● **DIP-VID (Src-Dst-Ip):** forward method dip+sip.
IPv6	Set the ipv6 multicast forward method. ● **DMA-VID (MAC):** forward method dmac+vid. ● **DIP-VID (Src-Dst-Ip):** forward method dip+sip(dip low 32 bit, sip low 24bit + 40~47bit).

Table 11-1 Multicast Property fields

11.1.2 Multicast Group Address

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

This page allow user to browse all IGMP snooping groups that dynamic learned or statically added. Also allows user to add, edit or delete static group for IGMP snooping.

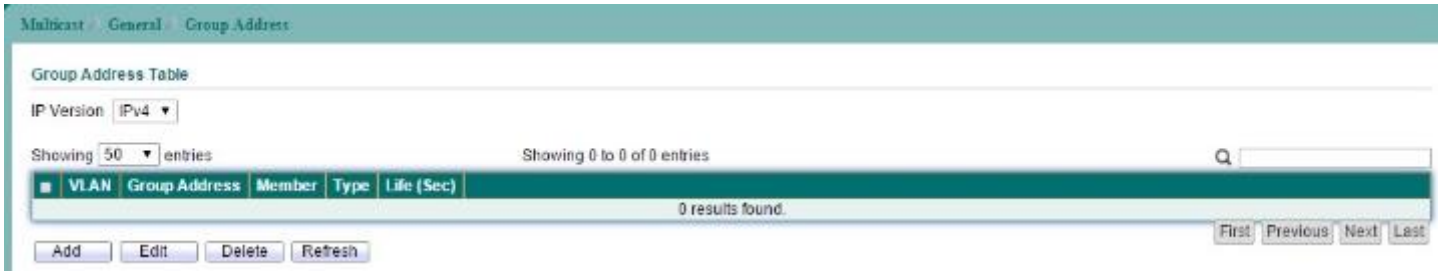


Figure 11-2 Multicast Group Address page

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

Table 11-2 Multicast Group Address fields

Click "Add" button to add a static multicast group.

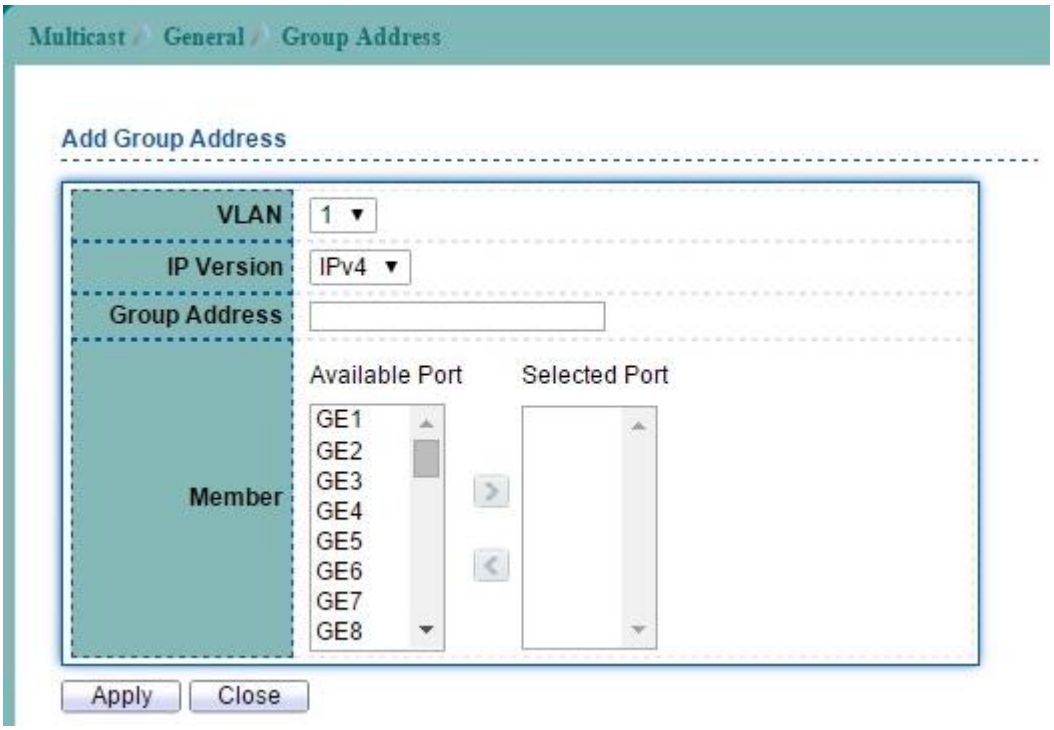


Figure 11-3 Add Multicast Group Address page

Field	Description
VLAN	Select the VLANs ID to configure.
IP Version	Group IP Address of IPv4 or IPv6.
Group Address	The multicast IP address of this group.

Member	The member ports of this group.

Table 11-2 Add Multicast Group Address fields

11.1.3 Multicast Router Port

To display Multicast Router Setting web page, click **Multicast** > **General** > **Router Port**.

This page allow user to browse all router information of IGMP Snooping. And also allows user to add, edit or delete static and forbidden router port on specific VLANs.

Figure 11-4 Multicast Router Port page

Field	Description
VLAN	The VLAN that router port belong to.
Member	The member ports.
Static Port	**Static Port:** All packets that need sent to router will forward to this port.
Forbidden Port	**Forbidden Port:** All packets that need sent to router will NOT forward to this port.
Life (Sec)	The expiry time of the router port.

Table 11-3 Multicast Router Port fields

Click "Add" button to configure new Multicast Router Port entry.

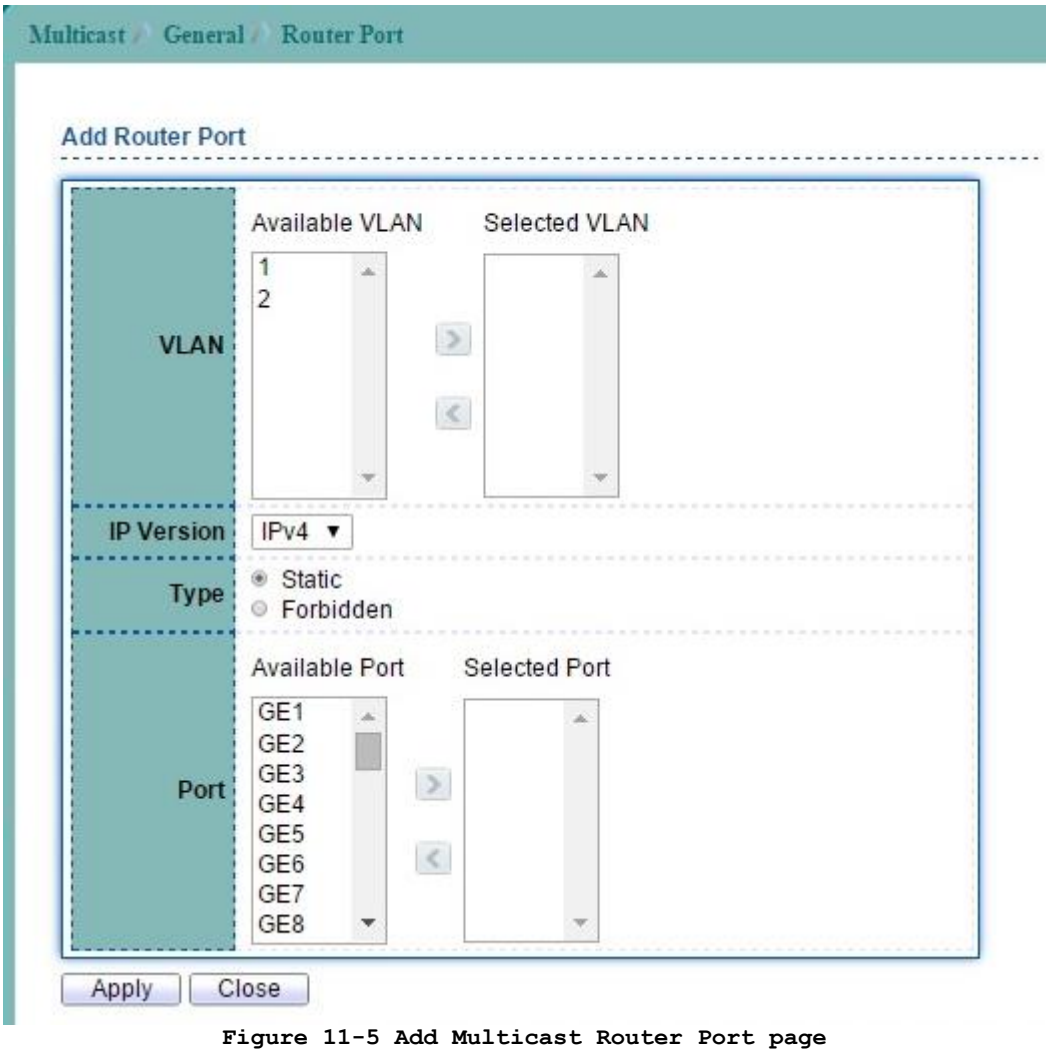


Figure 11-5 Add Multicast Router Port page

Field	Description
VLAN	The VLAN ID for router setting.
IP Version	IP version: IPv4 or IPv6
Type	The router port type ● **Static:** All packets that need sent to router will forward to this port. ● **Forbidden:** All packets that need sent to router will NOT forward to this port.
Port	The member ports.

Table 11-4 Add Multicast Router Port fields

11.1.4 Multicast Forward All

To display IGMP Forward All web page, click **Multicast** > **General** > **Forward All**.

This page allow user to configure all port forwarding status on specified VLAN of IGMP Snooping.

Figure 11-6 Multicast Forward All page

Field	Description
VLAN	The VLAN Create by user.
Static Port	All packets that on specified VLAN will forward to this port.
Forbidden Port	All packets that on specified VLAN will NOT forward to this port.

Table 11-5 Multicast Forward All Fields

Click "Add" button to create a new Forward All entry.

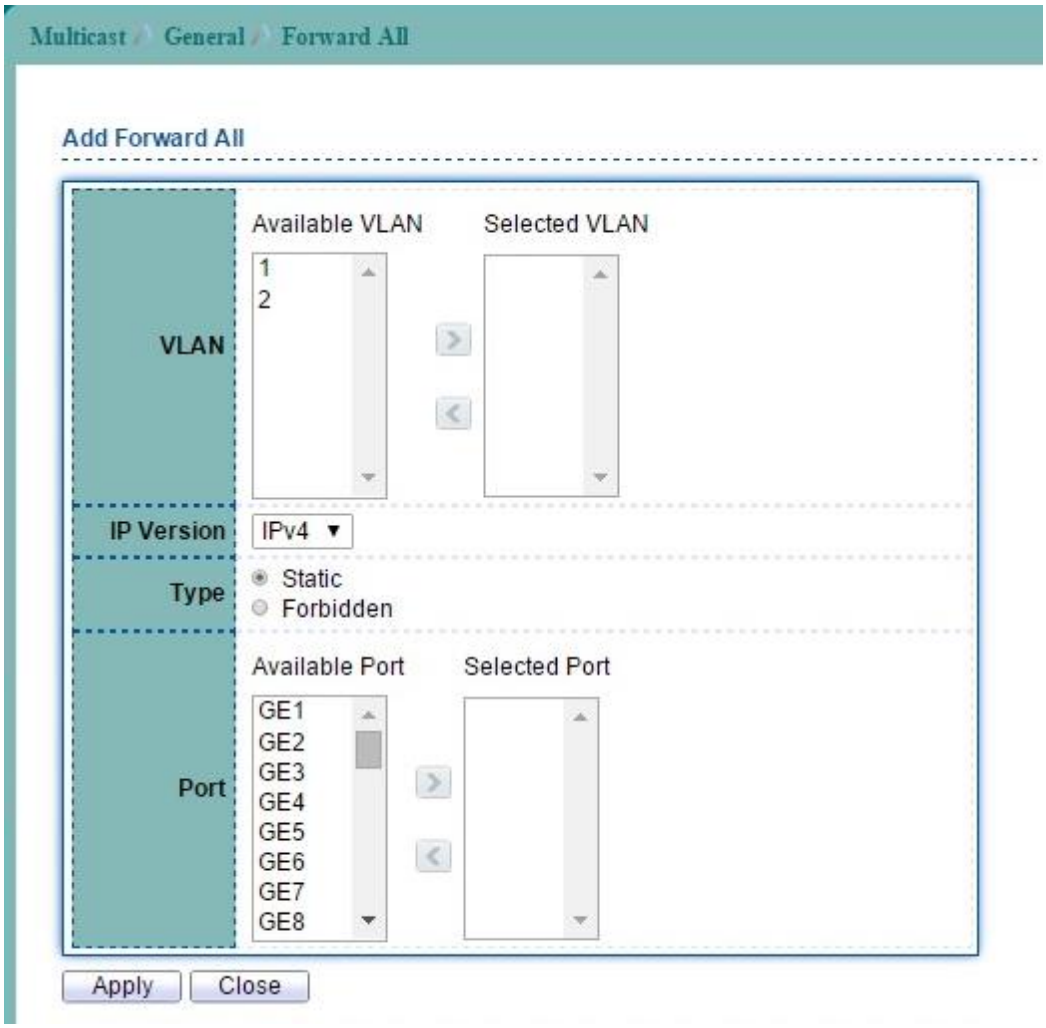


Figure 11-7 Add Multicast Forward All page

Field	Description
VLAN	The VLAN Create by user.
IP Version	IP version: IPv4 or IPv6
Type	The router port type ● Static: all packets that need sent to router will forward to this port. ● Forbidden: all packets that need sent to router will NOT forward to this port.
Port	Port or Ports that will be added to the forward all session.

Table 11-6 Add Multicast Forward All fields

11.1.5 Multicast Throttling

To display multicast max-groups number and action setting web page, click **Multicast** > **General** > **Throttling**.

This page allow user to configure all port forwarding status on specified VLAN of IGMP Snooping.

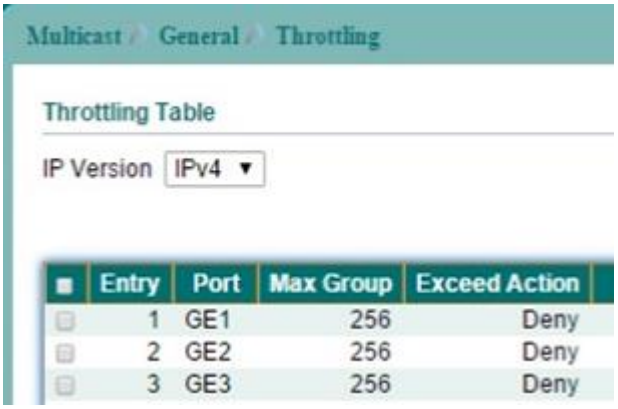


Figure 11-8 Multicast Throttling page

Select entry and click "Edit" button to configure Multicast Throttling entry.

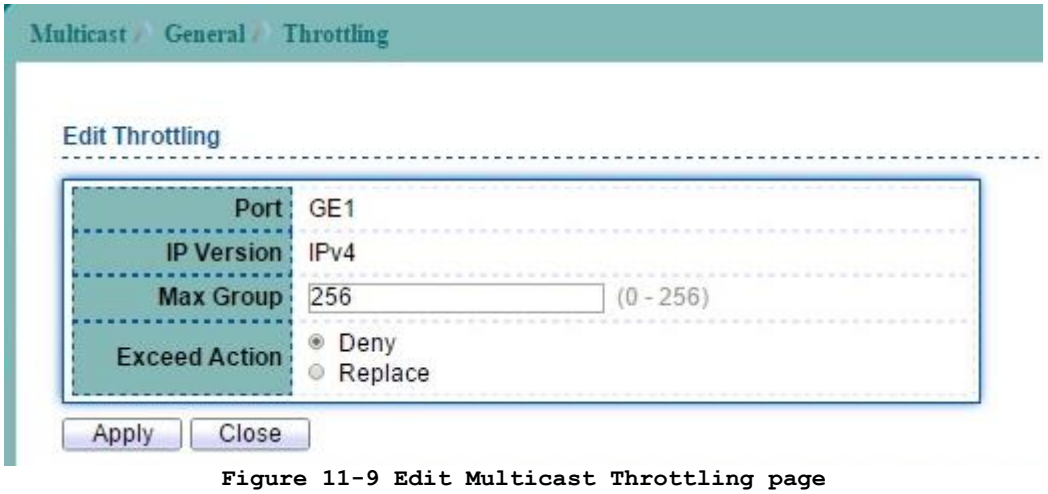


Figure 11-9 Edit Multicast Throttling page

Field	Description
Port	Selected port or ports.
IP Type	Ipv4 for IGMP snooping max groups setting.
Max Groups	Max number of group for port.
Exceed Action	Excess Max number of group action. • **Deny:** do not learning group. • **Replace:** random replace one exist group.

Table 11-7 Edit Multicast Throttling fields

11.1.6 Multicast Filtering Profile

To display Multicast Profile Setting web page, click **Multicast** > **General** > **Filtering Profile**.

This page allow user to add, edit or delete profile for IGMP or MLD snooping.

Figure 11-10 Multicast Filtering Profile page

Click "Add" button to add a multicast filtering profile.

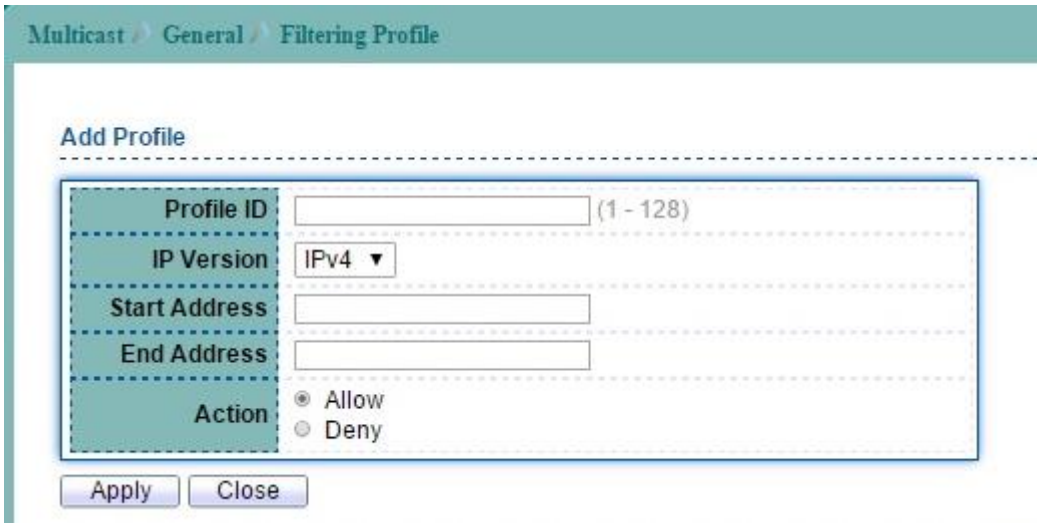


Figure 11-11 Add Multicast Filtering Profile page

Field	Description
Profile ID	Index of profile to set.
IP Version	IP type: ● **IPv4**: IGMP snooping profile. ● **IPv6**: MLD snooping profile.
Start Address	The range group ipv4 or ipv6 address of from.
End Address	The range group ipv4 or ipv6 address of to.
Action	The action of profile: ● **Allow**: permit all packets that match the profile. ● **Deny**: deny all packets that match the profile.

Table 11-8 Multicast Filtering Profile fields

11.1.7 Multicast Filtering Binding

To display Multicast Filtering Binding Setting web page, click **Multicast** > **General** > **Filtering Binding** > **IGMP** Filter Setting.

This page allow user to bind/remove profile to/from each port of IGMP snooping.

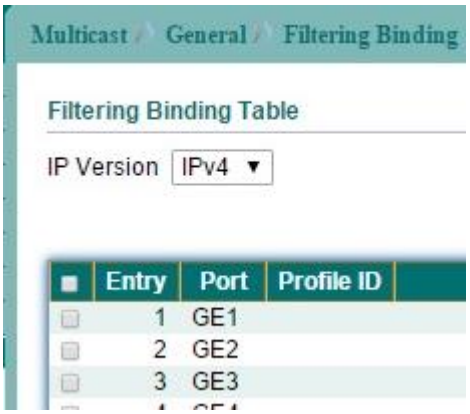


Figure 11-12 Multicast Filtering Binding page

Select entry and click "Edit" button to configure Multicast Filtering Binding entry.

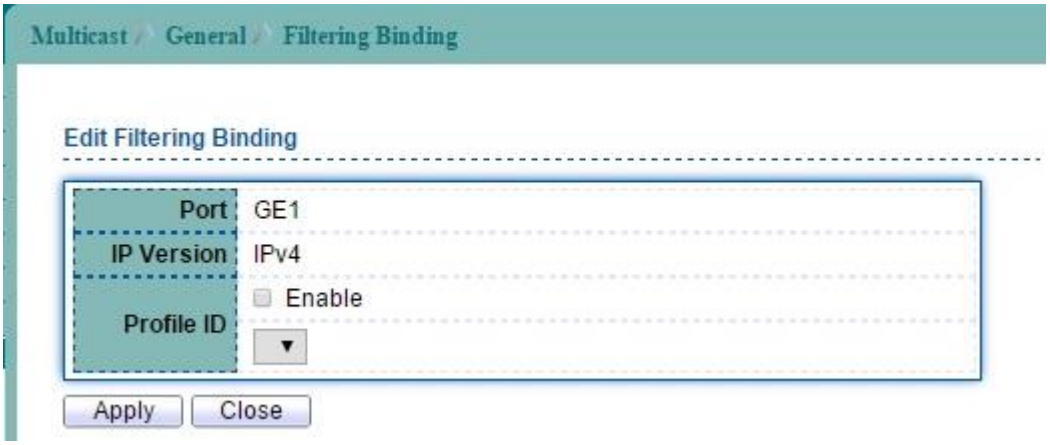


Figure 11-13 Edit Multicast Filtering Binding page

Field	Description
Port	Selected ports to configure
IP Version	IP type: ● **IPv4**: IGMP snooping profile. ● **IPv6**: MLD snooping profile.
Filter profile ID	Profile index.

Table 11-9 Multicast Filter Binding fields

11.2 IGMP Snooping

11.2.1 IGMP Property

To display IGMPVLAN Setting webpage, click **Multicast** > **IGMP Snooping** > **Property**.

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

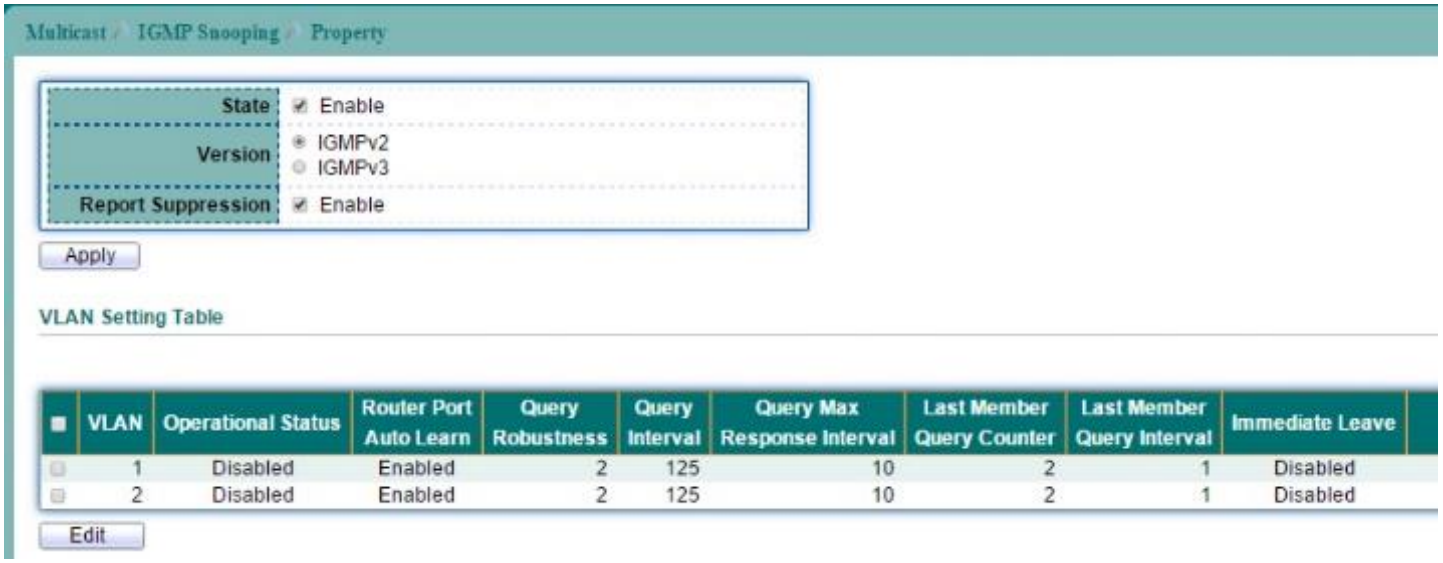


Figure 11-14 IGMP Snooping Property page

Field	Description
State	Set the enabling status of IGMP functionality ● **Enable:** Enable IGMP Snooping.
Version	Set the IGMP snooping version ● **v2:** Only support process IGMP v2 packet. ● **v3:** Support v3 basic and v2.
Report Suppression	Set the enabling status of IGMP v2 report suppression ● **Enable:** Enable IGMP Snooping v2 report suppression. ● **Disable:** Disable IGMP Snooping v2 report suppression.
VLAN Setting Table	
Entry No	The IGMP entry number.
VLAN	The IGMP entry VLAN ID
Operation Status	The enable status of IGMP VLAN functionality. ● **Enabled:** when IGMP Snooping enable and IGMP VLAN enable and multicast filtering enable. ● **Disabled:** when IGMP Snooping disable or IGMP VLAN disable or multicast filtering disable.
Router Ports Auto Learn	Set the enabling status of IGMP router port learning ● **Enabled:** Enable learning router port by query and PIM, DVRMP. ● **Disabled:** Disable learning dynamic router port.
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 Counter	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	Leave the group when receive IGMP Leave message. Enabled: Enable Fastleave. Disabled: Disable Fastleave.

Table 11-10 IGMP Snooping Property fields

Select entry and click "Edit" button to configure IGMP Snooping VLAN Setting entry.

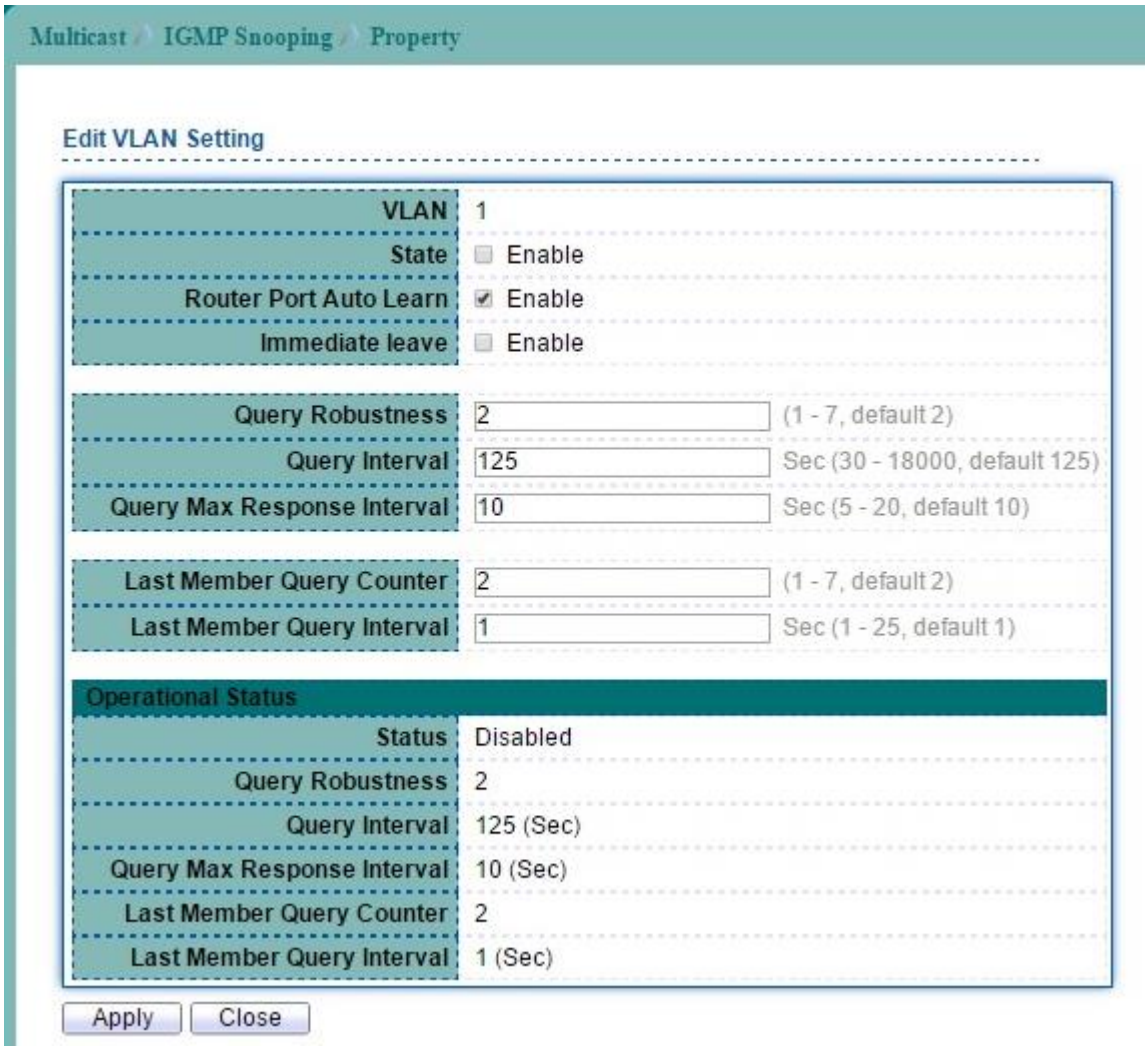


Figure 11-15 Edit IGMP Snooping Property page

Field	Description
VLAN	The IGMP VLAN ID.
State	The admin enable status of IGMP VLAN functionality ● **Enabled:** IGMP VLAN enabled. ● **Disabled:** IGMP VLAN disabled.
Router Ports Auto Learn	Set the enabling status of IGMP router port learning: ● **Enable:** Enable learning router port by query and PIM, DVRMP. ● **Disable:** Disable learning dynamic router port.
Immediate leave	Leave the group when receive IGMP Leave message. ● **Enable:** Enable Fast leave. ● **Disable:** Disable Fast leave.
Query Robustness	The Query Robustness variable allows tuning for the expected packet loss on a subnet.
Query Interval	The admin query interval.
Query Max Response Interval	The admin query max response interval.
Last Member Query counter	The operating last member query count.
Last Member Query Interval	The admin last member query interval.

Table 11-11 Edit IGMP Snooping Property fields

11.2.2 IGMP Querier Setting

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

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

Figure 11-16 IGMP Snooping Querier page

Select entry and click "Edit" button to configure IGMP Snooping Querier entry.

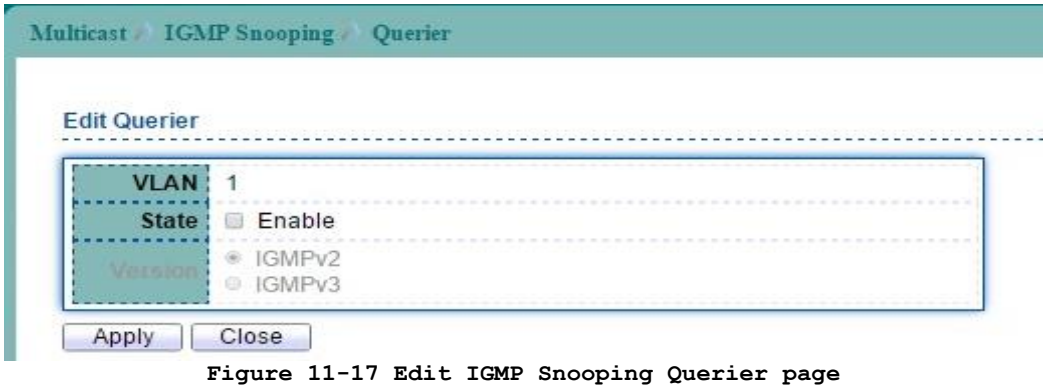


Figure 11-17 Edit IGMP Snooping Querier page

Field	Description
VLAN	Select the VLANs to configure.
State	Set the enabling status of IGMP Querier Election on the chose VLANs. ● Enabled: Enable IGMP Querier. ● Disabled: Disable IGMP Querier.
Operation Status	The enable status of IGMP VLAN functionality. ● Enabled: when IGMP Snooping enable and IGMP VLAN enable and multicast filtering enable. ● Disabled: when IGMP Snooping disable or IGMP VLAN disable or multicast filtering disable.
Querier Version	Set the query version of IGMP Querier Election on the chose VLANs. ● v2: Querier version 2. ● v3: Querier version 3.
Querier Address	The real Querier IP address on the VLAN.

Table 11-12 IGMP Snooping Querier fields

11.2.3 IGMP Snooping Statistics

To display IGMP Snooping Statistic web page, click **Multicast** > **IGMP Snooping** > **Statistics**.

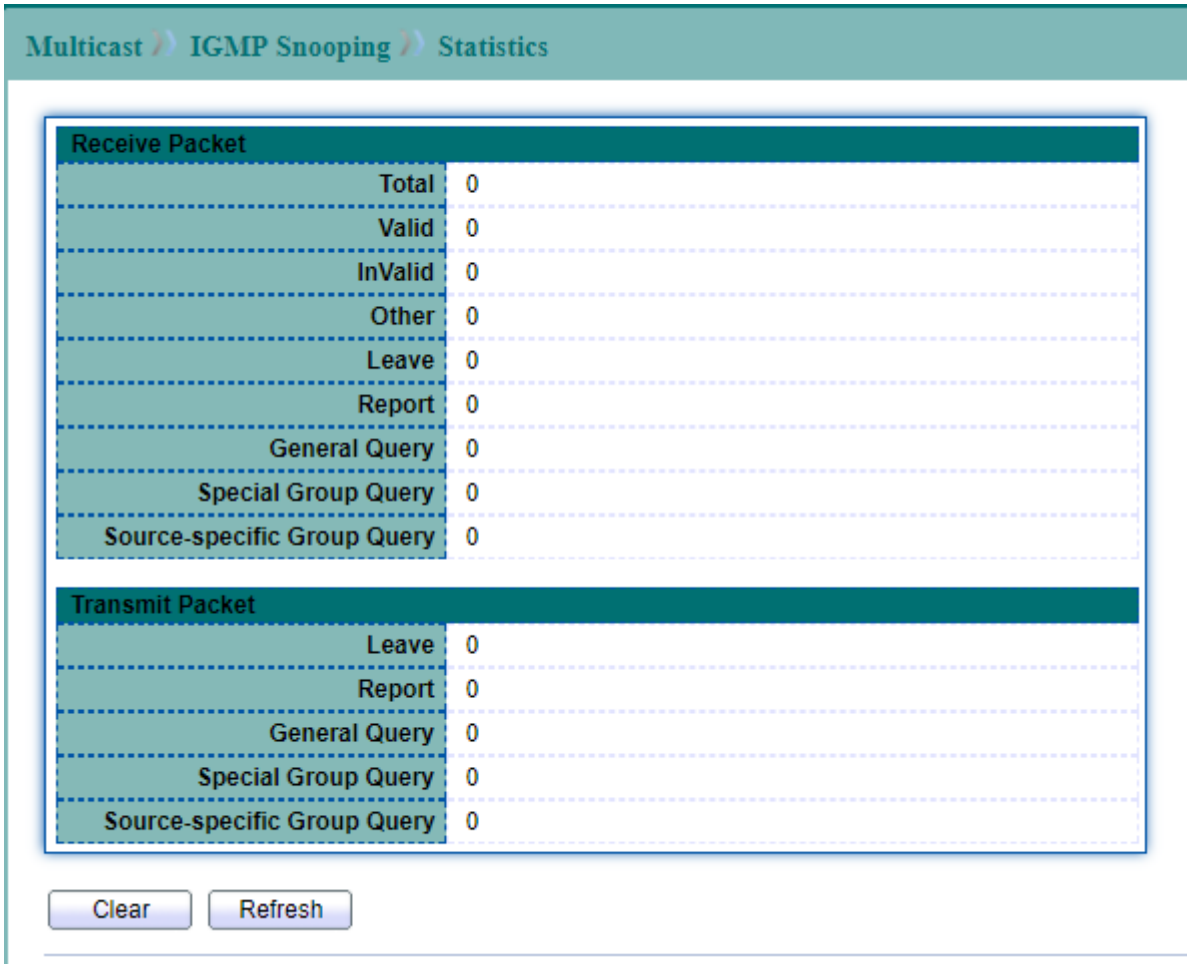


Figure 11-18 IGMP Snooping Statistics page

11.3 MLD Snooping

11.3.1 MLD Snooping Property

To display MLDVLAN Setting webpage, click **Multicast** > **MLD Snooping** > **Property**.

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

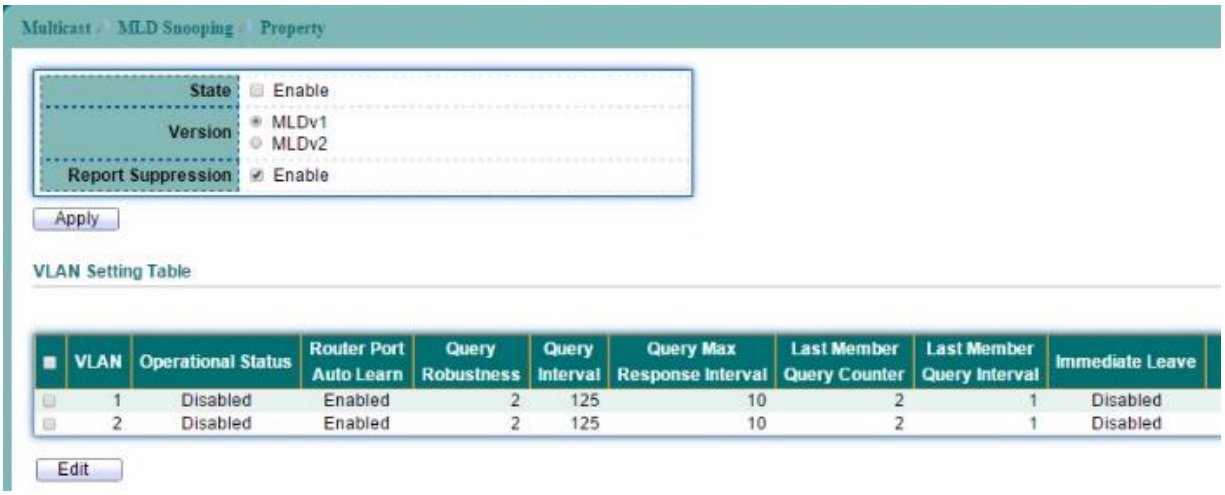


Figure 11-19 MLD Snooping Property page

Field	Description
MLD Snooping State	Set the enabling status of ,MLD functionality ● **Enable:** Enable MLD Snooping. ● **Disable:** Disable MLD Snooping.
Version	Set the MLD snooping version ● **v1:** Only support process MLD v1 packet. ● **v2:** Support v2 basic and v1.
Snooping Report Suppression	Set the enabling status of MLD v2 report suppression ● **Enable:** Enable MLD Snooping v1 report suppression. ● **Disable:** Disable MLD Snooping v1 report suppression.
VLAN Setting Table	
Entry No	The MLD entry number.
VLAN	The MLD entry VLAN ID.
Operation Status	The enable status of MLD VLAN functionality ● **Enabled:** when MLD Snooping enable and MLD VLAN enable and multicast filtering enable. ● **Disabled:** when MLD Snooping disable or MLD VLAN disable.
Router Ports Auto Learn	Set the enabling status of MLD router port learning ● **Enabled:** Enable learning router port by query and PIM, DVRMP. ● **Disabled:** Disable learning dynamic router port.
Query Robustness	The Query Robustness allows tuning for the expected packet loss on a subnet.
Query Interval	The interval of querier 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 Counter	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	Leave the group when receive MLD Leave message. ● **Enabled:** Enable Fastleave. ● **Disabled:** Disable Fastleave.

Table 11-13 MLD Snooping Property fields

Select entry and click "Edit" button to configure MLD Snooping VLAN Setting entry.

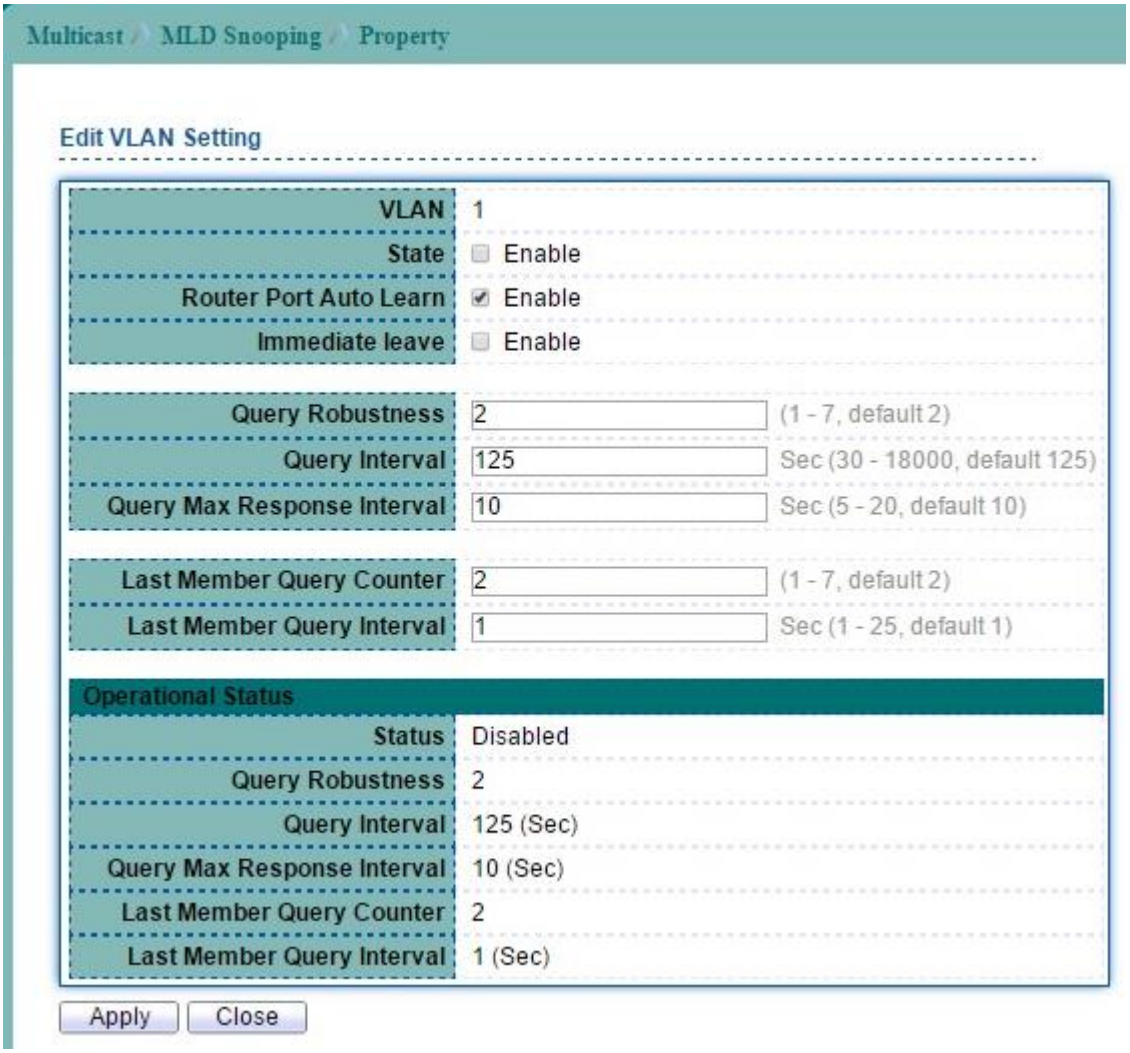


Figure 11-20 Edit MLD Snooping Property page

Field	Description
VLAN	The MLD VLAN ID
State	The admin enable status of MLD VLAN functionality ● **Enabled:** MLD VLAN enable. ● **Disabled:** MLD VLAN disable.
Router Ports Auto Learn	Set the enabling status of MLD router port learning ● **Enabled:** Enable learning router port by query and PIM, DVRMP. ● **Disabled:** Disable learning dynamic router port.
Immediate leave	Leave the group when receive MLD Leave message. ● **Enabled:** Enable Fast leave. ● **Disabled:** Disable Fast leave.
Query Robustness	The Query Robustness allows tuning for the expected packet loss on a subnet.
Query Interval	The query interval.
Query Max Response Interval	The query max response interval.
Last Member Query Counter	The last member query count.
Last Member Query Interval	The last member query interval.

Table 11-14 Edit MLD Snooping Property fields

11.3.2 MLD Snooping Statistics

To display MLD Snooping Statistic web page, click **Multicast** > **MLD Snooping** > **Statistics**.

Figure 11-21 MLD Snooping Statistics page

11.4 MVR

Multicast VLAN registration (MVR) allows a single multicast VLAN to be shared in the network while other subscribers remain in the different VLANS. MVR reduce the amount of bandwidth consumed by the same multicast traffic and makes multicast service become more efficiency.

11.4.1 MVR Property

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

This page allow user to configure MVR global function.

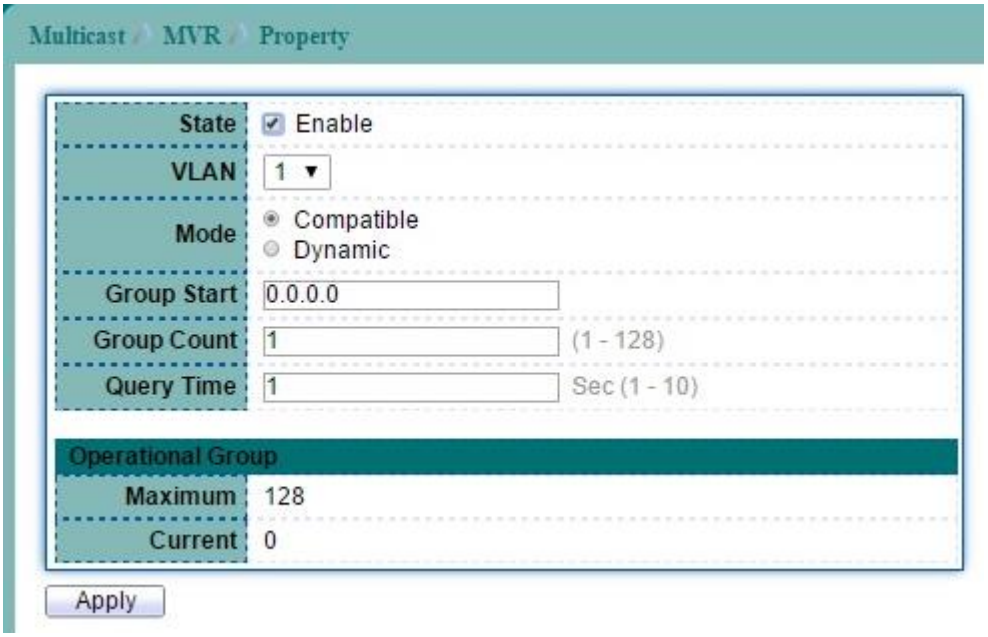


Figure 11-22 MVR Property page

Field	Description
State	To enable MVR on the switch.
VLAN	Select a VLAN in which multicast data is received; all source ports needs belong to this VLAN.
Mode	Specify group member mode. In Compatible mode, the group member only be receiver port. In Dynamic mode, the group member could be receiver port or source port.
Group	Group start address.
Group Count	Specifies the maximum number of MVR groups.
Query Time	Query response time

Table 11-15 MVR Property fields

11.4.2 MVR Port Setting

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

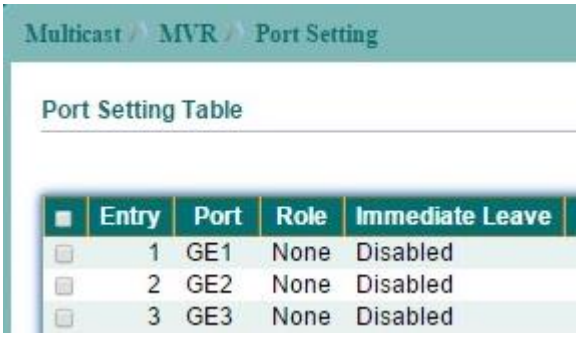


Figure 11-23 MVR Port Setting page

Select entry and click "Edit" button to configure MVR port setting entry.

Figure 11-24 Edit MVR Port Setting page

Field	Description
Port	Selected port.
Role	Select a Role for this port. ● **None:** MVR disabled on this port. ● **Receiver:** The subscriber port, it only receive multicast data. ● **Source:** The port that receives and send multicast data.
Immediate Leave	Enable immediate leave feature of MVR on the port. Immediate Leave should only apply to the Receiver port.

Table 11-16 MVR Port Setting fields

11.4.3 MVR Group Address

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

Figure 11-25 MVR Group Address page

Click "Add" button to create a new MVR Group Address entry.

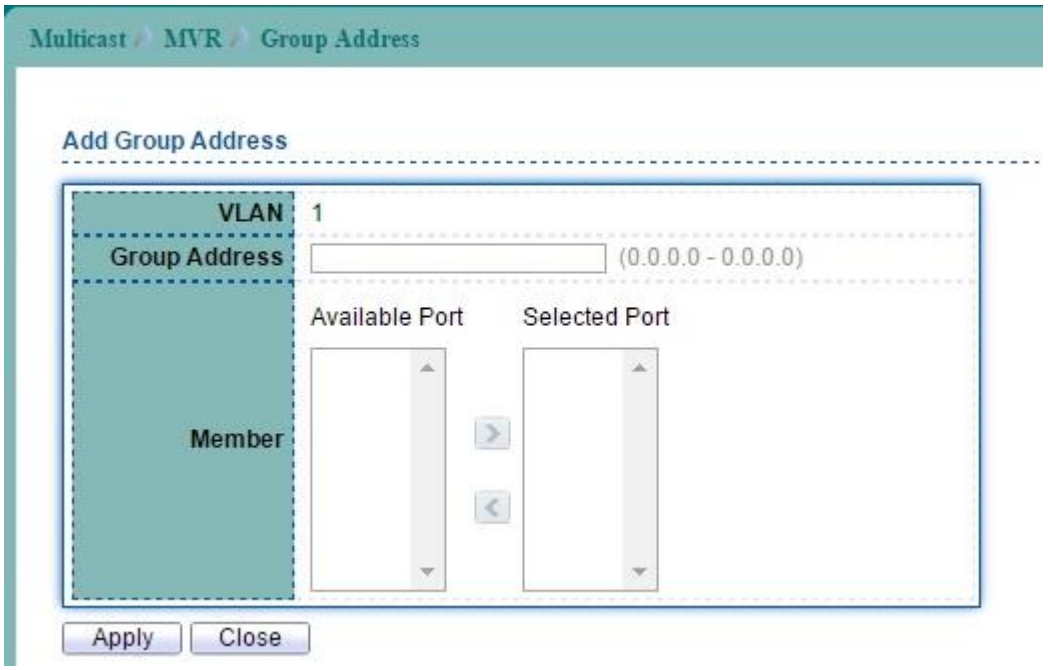


Figure 11-26 Add MVR Group Address page

Field	Description
VLAN	Selected VLAN.
Group Address	Entry the range of group multicast address.
Member	Specify the group member port(s).

Table 11-17 MVR Group Address fields

12 Security

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

12.1 RADIUS Server

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

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

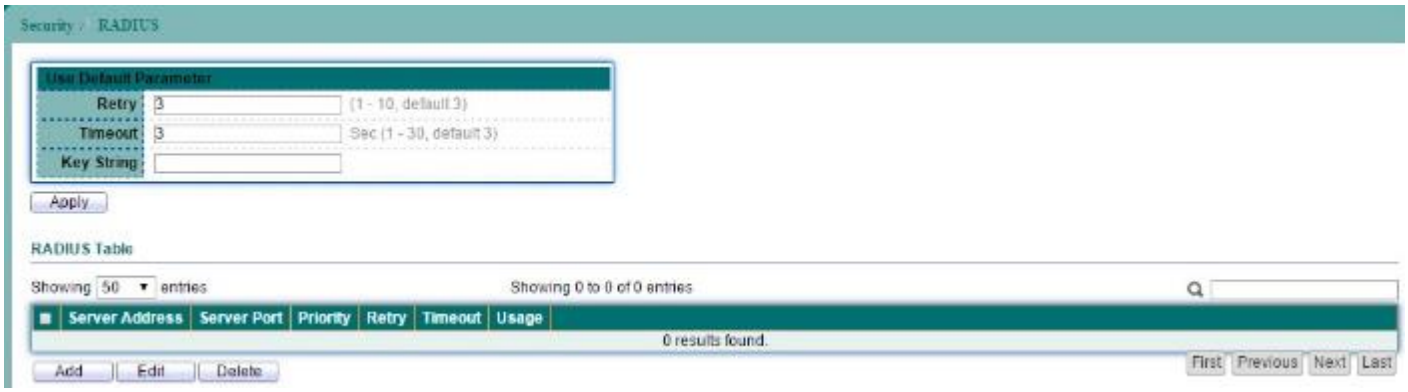


Figure 12-1 RADIUS Server page

Field	Description
Retry	RADIUS server default retry times.
Timeout	RADIUS server default timeout value.
Key String	RADIUS server default key string.

Table 12-1 RADIUS Server fields

Click "Add" button to create a new RADIUS server entry.

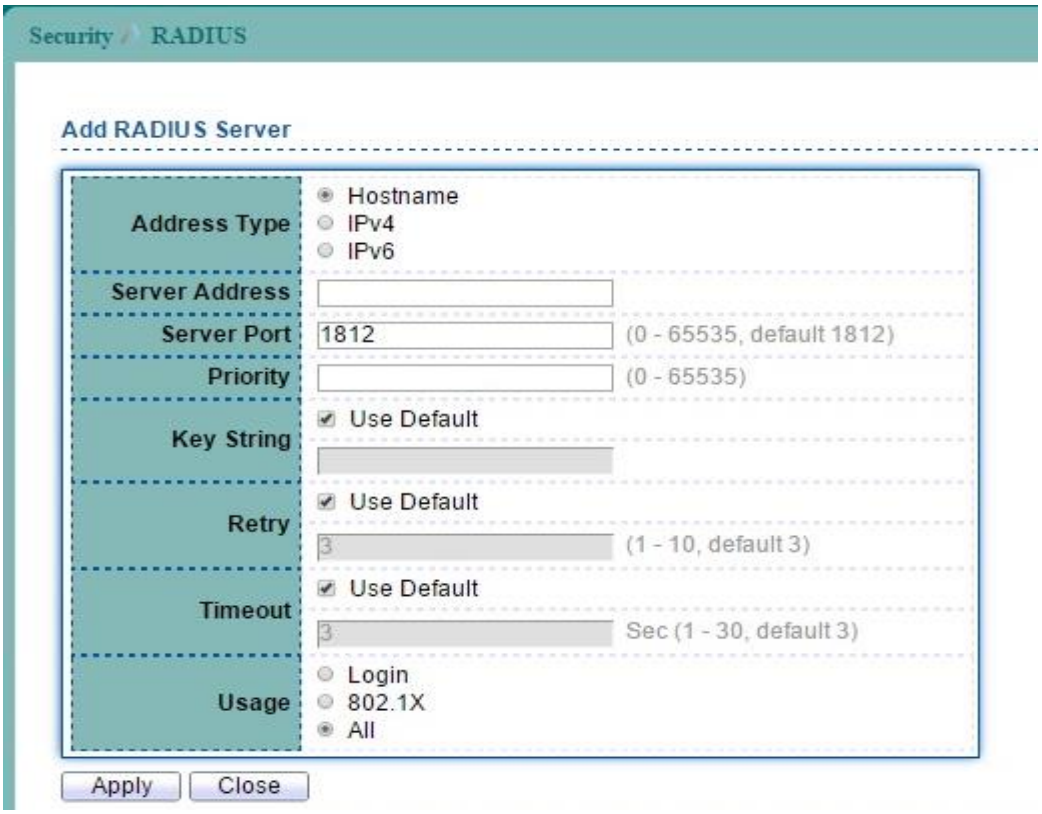


Figure 12-2 Add RADIUS Server page

Field	Description
Address Type	Server Address Type: ● **Host name:** Use host name as server address. ● **IPv4 address:** Use IPv4 address as server address. ● **IPv6 address:** Use IPv6 address as server address.
Server Address	RADIUS server IP address.
Server Port	RADIUS server UDP port for Authentication.
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.
Key String	RADIUS server key string.
Timeout for Reply	RADIUS server timeout value. If it is fail to connect to server, it will keep trying until timeout.
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 dead time of session.
Usage	RADIUS server usage type ● **Login:** For login authentication ● **802.1x:** For 802.1x authentication ● **All:** For all types

Table 12-2 Add RADIUS Server fields

12.2 TACACS+ Server

To display TACACS+ Server web page, click **Security** > **TACACS+**.

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

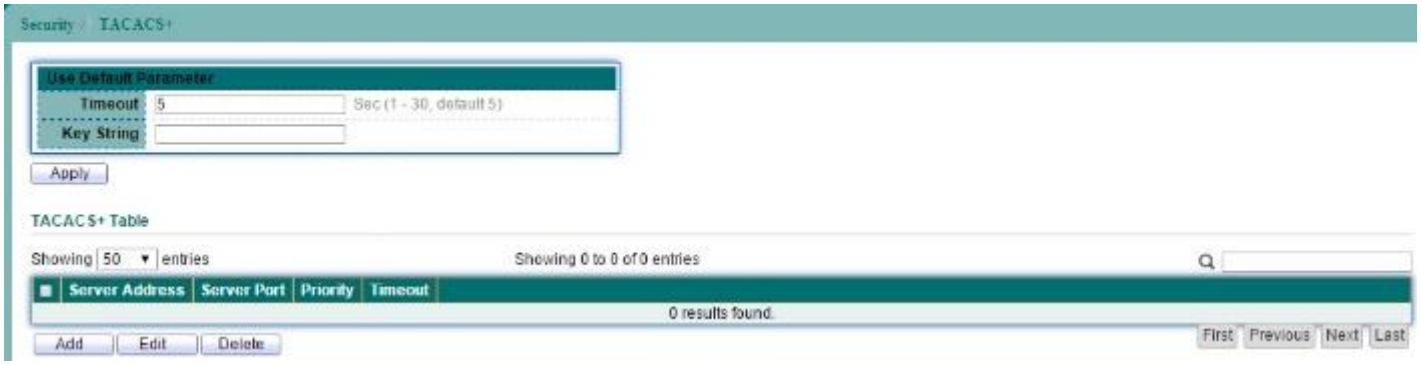


Figure 12-3 TACACS+ Server page

Field	Description
Timeout	TACACS+ server default timeout value.
Key String	TACACS+ server default key value.

Table 12-3 TACACS+ Server fields

Click "Add" button to create a new TACACS+ server entry.

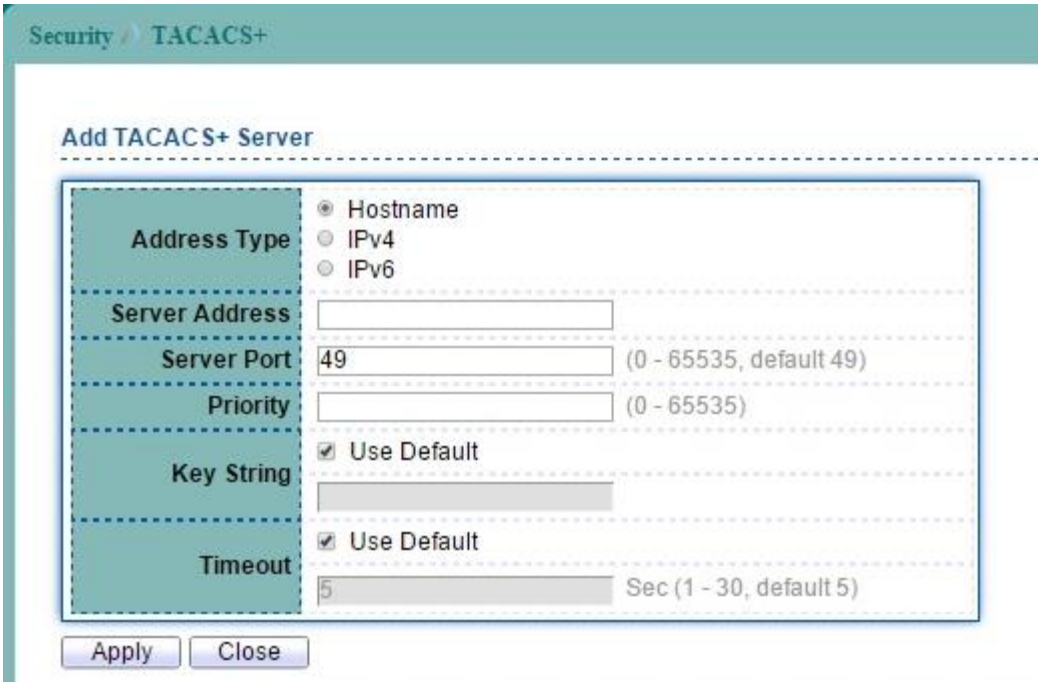


Figure 12-4 Add TACACS+ Server page

Field	Description
Address Type	Server Address Type • **Host name:** Use host name as server address. • **IPv4 address:** Use IPv4 address as server address. • **IPv6 address:** Use IPv6 address as server address.
Server Address	TACACS+ server IP address.
Server Port	TACACS+ server UDP port.
Priority	TACACS+ server priority (smaller value has higher priority). TACACS+ session will try to establish with the server setting which has highest priority. If failed, it will try to connect to the server with next higher priority.
Key String	TACACS+ server key value or use default parameter.
Timeout	TACACS+ server timeout value. If it is fail to connect to server, it will keep trying until timeout. Or use default parameter.

Table 12-4 Add TACACS+ Server fields

12.3 AAA

12.3.1 AAA Method List

To display Login List web page, click **Security** > **AAA** > **Method List.**

This page allow user to add, edit or delete login authentication list settings (The "default" list cannot be deleted.). The line combined to this list will authenticate login user by methods in this list. If the first method is failed, it will try to use the next priority method to authenticate if it exists.

With RADIUS and TACACS+ methods, the failed means connecting to server fail. With Local method, the failed means cannot find the user in local database.

Figure 12-5 AAA Method List page

Click "Add" button to create a new AAA Method List entry.

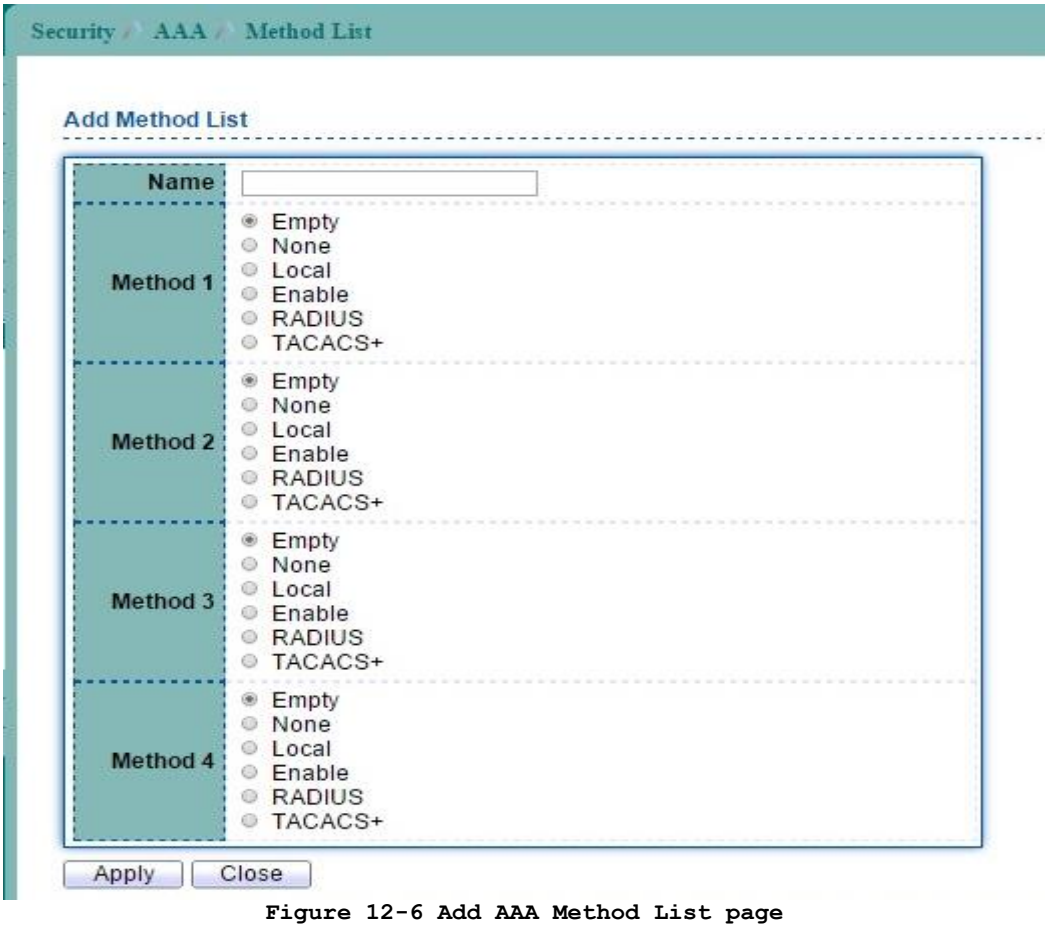


Figure 12-6 Add AAA Method List page

Field	Description
Name	New login authentication list name. This name should be different from other existing lists.
Method 1	Select first priority of login authentication method.

	• **Empty**: Function disabled. • **None**: Authenticated with any condition. • **Local**: Use local accounts database to authenticate • **Enable**: Use local enable password to authenticate. • **Radius**: Use remote Radius server to authenticate. • **TACACS+**: Use remote TACACS+ server to authenticate.
Method 2	Select first priority of login authentication method. • **Empty**: Function disabled. • **None**: Authenticated with any condition. • **Local**: Use local accounts database to authenticate • **Enable**: Use local enable password to authenticate. • **Radius**: Use remote Radius server to authenticate. • **TACACS+**: Use remote TACACS+ server to authenticate
Method 3	Select first priority of login authentication method. • **Empty**: Function disabled. • **None**: Authenticated with any condition. • **Local**: Use local accounts database to authenticate • **Enable**: Use local enable password to authenticate. • **Radius**: Use remote Radius server to authenticate. • **TACACS+**: Use remote TACACS+ server to authenticate
Method 4	Select first priority of login authentication method. • **Empty**: Function disabled. • **None**: Authenticated with any condition. • **Local**: Use local accounts database to authenticate • **Enable**: Use local enable password to authenticate. • **Radius**: Use remote Radius server to authenticate. • **TACACS+**: Use remote TACACS+ server to authenticate

Table 12-5 Add AAA Method List fields

12.3.2 AAA Login Authentication.

To display AAA Login Authentication web page, click **Security** > **AAA** > **Login Authentication**.

This page also allow user to select one of AAA Method lists to Console, Telnet, SSH, HTTP and HTTPS connections. The user accesses switch from those connections will be authenticated by AAA Method lists we created from "Method List" page.

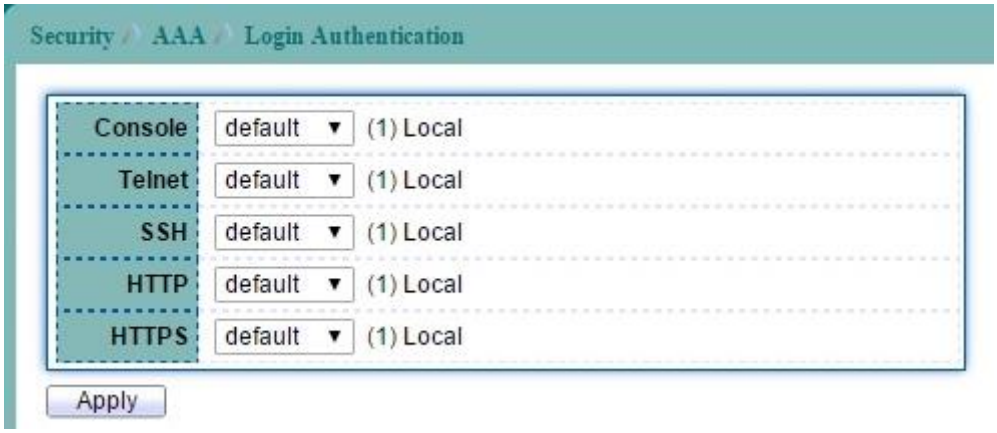


Figure 12-7 AAA Login Authentication page

Field	Description
Console	Login Authentication for Console connection.
Telnet	Login Authentication for Telnet connection.
SSH	Login Authentication for SSH connection.
HTTP	Login Authentication for HTTP connection.
HTTPS	Login Authentication for HTTPS connection.

Table 12-6 AAA Login Authentication fields

12.4 Management Access

12.4.1 Management VLAN

To display Management VLAN web page, click **Security** > **Management Access** > **Management VLAN.**

This page allow user to change management VLAN.

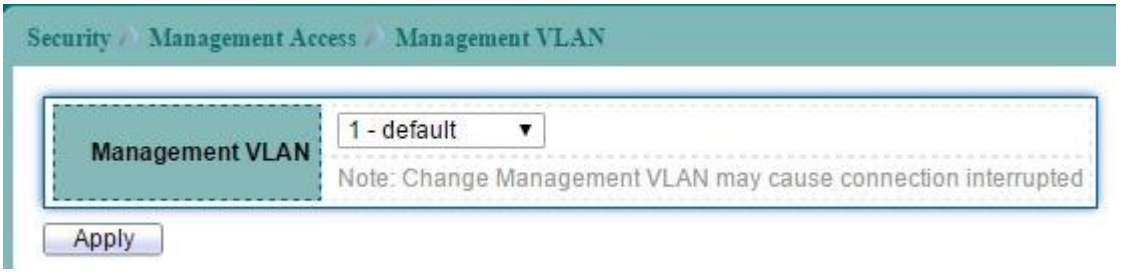


Figure 12-8 Management VLAN page

Field	Description
Management VLAN	Management connection, such as http, https, snmp etc.., has the same VLAN of management VLAN are allow connecting to device. Others will be dropped.

Table 12-7 Management VLAN fields

12.4.2 Management Service

To display Management Service web page, click **Security** > **Management Access** > **Management Service**.

This page allow user to configure Management Service setting.

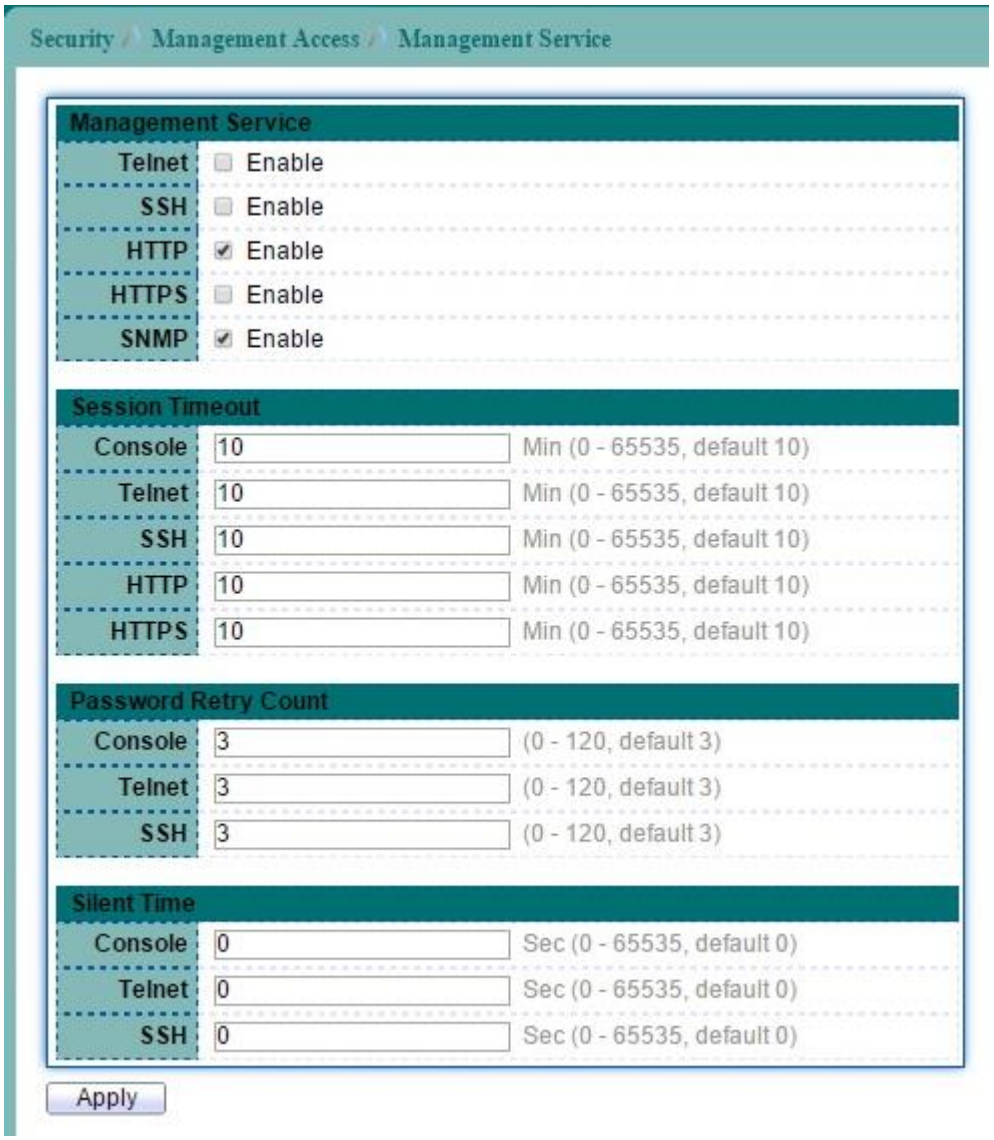


Figure 12-9 Management Service page

Field	Description
Management Service	
Telnet	Support Telnet Connection ● **Enable:** Enable Telnet service.
SSH	Support SSH Connection Enable: Enable SSH service.
HTTP	Support HTTP Connection ● **Enable:** Enable HTTP service.
HTTPS	Support HTTPS Connection Enable: Enable HTTPS service.
SNMP	Support SNMP Connection ● **Enable:** Enable SNMP service.
Session Timeout	
Console	Set session timeout minutes for user access CLI from console line. If user does not response after session

	timeout minute, CLI will logout automatically. 0 minutes means never timeout.
Telnet	Set session timeout minutes for user access CLI from Telnet connection. If user does not response after session timeout minute, CLI will logout automatically. 0 minutes means never timeout.
SSH	Set session timeout minutes for user access CLI from SSH connection. If user does not response after session timeout minute, CLI will logout automatically. 0 minutes means never timeout.
HTTP	Set session timeout minutes for user access CLI from HTTP connection. If user does not response after session timeout minute, WEBUI will logout automatically. 0 minutes means never timeout.
HTTPS	Set session timeout minutes for user access CLI from HTTPS connection. If user does not response after session timeout minute, WEBUI will logout automatically. 0 minutes means never timeout.
Password Retry Count	
Console	Set session timeout minutes for user access CLI from console line. If user does not response after session timeout minute, CLI will logout automatically. 0 minutes means never timeout.
Telnet	Set session timeout minutes for user access CLI from Telnet connection. If user does not response after session timeout minute, CLI will logout automatically. 0 minutes means never timeout.
SSH	Set session timeout minutes for user access CLI from SSH connection. If user does not response after session timeout minute, CLI will logout automatically. 0 minutes means never timeout.
Silent Time	
Console	After input error password exceeds password retry count, the CLI will freeze after silent time.
Telnet	After input error password exceeds password retry count, the Telnet will freeze after silent time.
SSH	After input error password exceeds password retry count, the SSH will freeze after silent time.

Table 12-8 Management Service fields

12.4.3 Management ACL

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

This page allow user to create, active or deactivate Management ACL profile. Only one profile can be active in device. All packets will be dropped if match deny rule or not match any permit rule.

Figure 12-10 Management ACL page

Field	Description
ACL Name	Input profile name. If the name is not existed, a new profile will be created. Or the rule will append to exist profile.

Table 12-9 Management ACL fields

12.4.4 Management ACE

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

This page allow user to add, edit or delete Management access profile rules. A profile could have many rules with different priority (1 is highest priority). Every profile must have unique name.

Figure 12-11 Management ACE page

Field	Description
ACL Name	Select a rule that created from Management ACL page, to add, edit or delete the rule.

Table 12-10 Management ACE fields

Click "Add" button to create a new ACE entry.

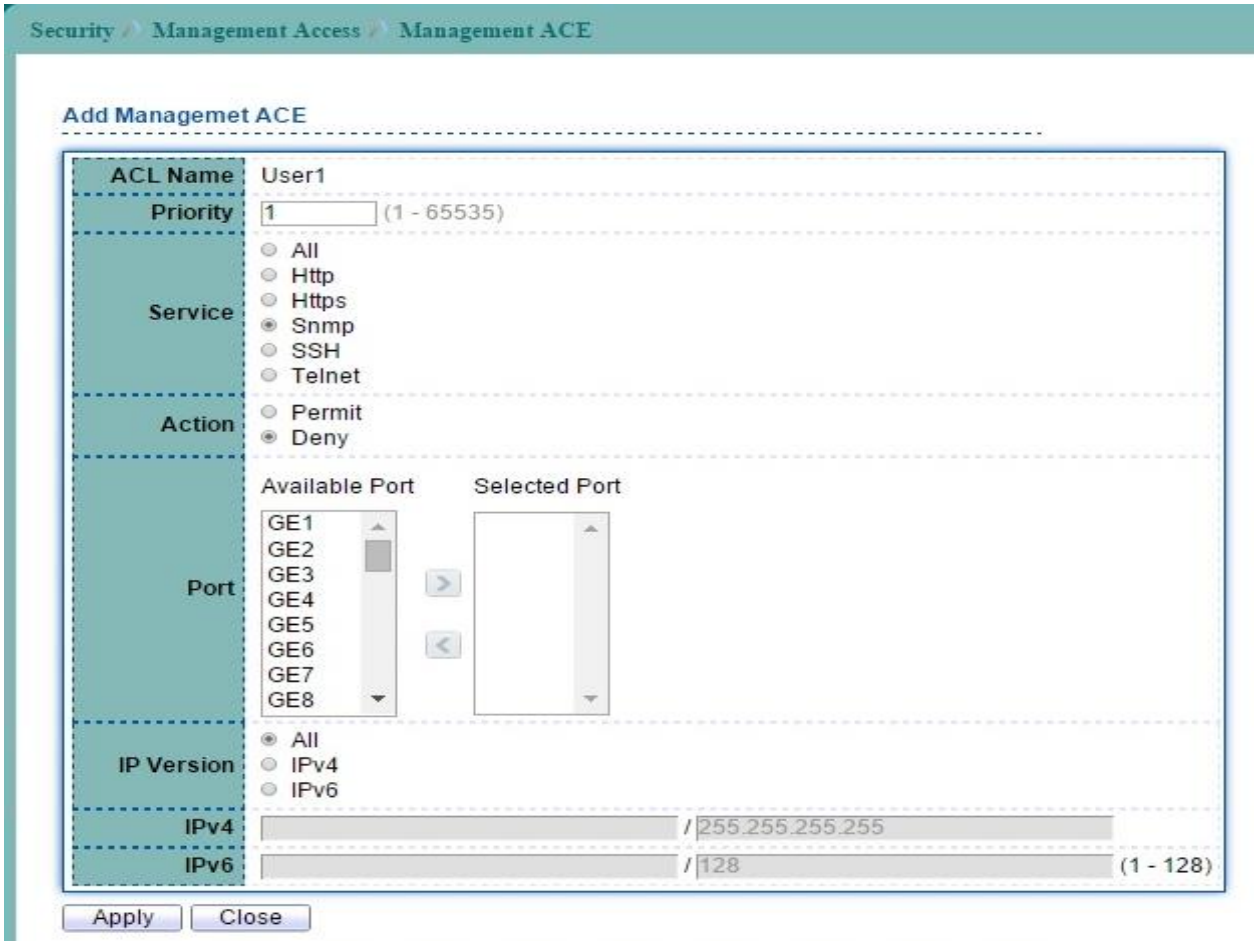


Figure 12-12 Add Management ACE page

Field	Description
ACL Name	Profile name.
Priority	Specify the priority of the rule. Rules with higher priority are

	processed first (1 is the highest priority).
Service	Select management service of rule. All: Manage all services ● **HTTP**: Manage only http server. ● **HTTPs**: Manage only https server. ● **SNMP**: Manage only SNMP server. ● **SH**: Manage only SSH server. ● **Telnet**: Manage only telnet server.
Action	Select action if rule matched. ● **Permit**: Permit packet access. ● **Deny**: Deny access. Packet will be drop.
Port	Select interface that packet can access.
IP Version	Input source IP address that can access. All: All IP addresses can access. ● **IPv4**: Specify ipv4 address that allowed. ● **IPv6**: Specify ipv6 address that allowed.
IPv4	IPv4/Mask: Specify ipv4 address and mask that allowed.
IPv6	IPv6/Prefix: Specify ipv6 address and prefix that allowed.

Table 12-11 Add Management ACE fields

12.5 Authentication Manager

12.5.1 Authentication Manager Property

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

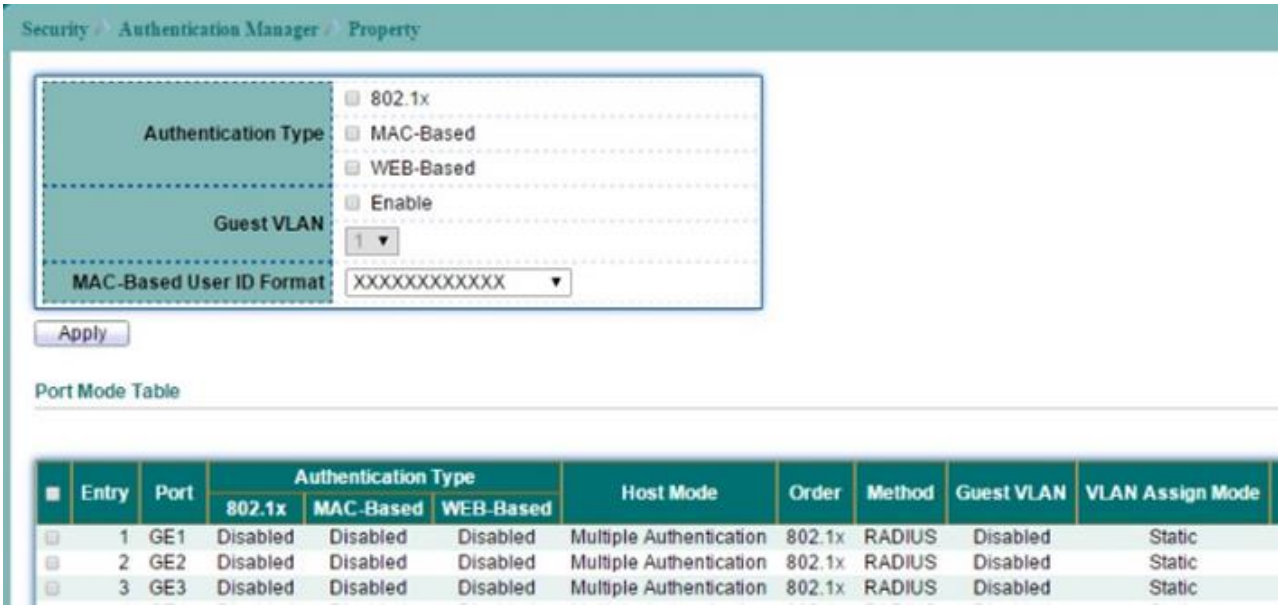


Figure 12-13 Authentication Manager Property page

Select entry and click "Edit" button to configure Authentication Manager Port Mode entry.

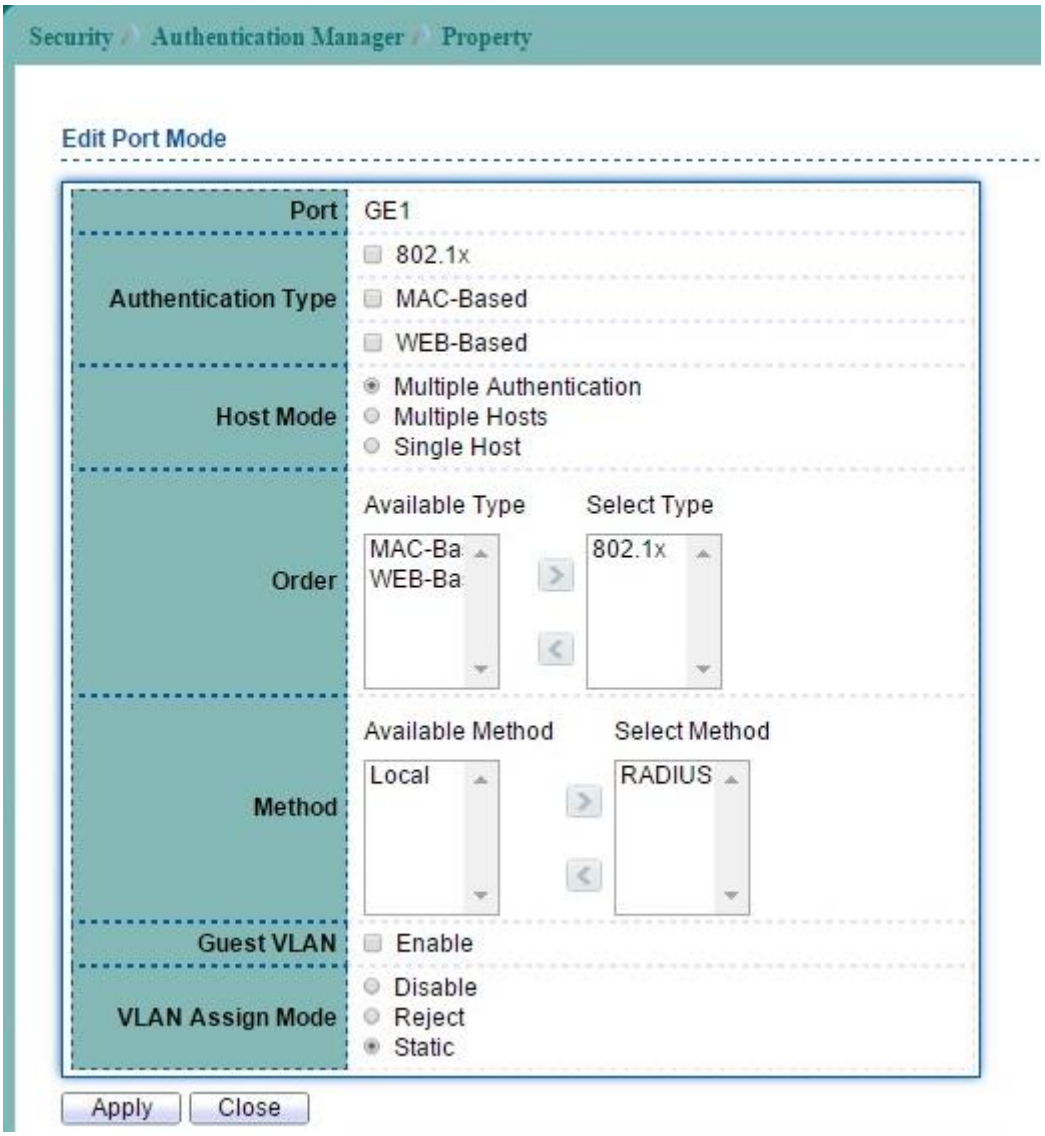


Figure 12-14 Edit Authentication Manager Property page

Field	Description
Port	Port Number
Authentication Type	The authentication type will be used.
Host Mode	The mode to decide how many hosts should pass authentication.
Order	Specify the order of authentication type. Authentication type with higher priority are processed first (1 is the highest priority).
Method	The authentication method.
Guest VLAN	To enable guest VLAN for the hosts that authentication fail.
VLAN Assign Mode	Specify the VLAN assign mode after finish authentication.

Table 12-12 Edit Authentication Manager Property fields

12.5.2 Authentication Port Setting

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

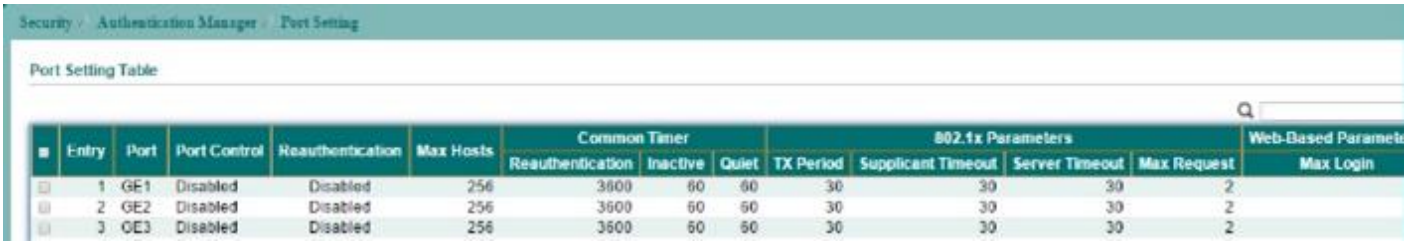


Figure 12-15 Authentication Manager Port Setting page

Field	Description
Entry	Port entry.
Port	Select one or multiple ports to configure.
Port Control	• **Disabled:** Disable authentication. • **Force Authorized:** Force this port to be 802.1X authenticated. • **Force Unauthorized:** Force this port to be 802.1X unauthenticated. • **Auto:** Enable 802.1X port-based authentication for this port.
Reauthentication	• **Enabled:** Reauthentication enabled. • **Disabled:** Reauthentication disabled.
Max Hosts	Maximum number of hosts allowed for the authentication setting.
Common Timer	
Reauthentication	Show the Reauthentication period
Inactive	Show the Inactive period.
Quiet	Show the Quiet period.
802.1x Parameters	
TX Period	Show the TX Period.
Supplicant Timeout	Show the Supplicant period.
Server Timeout	Show the Server Timeout period.
Maximum Request Retries	Show the maximum request retries.
Web-Based Parameters	
Max Login	Maximum users.
Max Login	The Maximum users.

Table 12-13 Authentication Manager Port Setting fields

Select entry and click "Edit" button to configure Authentication Manager Port Setting entry.

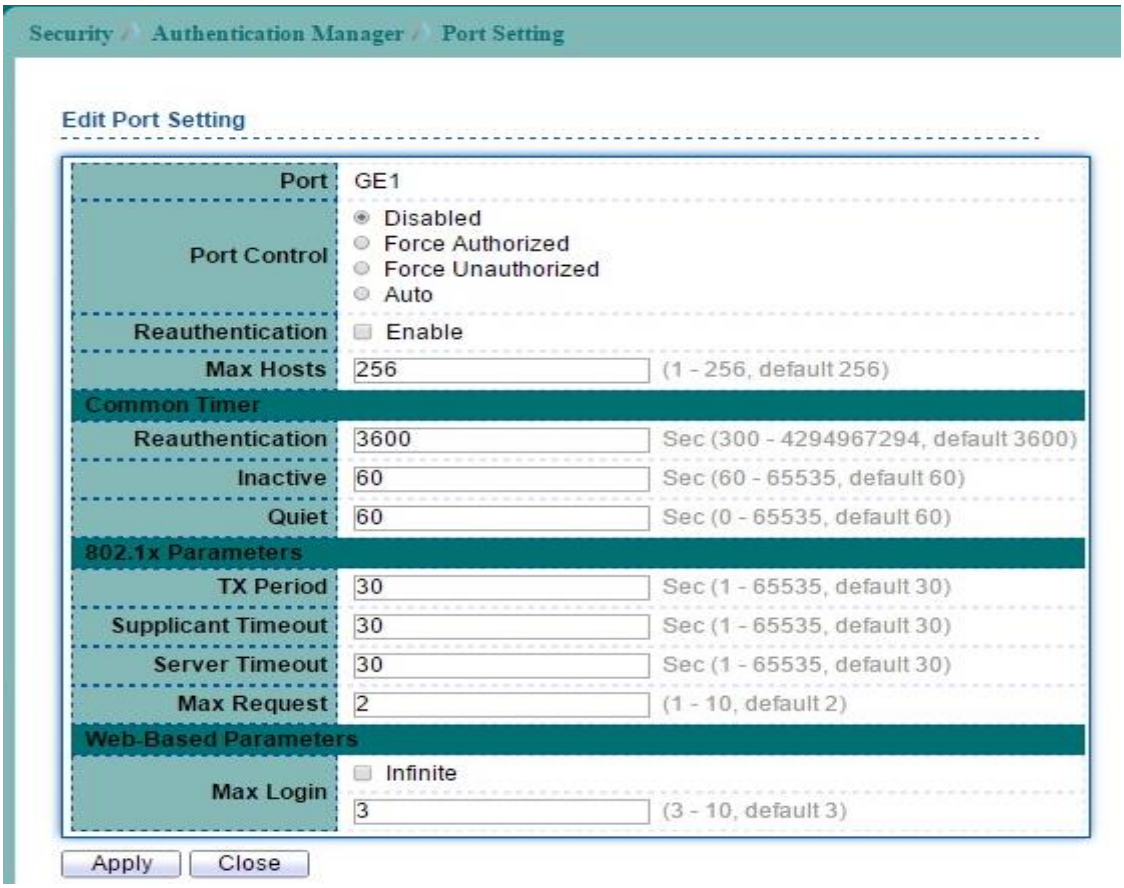


Figure 12-16 Edit Authentication Manager Port Setting page

Field	Description
Port	Select one or multiple ports to configure.
Port Control	• **Disabled:** Disable authentication. • **Force Authorized:** Force this port to be 802.1X authenticated. • **Force Unauthorized:** Force this port to be 802.1X unauthenticated. • **Auto:** Enable 802.1X port-based authentication for this port.
Reauthentication	• **Enabled:** Enable reauthentication.
Max Hosts	Maximum number of hosts allowed for the authentication setting.
Common Timer	
Reauthentication	Set the Reauthentication period.
Inactive	Set the Inactive period.
Quiet	Set the Quiet period.
802.1x Parameters	
TX Period	Set the TX Period.
Supplicant Timeout	Set the Supplicant period.
Server Timeout	Set the Server Timeout period.
Maximum Request Retries	Set the maximum request retries.
Web-Based Parameters	
Max Login	The Maximum users.

Table 12-14 Edit Authentication Manager Port Setting fields

12.5.3 MAC-Based Local Account

To display MAC-Based Local Account web page, click **Security** > **Authentication Manager** > **MAC-Based Local Account.**

This page allow user to add MAC-Based Local Accounts base on the users' MAC address.

Figure 12-17 MAC-Base Local Account page

Click "Add" button to create a new MAC-Based Local Account entry.

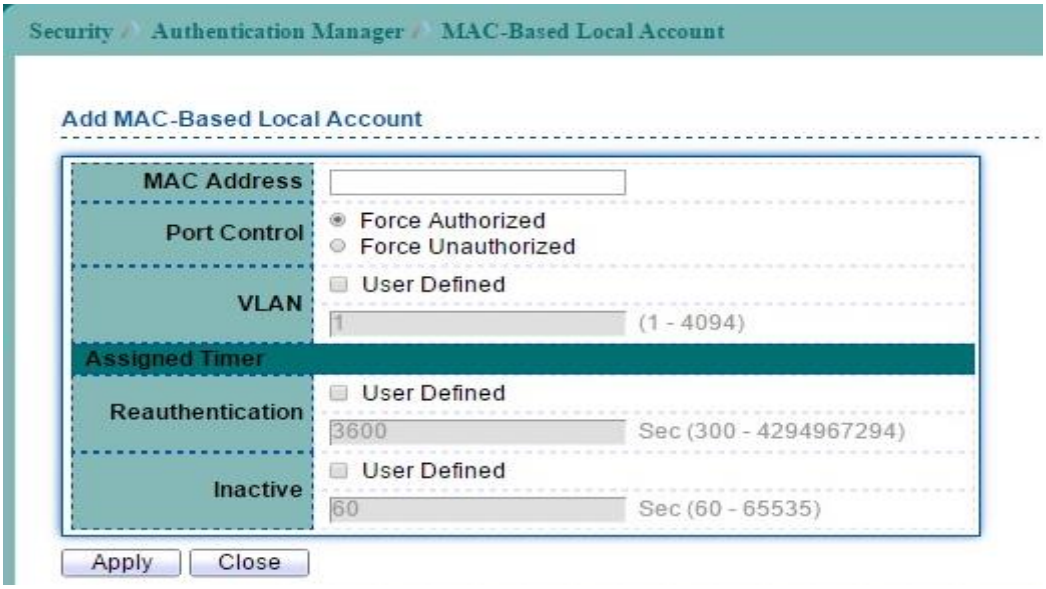


Figure 12-18 Add MAC-Base Local Account page

Field	Description
Mac Address	The Mac Address of this host.
Port Control	Authentication Method • **Force Authorized:** Force this port to be 802.1X authenticated. • **Force Unauthorized:** Force this port to be 802.1X unauthenticated.
VLAN	VLAN ID.
AssignedTime	
Reauthentication	Set the Reauthentication period.
Inactive	Set the Inactive period.

Table 12-15 Add MAC-Base Local Account fields

12.5.4 Web-Based Local Account

To display Web-Based Local Account web page, click **Security** > **Authentication Manager** > **Web-Based Local Account.**

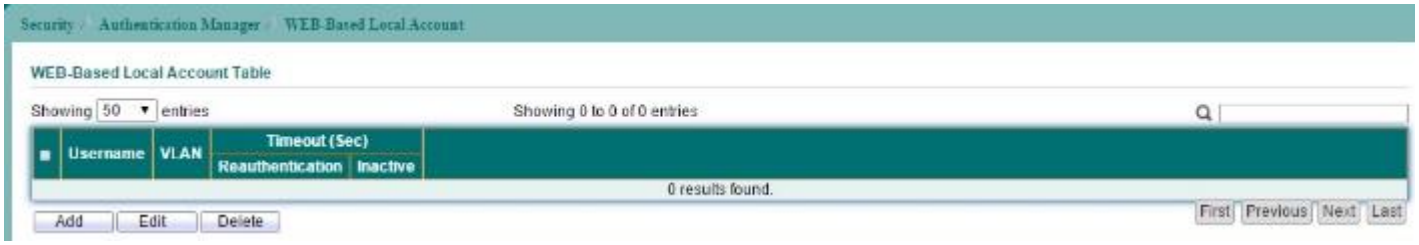


Figure 12-19 Web-Base Local Account page

Click "Add" button to create a new WEB-Based Local Account entry.

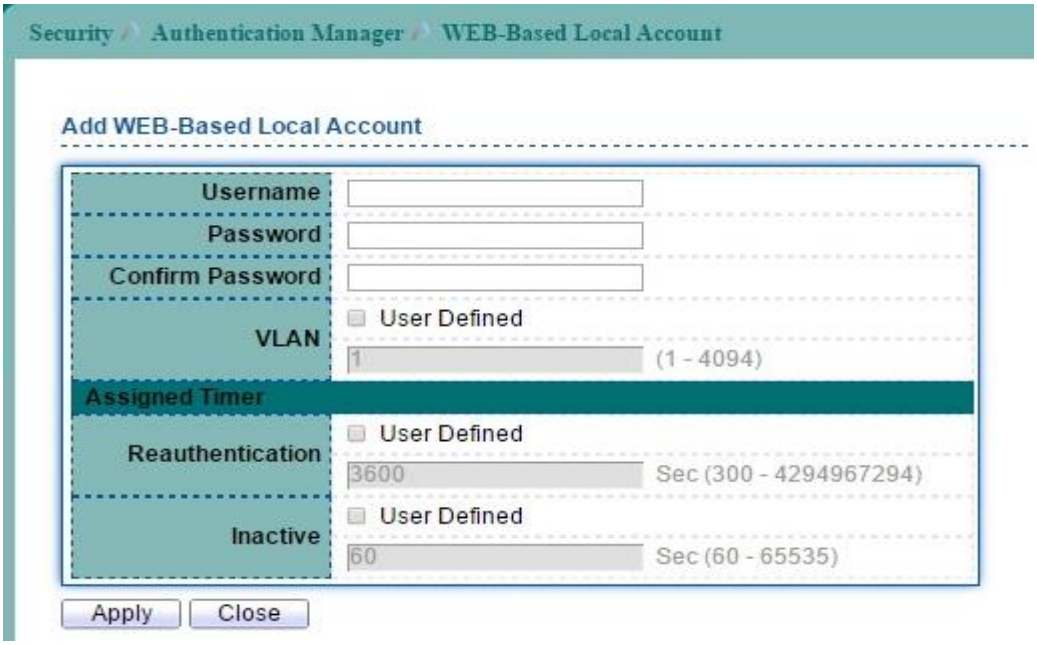


Figure 12-20 Add Web-Base Local Account page

Field	Description
Username	Create a user name for Web-Base Local Account.
Password	Set the user password
Confirm Password	Retype password to make sure the password is exactly you typed before in "Password" field.
VLAN	VLAN ID.
AssignedTime	
Reauthentication	Set the Reauthentication period.
Inactive	Set the Inactive period.

Table 12-16 Add Web-Base Local Account fields

12.5.5 Sessions

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

This page shows user about Sessions information.

Figure 12-21 Authentication Manager Sessions page

12.6 Port Security

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

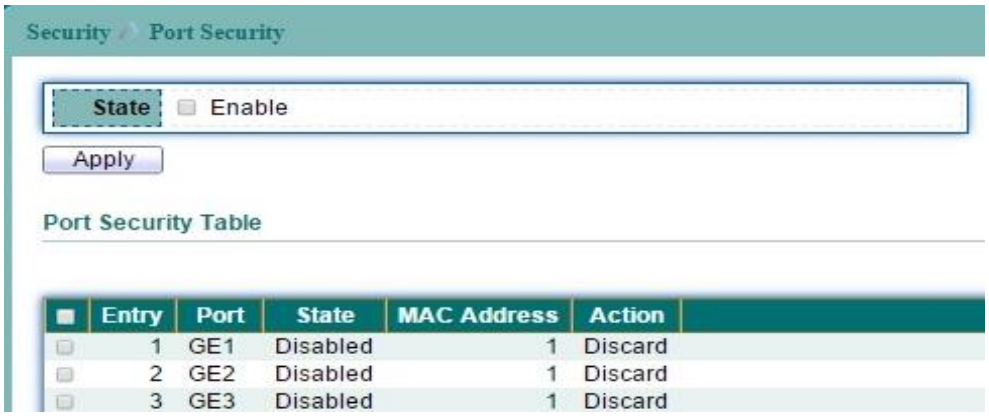


Figure 12-22 Port Security page

Select entry and click "Edit" button to configure Port Security entry.

Figure 12-23 Edit Port Security page

Field	Description
Port	Select one or multiple ports to configure.
State	• **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 MAC is new to system and exceed the learning-limit number. • **Discard:** Discard this packet whose MAC is new to system and exceed the learning-limit number. • **Shutdown:** Shutdown this port when receives a packet whose MAC is new to system and exceed the learning limit number.

Table 12-17 Port Security fields

12.7 Protected Ports

To display Protected Ports web page, click **Security** > **Protected Ports**.

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.

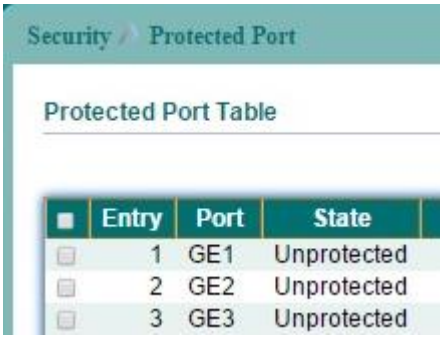


Figure 12-24 Protected Port page

Select entry and click "Edit" button to configure Protected Port entry.

Figure 12-25 Edit Protected Port page

Field	Description
Port	Select one or multiple ports to configure.
State	Protected: Enable Protected Port function.

Table 12-18 Protected Port fields

12.8 Storm Control

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

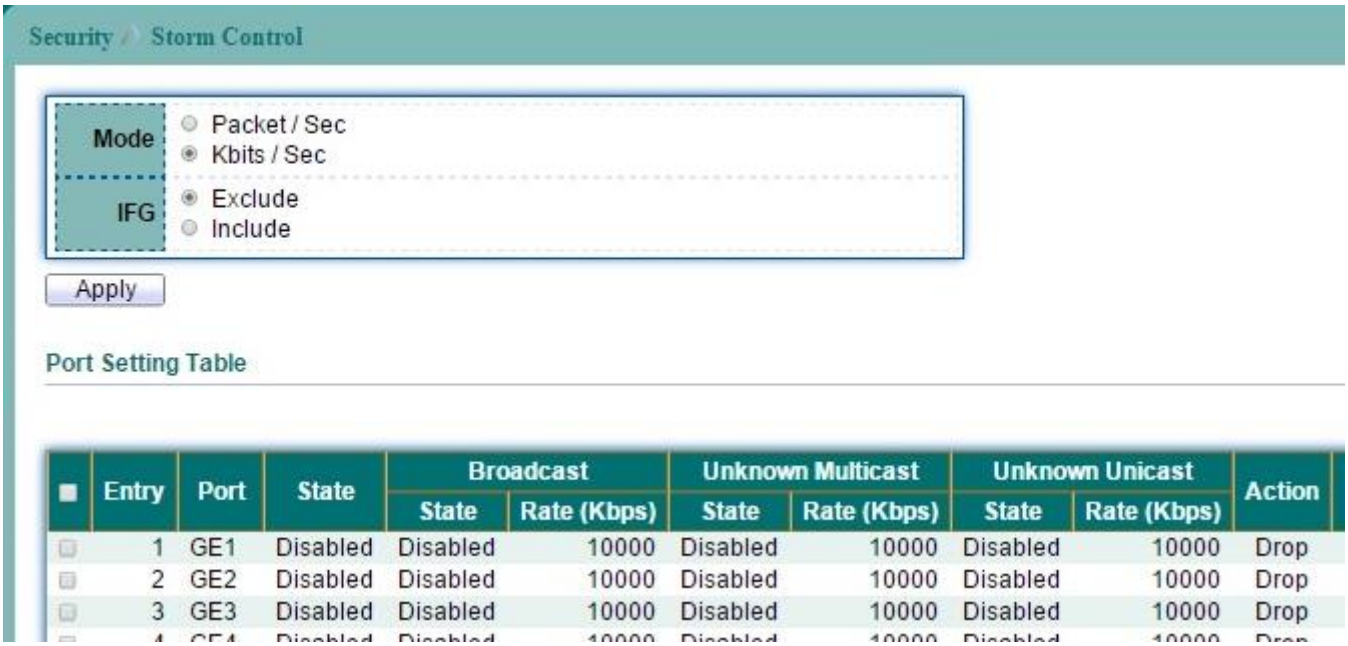


Figure 12-26 Storm Control page

Field	Description
Mode	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.

Table 12-19 Storm Control fields

Select entry and click "Edit" button to configure Storm Control entry.

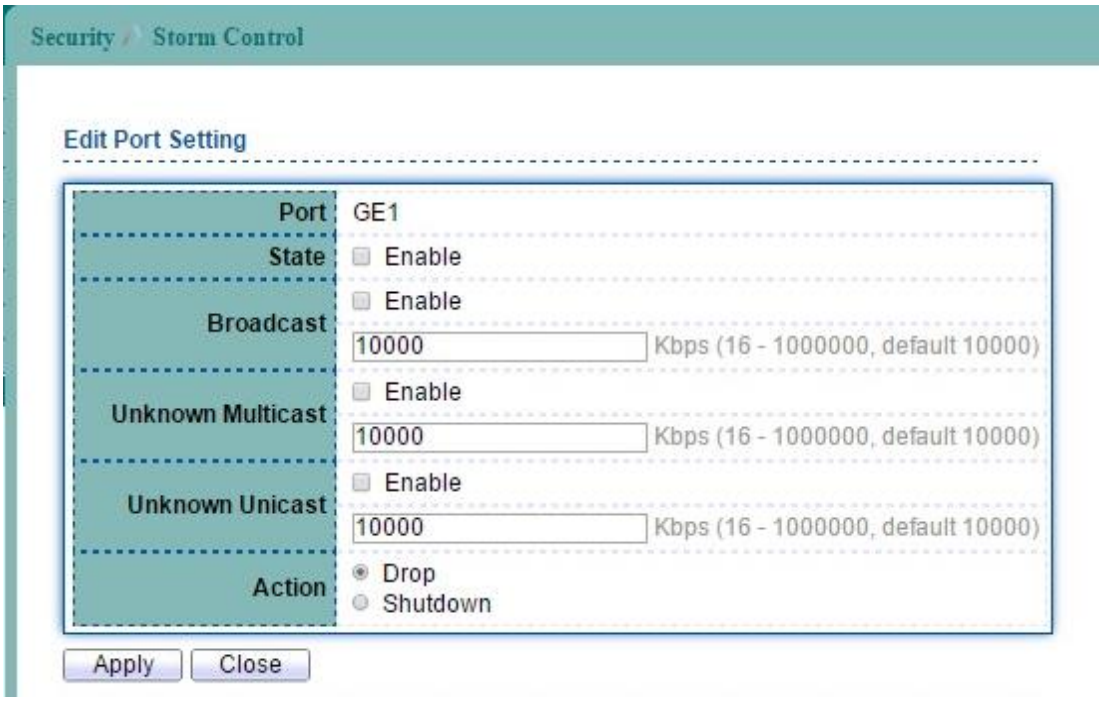


Figure 12-27 Edit Storm Control page

Field	Description
Port	Selected port.
State	• **Enable:** Enable the storm control function.
Broadcast	• **Enable:** Enable Broadcast packet Storm Control. Value of storm control rate, Unit: pps (packet per-second) or Kbps (Kbits per-second) depends on global mode setting. The range is from 0 to 1000000.
Unknown Multicast	• **Enable:** Enable Unknown Multicast packet Storm Control. Value of storm control rate, Unit: pps (packet per-second) or Kbps (Kbits per-second) depends on global mode setting. The range is from 0 to 1000000.
Unknown Unicast	• **Enable:** Enable Unknown Unicast packet Storm Control. Value of storm control rate, Unit: pps (packet per-second) or Kbps (Kbits per-second) depends on global mode setting. The range is from 0 to 1000000.
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.

Table 12-20 Edit Storm Control fields

12.9 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.

12.9.1 Dos Property

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

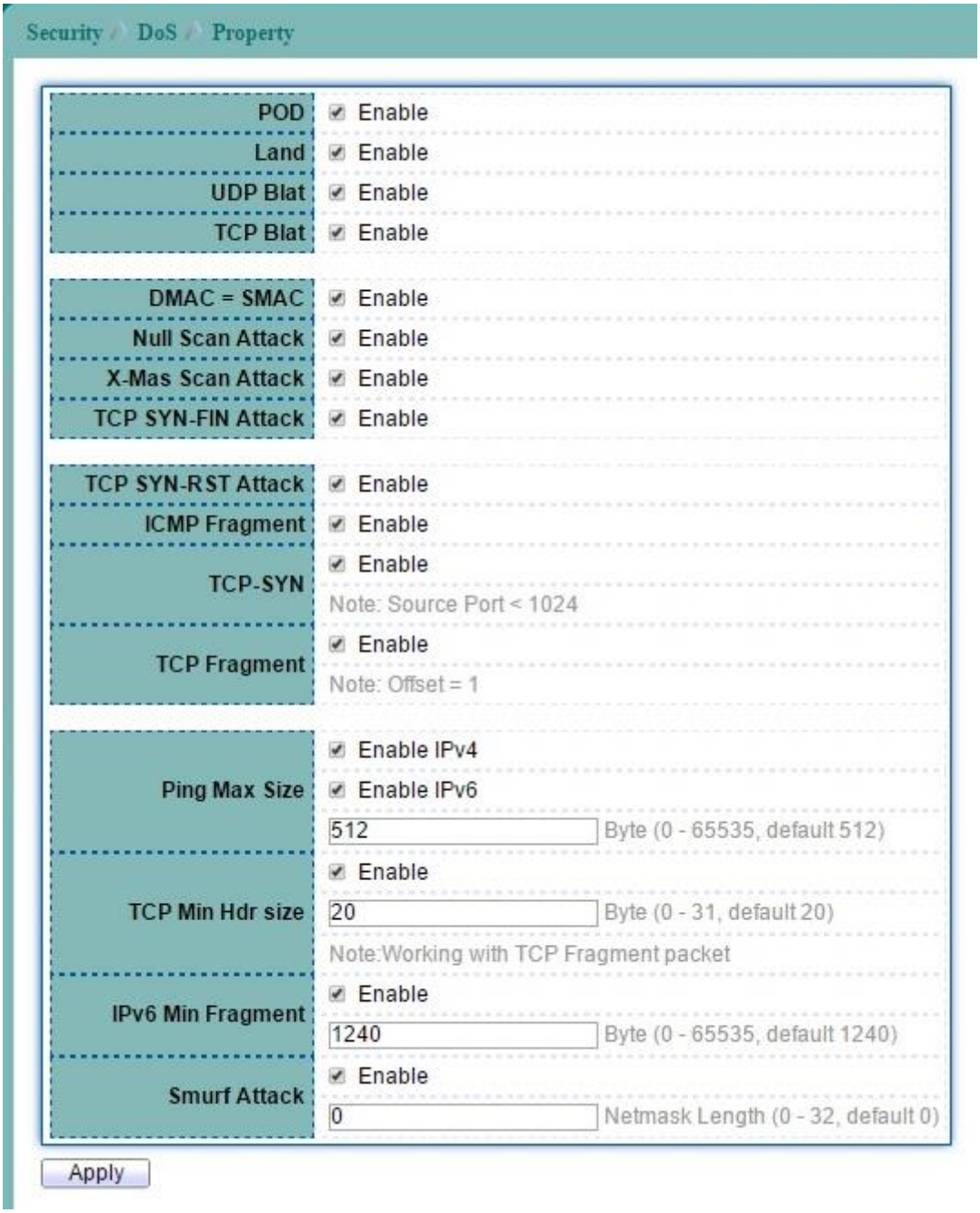


Figure 12-28 DoS Property page

Field	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(SPORT<1024)	Drops SYN packets with sport less than 1024.
TCP SYN-FIN Attack	Drops the packets with SYN and FIN bits set.
TCP SYN-RST Attack	Drops the packets with SYN and RST bits set.
ICMP Fragment	Drops the fragmented ICMP packets.
TCP Fragment	Drops the TCP fragment packets with offset equals to one.
Ping Max Size	IPv4 Ping Max Size: Checks the maximum size of ICMP ping packets, and drops the packets larger than the maximum packet size. IPv6 Ping Max Size: Checks the maximum size of ICMPv6 ping packets, and drops the packets larger than the maximum packet size. 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.
TCP Min Hdr Size	Checks the minimum TCP header and drops the TCP packets with the header smaller than the minimum size. The length range is from 0 to 31 bytes, and default length is 20 bytes.
IPv6 Min Fragment	Checks the minimum size of IPv6 fragments, and drops the packets smaller than the minimum size. The valid range is from 0 to 65535 bytes, and default value is 1240 bytes.
Smurf Attack	Avoids smurf attack. The length range of the netmask is from 0 to 323 bytes, and default length is 0 bytes.

Table 12-21 DoS Property fields

12.9.2 Dos Port Setting

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

Figure 12-29 DoS Port Setting page

Select entry and click "Edit" button to configure DoS Port Setting entry.

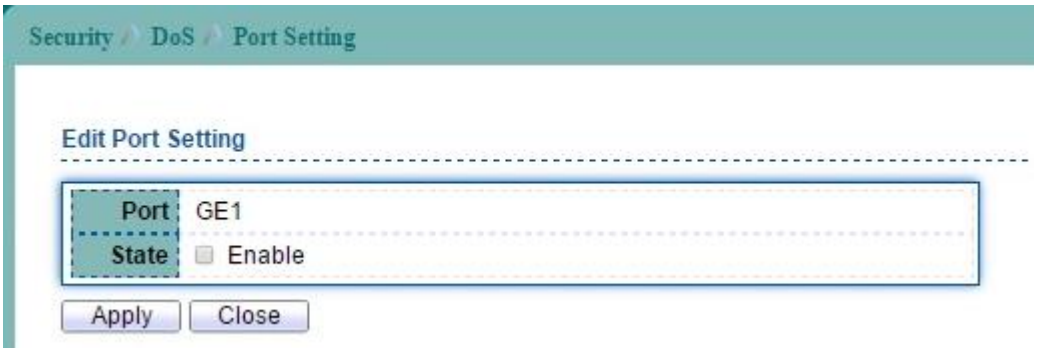


Figure 12-30 Edit DoS Port Setting page

Field	Description
Port	Select ports to set settings.
State	Enable/Disable the DoS protection on the interface.

Table 12-22 DoS Port Setting fields

12.10 Dynamic ARP Inspection

12.10.1 DAI property

To display Dynamic ARP Inspection Setting web page, click **Security** > **Dynamic ARP Inspection** > **Statistics**.

This page allow user to enable/disable DAI function.

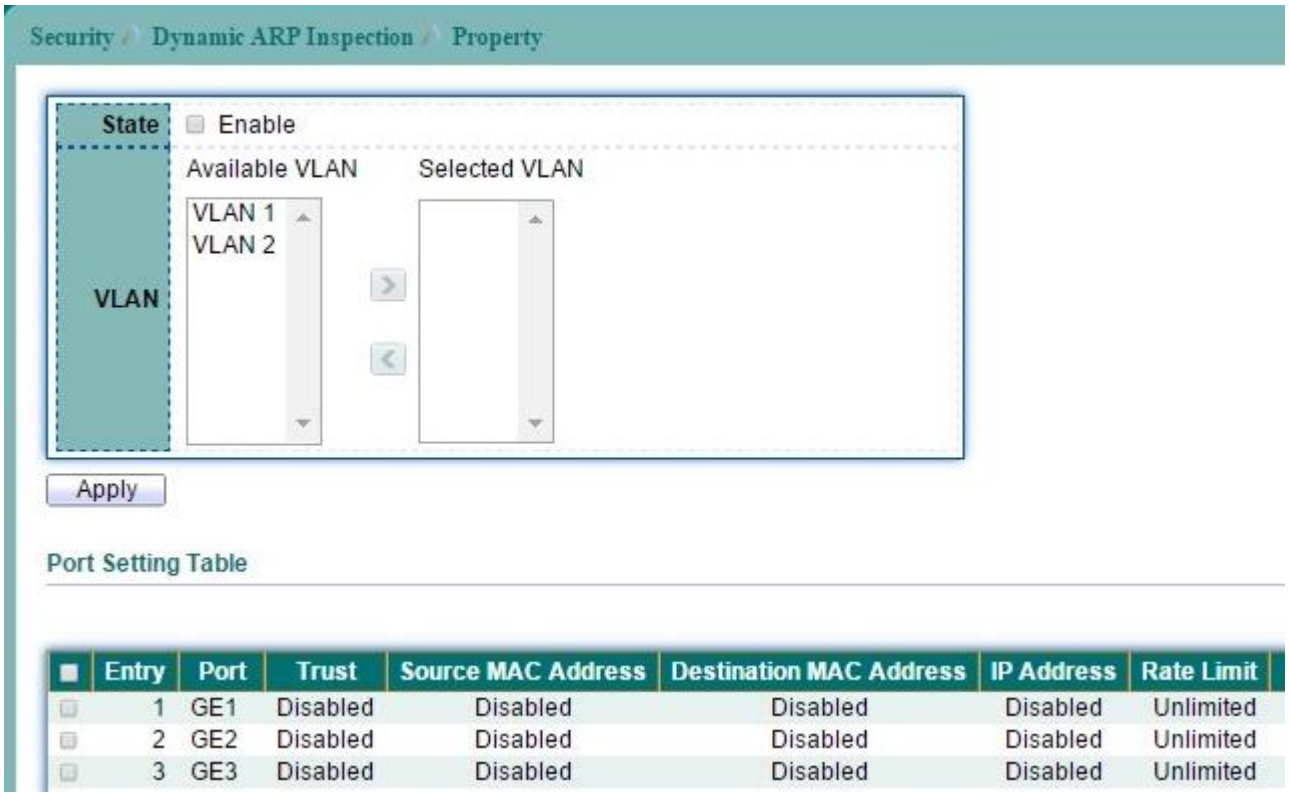


Figure 12-31 DAI Property page

Field	Description
State	To enable or disable dynamic Arp inspection function. Default is that all VLAN disabled.
VLAN LIST	Select VLAN from the Available VLAN list to enable or disable dynamic Arp inspection function.

Table 12-23 DAI Property fields

Select entry and click "Edit" button to configure DAI Port Setting entry.

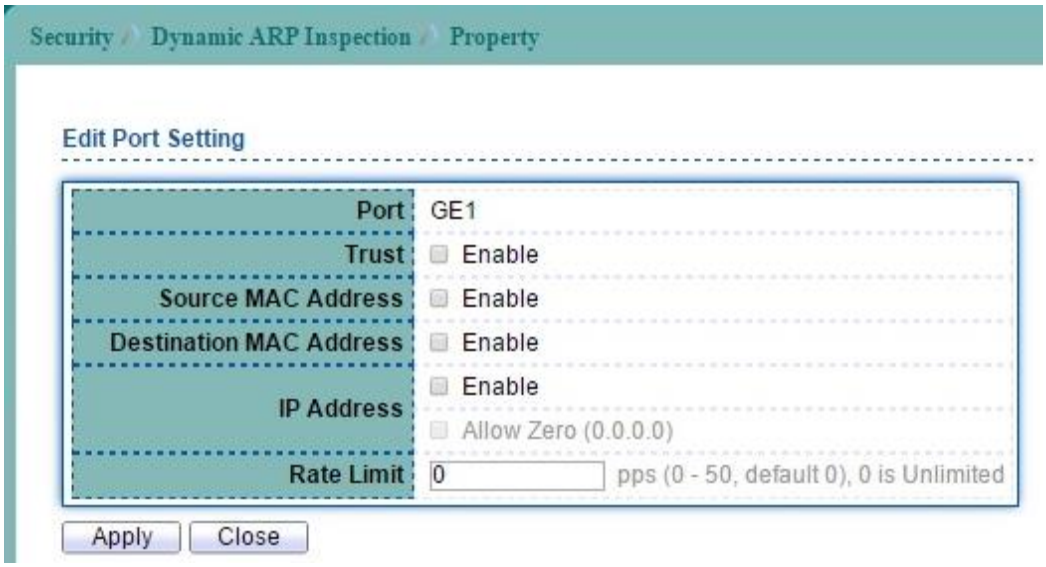


Figure 12-32 Edit DAI Property page

Field	Description
Port	Selected ports.
Trust	Set ports to un-trusted or trusted. Default is that all ports are un-trusted.
Source MAC Address	Check the check box to enable source MAC address check on ports. Default is that all ports are disabled. Enable src-mac check will check whether sender mac is same as source mac in Ethernet header.
Destination MAC Address	Check the check box to enable destination MAC address on ports. Default is that all ports are disabled. Enable dst-mac check will check whether target mac is same as destination mac in Ethernet header.
IP Address	Check the check box to enable IP check on ports. Default is that all ports are disabled. Enable ip-check will check whether IP address is 0.0.0.0, 255.255.255.255 or multicast address. **Allow Zero:** To enable allow all zero IP address on ports. Default is that all ports are disabled. Enable means 0.0.0.0 IP address is allowed.
Rate Limit	Input rate of user-defined ARP packets rate limitation.

Table 12-24 Edit DAI Property fields

12.10.2 Dynamic ARP Inspection Statistics

To display Dynamic ARP Inspection Statistics web page, click **Security** > **Dynamic ARP Inspection** > **Statistics**.

Figure 12-33 DAI Statistics page

12.11 DHCP Snooping

12.11.1 Property

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

This page allow user to enable or disable DHCP snooping function.

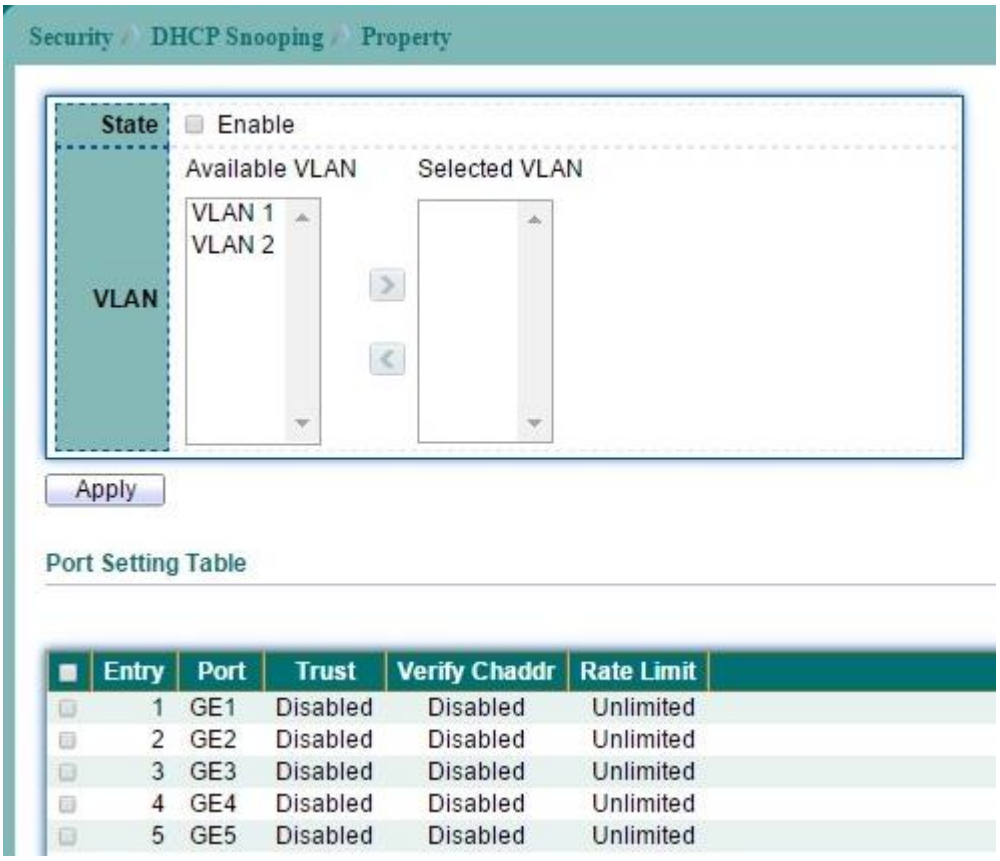


Figure 12-34 DHCP Snooping Property page

Field	Description
State	To enable DHCP Snooping function. Default is disabled.
VLAN	Select VLAN from the Available VLAN list to enable or disable DHCP Snooping function.

Table 12-25 DHCP Snooping Property fields

Select entry and click "Edit" button to configure DHCP Snooping Port Setting entry.

Figure 12-35 Edit DHCP Snooping Property page

Field	Description
Port	Selected port.
Trust	Set ports to trusted status. Default is that all ports are un-trusted.
Verify Chaddr	To enable chaddr check on ports. Default is that all ports are disabled. Enable this feature will check whether chaddr in DHCP request packet same as source MAC address of Ethernet header.
Rate Limit	DHCP packets rate limit. Packets will be drop if over rate limitation.

Table 12-26 Edit DHCP Snooping Property fields

12.11.2 Statistics

To display DHCP Snooping Setting web page, click **Security** > **DHCP Snooping** > **Statistic**.

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

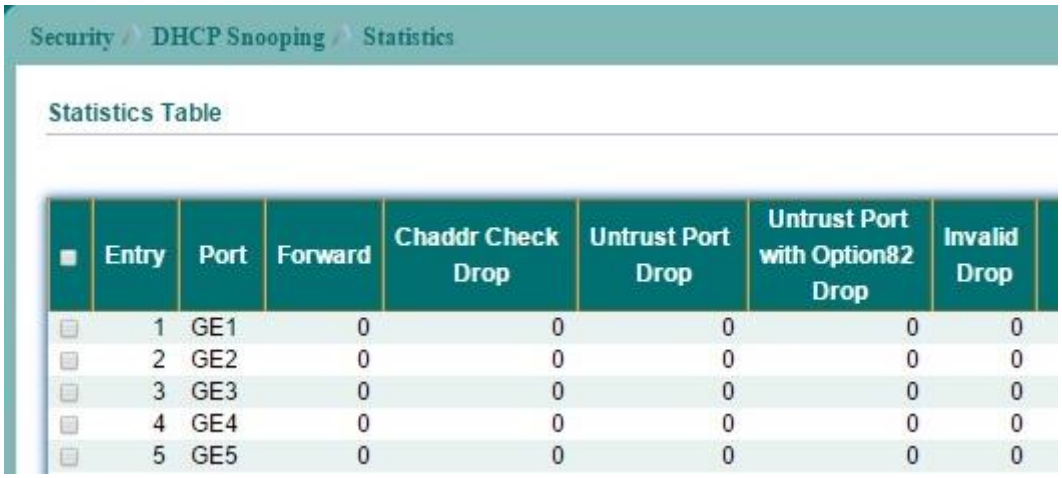


Figure 12-36 DHCP Snooping Statistics page

Field	Description
Port	Interface Ports.
Forwarded	Show how packets forwarded normally.
Chaddr Check Drop	Show how many packets dropped by chaddr checking.
Untrusted Port Drop	Show how many DHCP server packets that are received by untrusted port dropped.
Untrusted Port with Option82 Drop	Show how many packets dropped by untrusted port with option82 checking.
Invalid Drop	Show how many packets dropped by invalid drop.

Table 12-27 DHCP Snooping Statistics fields

12.11.3 Option82 Property

To display DHCP Snooping Option 82 Setting web page, click **Security** > **DHCP Snooping** > **Option82 Property**.

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

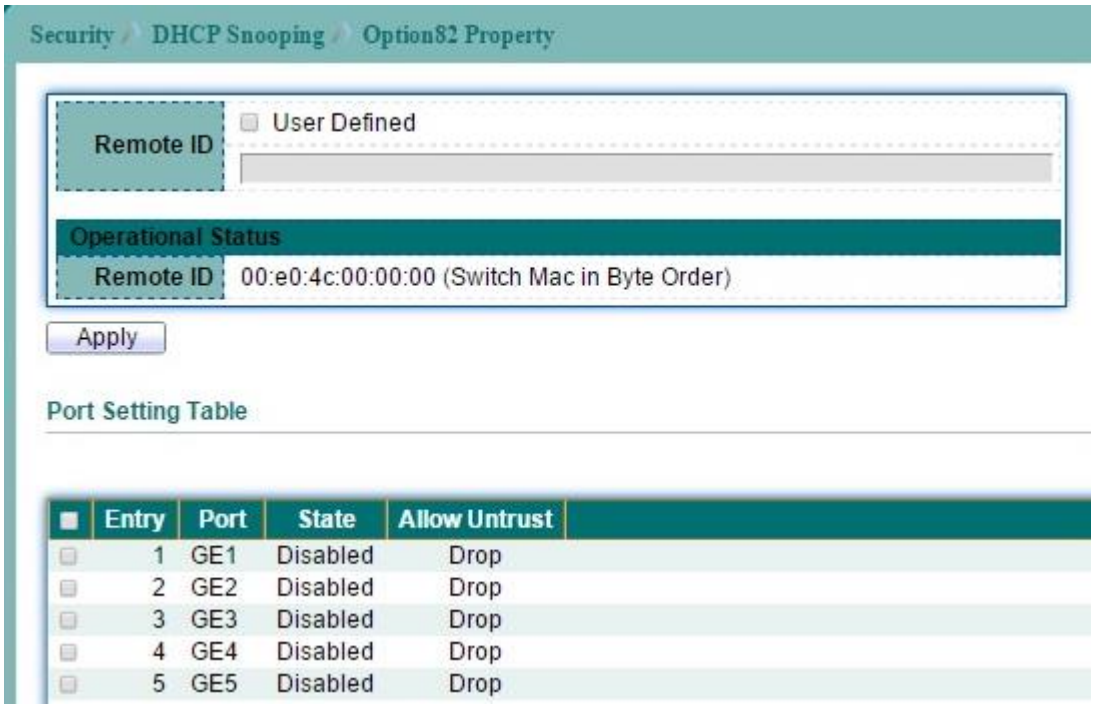


Figure 12-37 DHCP Snooping Option82 Property page

Field	Description
Option82 Remote ID	Check the check box to default or user defined remote ID. Default is device MAC address in format.

Table 12-28 DHCP Snooping Option82 fields

Select entry and click "Edit" button to configure DHCP Snooping Option82 Port Setting entry.

Figure 12-38 Edit DHCP Snooping Option82 Property page

Field	Description
Port	Selected ports.
State	To enable option82 function on ports.
Allow Untrust	Select the action perform when untrusted port receive DHCP packet has option82 filed. Default is drop.

	• **Keep:** Keep original option82 content. • **Drop:** Drop packets with option82. • **Replace:** Replace option82 content by switch setting.

Table 12-29 Edit DHCP Snooping Option82 Property fields

12.11.4 Option82 Circuit ID Setting

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

Figure 12-39 DHCP Snooping Option82 Circuit-ID page

Click "Add" button to create DHCP Snooping Option82 Circuit ID entry.

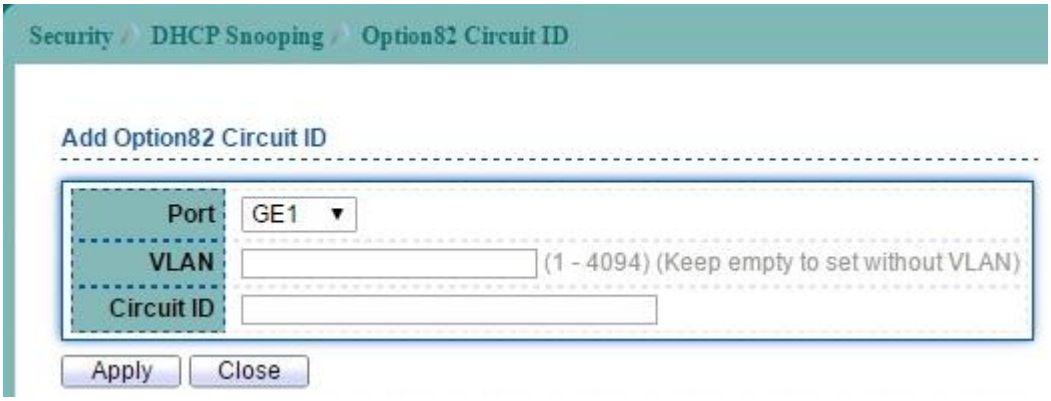


Figure 12-40 Add DHCP Snooping Option82 Circuit-ID page

Field	Description
Port	Select ports to set settings.
VLAN	Input VLAN list.
Circuit ID	Input user defined circuit ID string.

Table 12-30 DHCP Snooping Option82 Circuit-ID fields

13 ACL

13.1 MAC ACL

To display MAC ACL Setting web page, click **ACL** > **MAC ACL**

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

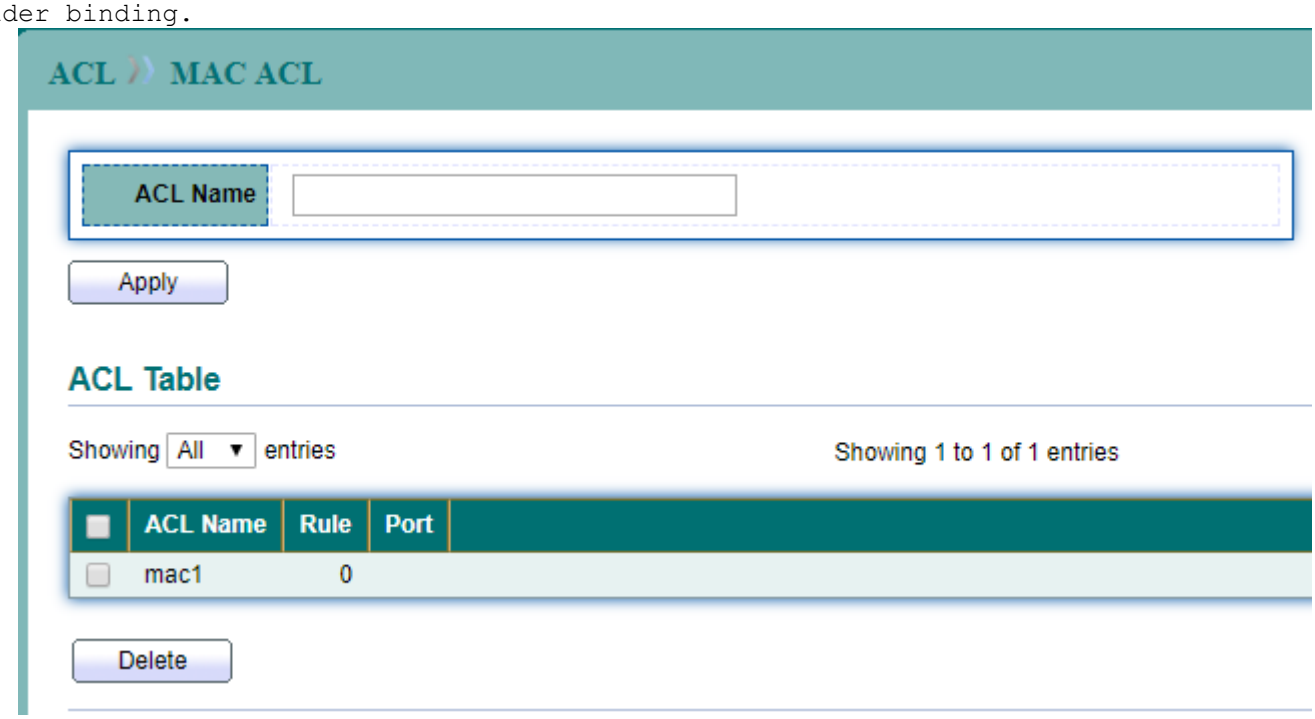


Figure 13-1 MAC ACL page

Field	Description
ACL Name	Set MAC ACL name.
Rule	The number of rule in the ACL.
Port	The port number that bind in the ACL.

Table 13-1 MAC ACL fields

13.2 MAC ACE

To display MAC ACE Setting web page, click **ACL** > **MAC ACE**

This page allow user to add, edit or delete a MAC ACE rule. A rule cannot be deleted if under binding. New MAC ACE rule cannot be added if the ACL is under binding.

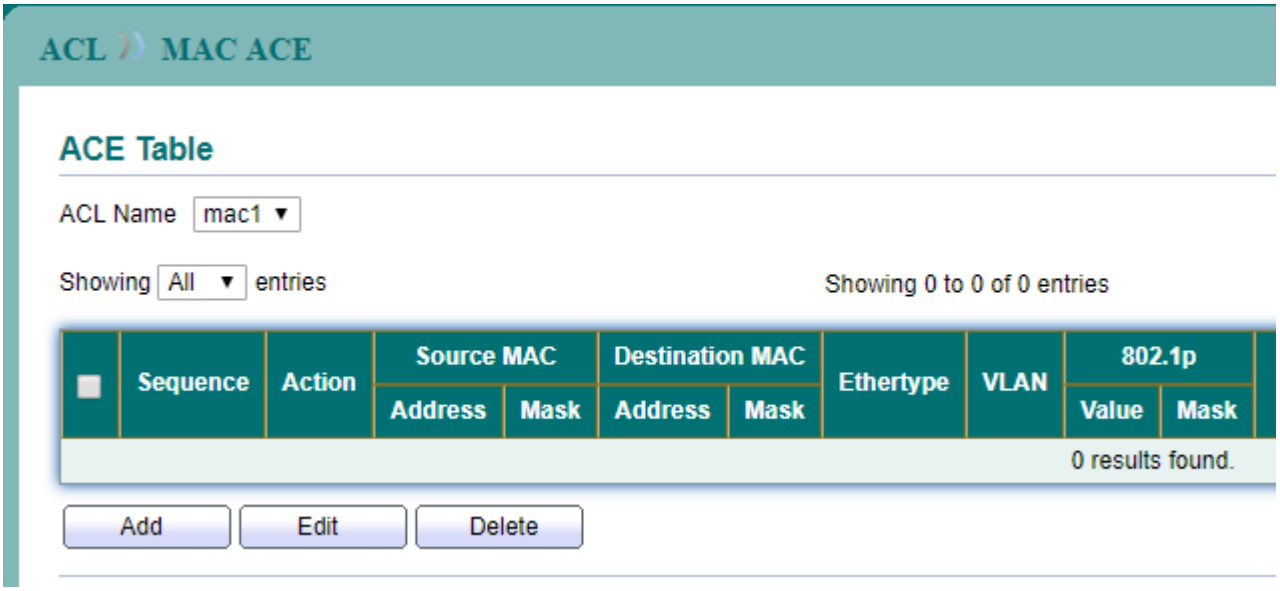


Figure 13-2 MAC ACE page

Click "Add" button to create a new MAC ACE entry.

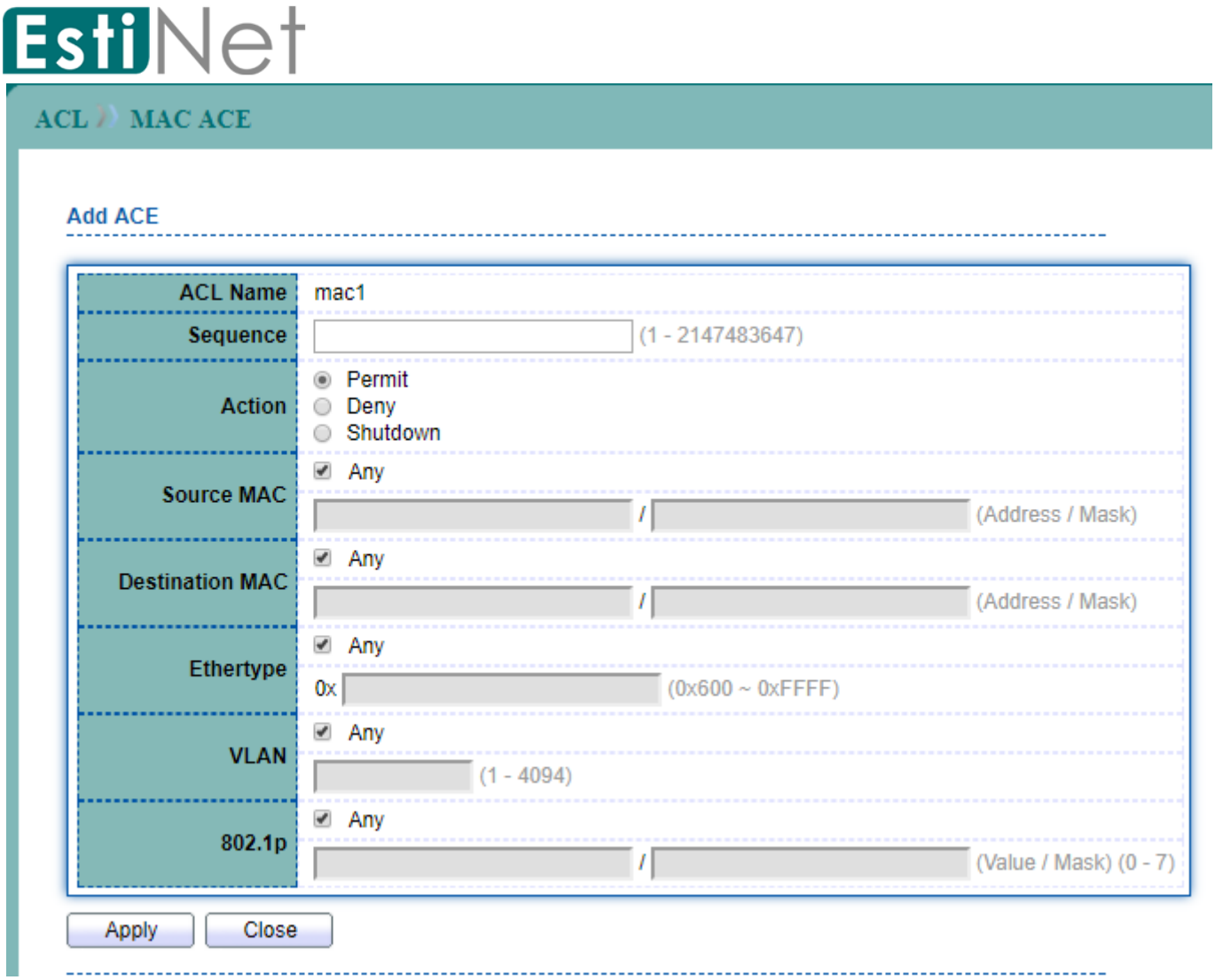


Figure 13-3 Add MAC ACE page

Field	Description
ACL Name	Set MAC ACL name.
Sequence	Specify the sequence of the ACE. ACEs with higher sequence are processed first(1 is the highest priority)
Action	Select the action for a match. ● **Permit:** Forward packets that meet the ACE criteria. ● **Deny:** Drop packets that meet the ACE criteria. ● **Shutdown:** Drop packets that meet the ACE criteria and disable the port from where the packets were received. Ths disabled port can be reactivated from the Port Settings page.
Source MAC	Select the type for source MAC address. ● **Any:** All source addresses are acceptable. ● **User Defined:** Only a source address or a range of source address which user define are acceptable.
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 address which user define are acceptable.
Ethertype	Enter the frame Ethertype to be matched
VLAN	The VLAN ID number of the VLAN on which the above MAC address resides
802.1p	Select include to use 802.1p

Table 13-2 MAC ACE fields

13.3 IPv4 ACL

To display IPv4 ACL Setting web page, click **ACL** > **IPv4 ACL**

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

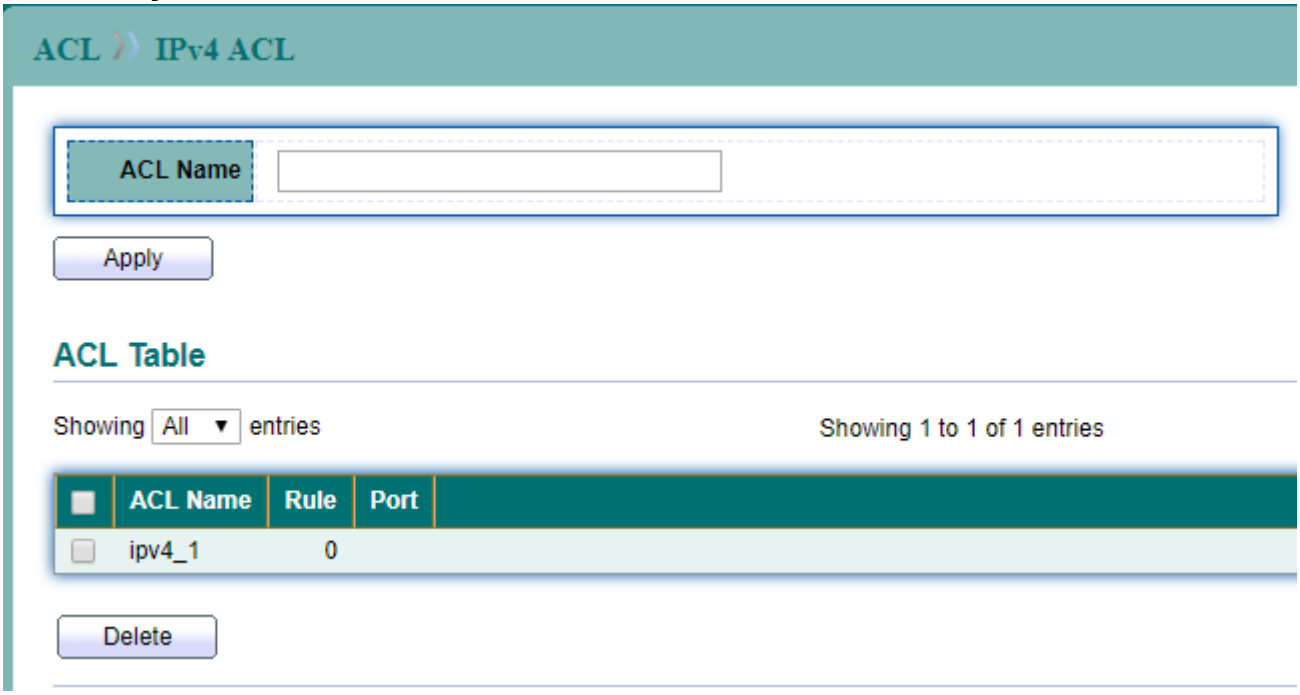


Figure 13-4 IPv4 ACL page

Field	Description
ACL Name	Set IPv4 ACL name.
Rule	The number of rule in the ACL.
Port	The port number that bind in the ACL.

Table 13-3 IPv4 ACL fields

13.4 IPv4 ACE

To display IPv4 ACE Setting web page, click **ACL** > **IPv4 ACE**

This page allow user to add, edit or delete an IPv4 ACE rule. A rule cannot be deleted if under binding. New IPv4 ACE rule cannot be added if the ACL is under binding.

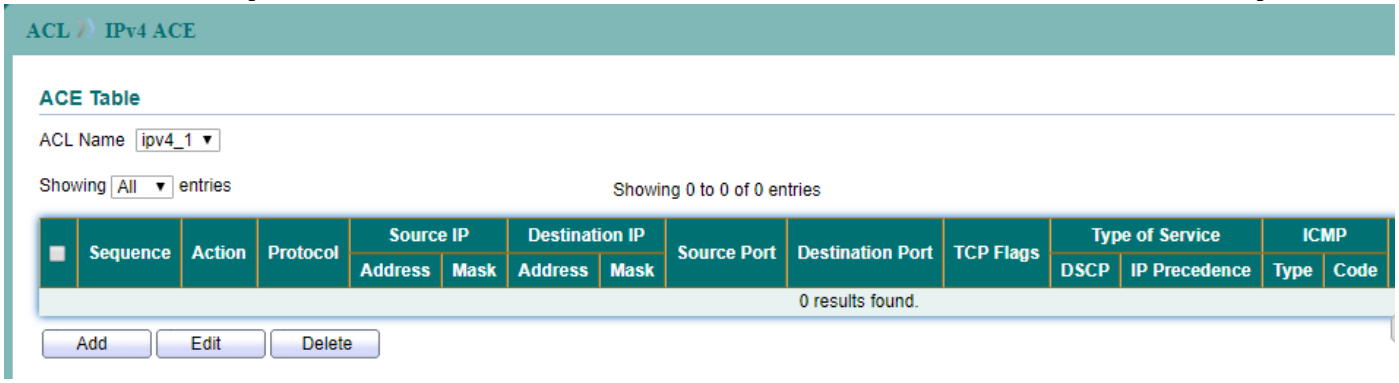


Figure 13-5 IPv4 ACE page

Click "Add" button to create a new IPv4 ACE entry.

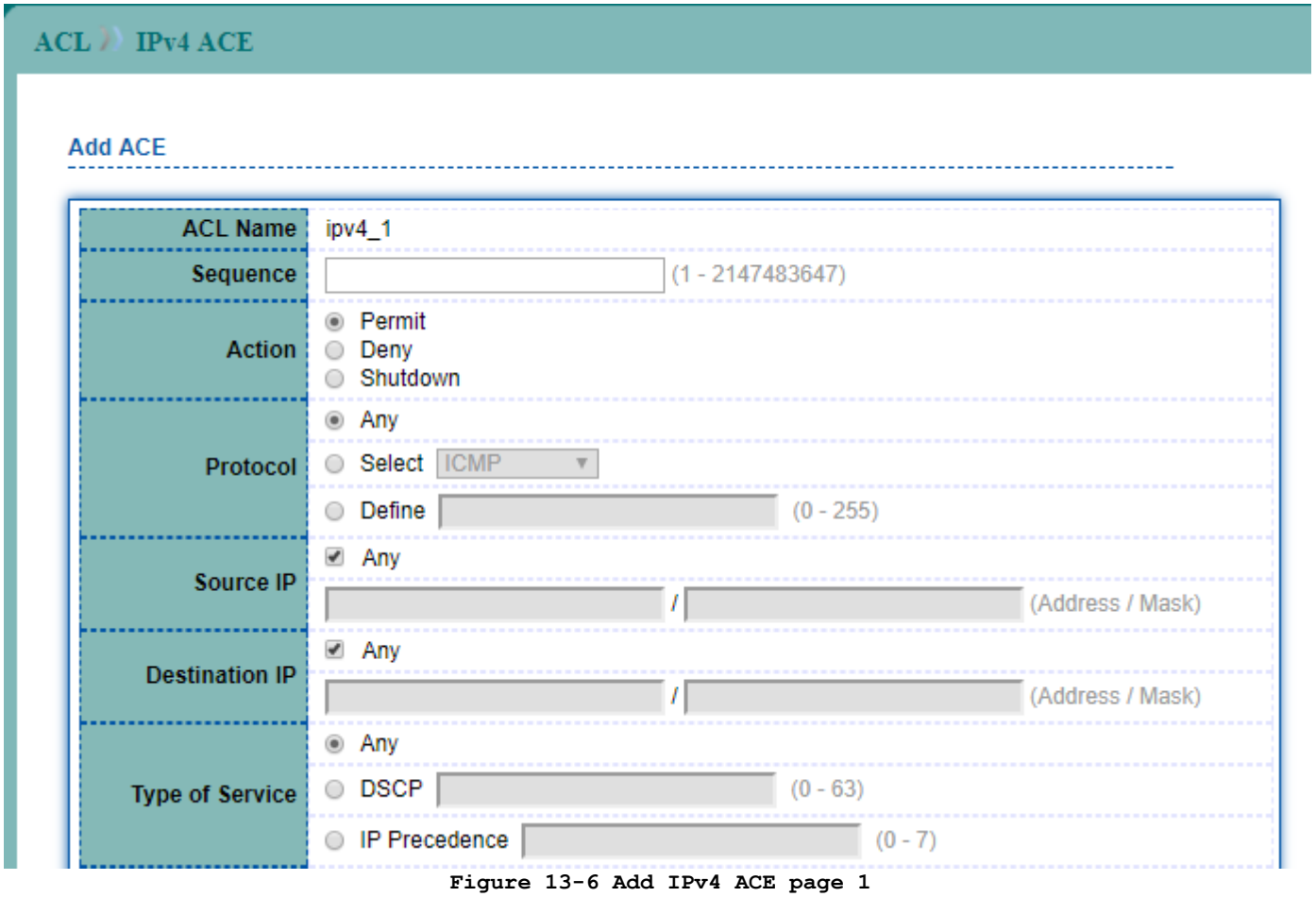


Figure 13-6 Add IPv4 ACE page 1

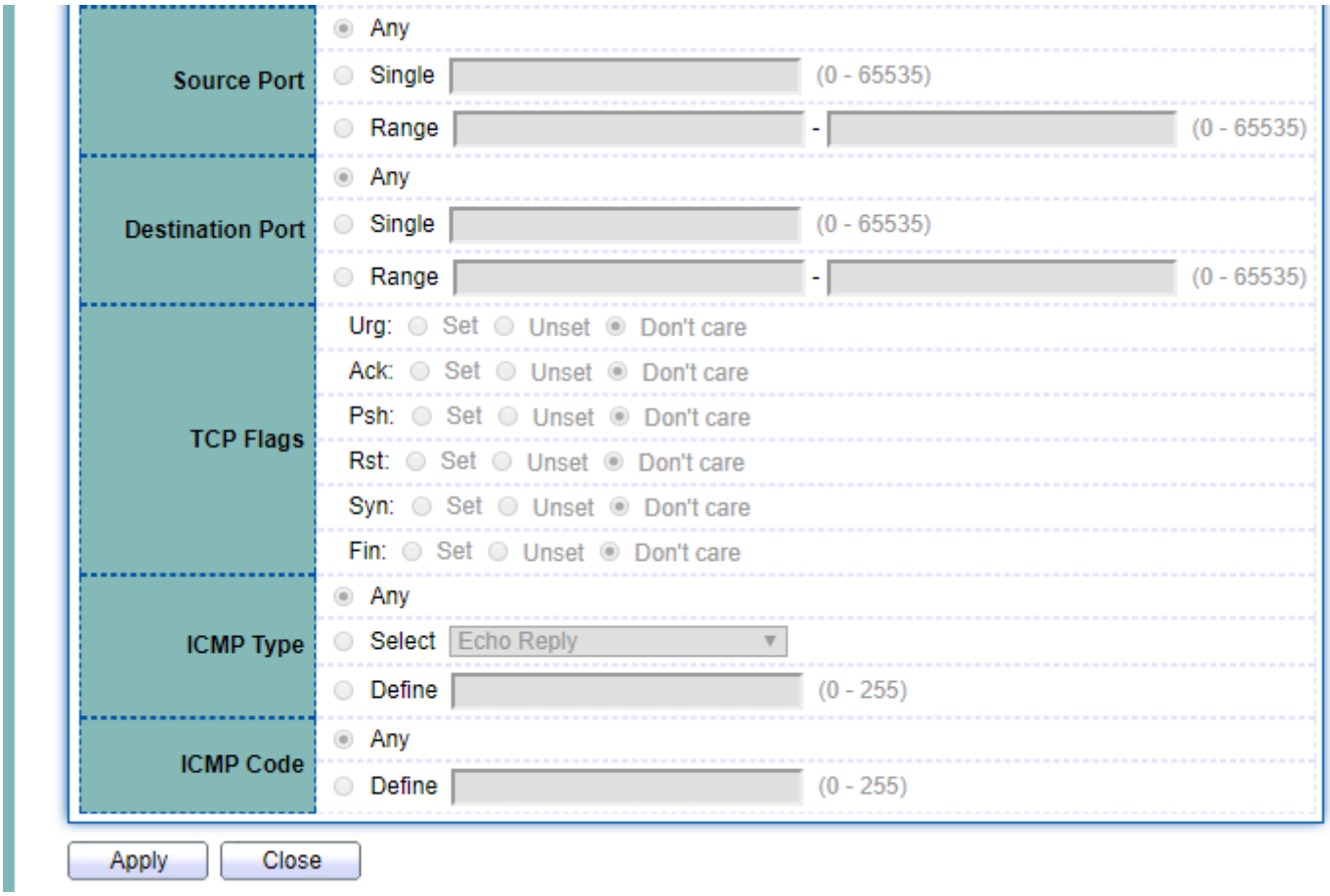


Figure 13-7 Add IPv4 ACE page 2

Field	Description
ACL Name	Set MAC ACL name.
Sequence	Specify the sequence of the ACE. ACEs with higher sequence are processed first(1 is the highest priority)
Action	Select the action for a match. ● **Permit:** Forward packets that meet the ACE criteria. ● **Deny:** Drop packets that meet the ACE criteria. ● **Shutdown:** Drop packets that meet the ACE criteria and disable the port from where the packets were received. The disabled port can be reactivated from the Port Settings page.
Protocol	Select the type of protocol for a match ● **Any:** All IP protocols are acceptable. ● **Select from list:** Select one of the following protocols. (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 address which user define are acceptable.
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 address which user define are acceptable.
Type of Service	Select the type of service for a match. ● **Any:** All types of service are acceptable. ● **DSCP to match:** Enter a Differentiated Serves Code Point(DSCP) to match.

	• **IP Precedence to match:** Enter a IP Precedence to match.
Source Port	Select the TCP/UDP source port for a match. • **Any:** All TCP/UDP 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.
Destination Port	Select the TCP/UDP destination port for a match. • **Any:** All TCP/UDP destination ports are acceptable. • **Single:** Enter a single TCP/UDP destination port to which packets are matched. • **Range:** Select a range of TCP/UDP destination ports to which the packet is matched.
TCP Flags	Select one or more TCP flags with which to filter packets.
ICMP Type	Select the ICMP type for a match. • **Any:** All ICMP types are acceptable. • **Select from list:** Select ICMP type by name. • **Protocol ID to match:** Enter the number of ICMP type.
ICMP Code	Select ICMP code for a match. • **Any:** All ICMP codes are acceptable. • **User Defined:** Enter an ICMP code.

Table 13-4 IPv4 ACE fields

13.5 IPv6 ACL

To display IPv6 ACL Setting web page, click **ACL** > **IPv6 ACL**

This page allow user to add or delete an IPv6 ACL rule. A rule cannot be deleted if under binding.

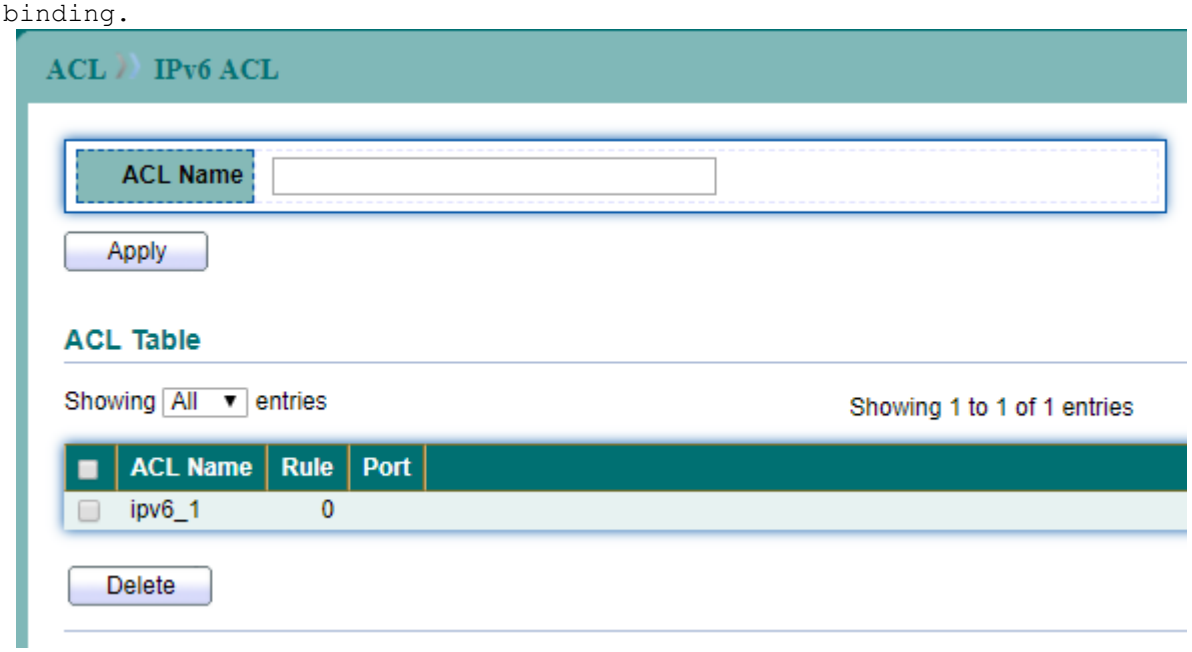


Figure 13-8 IPv6 ACL page

Field	Description
ACL Name	Set IPv6 ACL name.
Rule	The number of rule in the ACL.
Port	The port number that bind in the ACL.

Table 13-5 IPv6 ACL fields

13.6 IPv6 ACE

To display IPv6 ACE Setting web page, click **ACL** > **IPv6 ACE**

This page allow user to add, edit or delete an IPv6 ACE rule. A rule cannot be deleted if under binding. New IPv6 ACE rule cannot be added if the ACL is under binding.

Figure 13-9 IPv6 ACE page

Click "Add" button to create a new IPv6 ACE entry.

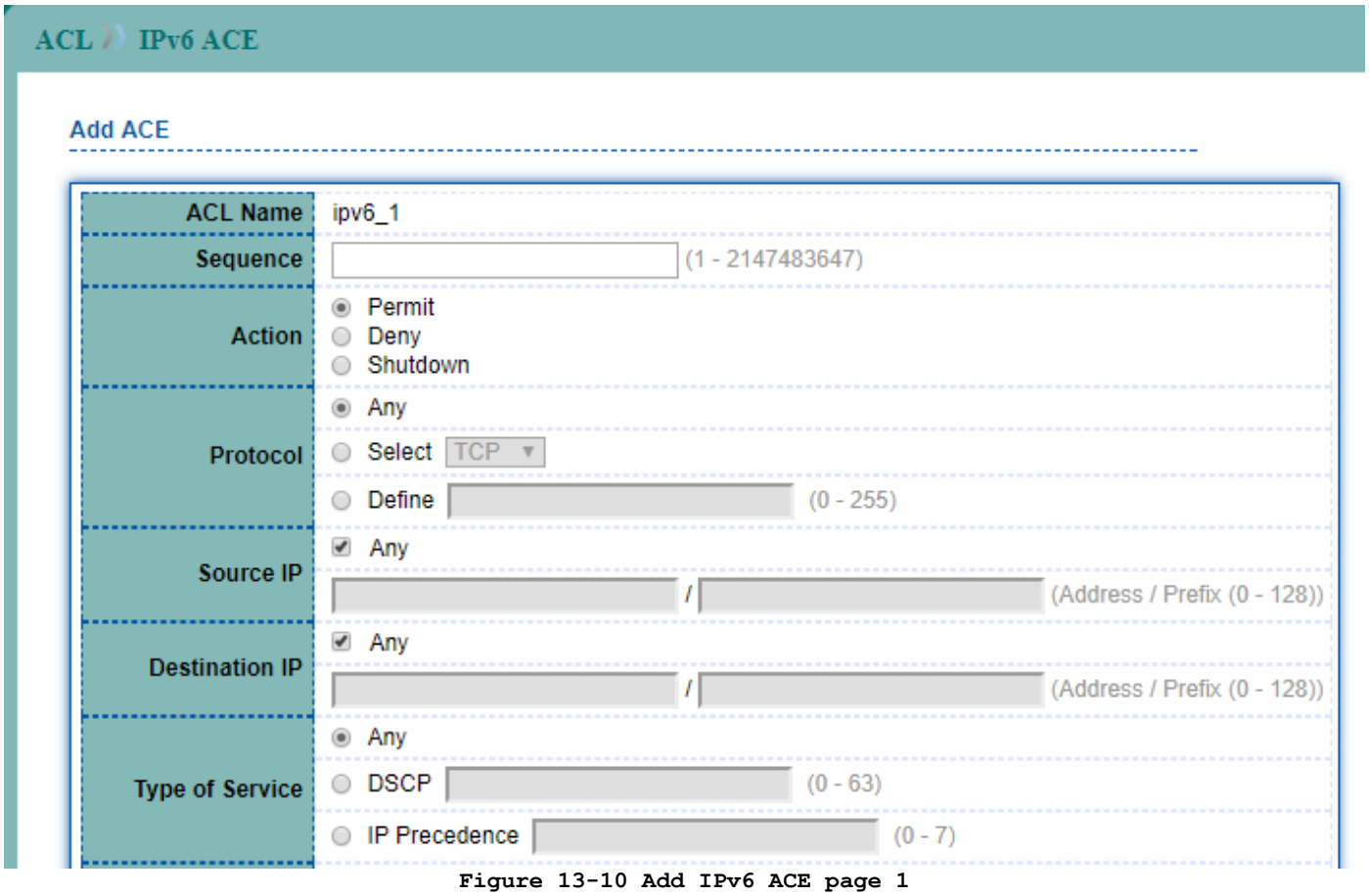


Figure 13-10 Add IPv6 ACE page 1

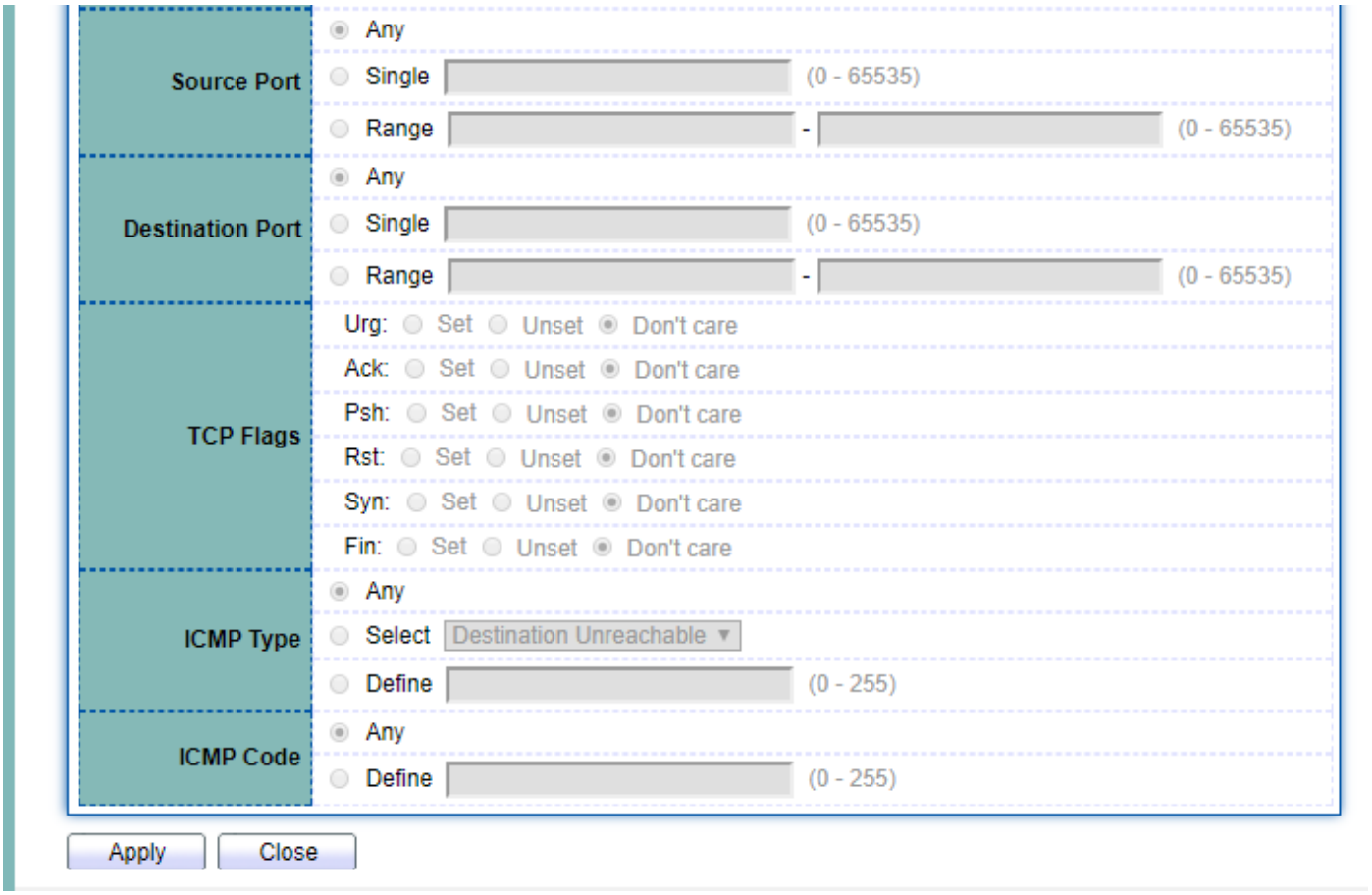


Figure 13-11 Add IPv6 ACE page 2

Field	Description
ACL Name	Set IPv6 ACL name.
Sequence	Specify the sequence of the ACE. ACEs with higher sequence are processed first(1 is the highest priority)
Action	Select the action for a match. ● **Permit:** Forward packets that meet the ACE criteria. ● **Deny:** Drop packets that meet the ACE criteria. ● **Shutdown:** Drop packets that meet the ACE criteria and disable the port from where the packets were received. The disabled port can be reactivated from the Port Settings page.
Protocol	Select the type of protocol for a match ● **Any:** All IP protocols are acceptable. ● **Select from list:** Select one of the following protocols. (TCP/UDP/ICMP). ● **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 address which user define are acceptable.
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 address which user define are acceptable.
Type of Service	Select the type of service for a match. ● **Any:** All types of service are acceptable. ● **DSCP to match:** Enter a Differentiated Serves Code Point(DSCP) to match. ● **IP Precedence to match:** Enter a IP Precedence to match.

Source Port	Select the TCP/UDP source port for a match. ● **Any:** All TCP/UDP 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.
Destination Port	Select the TCP/UDP destination port for a match. ● **Any:** All TCP/UDP destination ports are acceptable. ● **Single:** Enter a single TCP/UDP destination port to which packets are matched. ● **Range:** Select a range of TCP/UDP destination ports to which the packet is matched.
TCP Flags	Select one or more TCP flags with which to filter packets.
ICMP Type	Select the ICMP type for a match. ● **Any:** All ICMP types are acceptable. ● **Select from list:** Select ICMP type by name. ● **Protocol ID to match:** Enter the number of ICMP type.
ICMP Code	Select ICMP code for a match. ● **Any:** All ICMP codes are acceptable. ● **User Defined:** Enter an ICMP code.

Table 13-6 IPv6 ACE fields

13.7 ACL Binding

To display ACL Binding Setting web page, click **ACL** > **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 interface simultaneously.

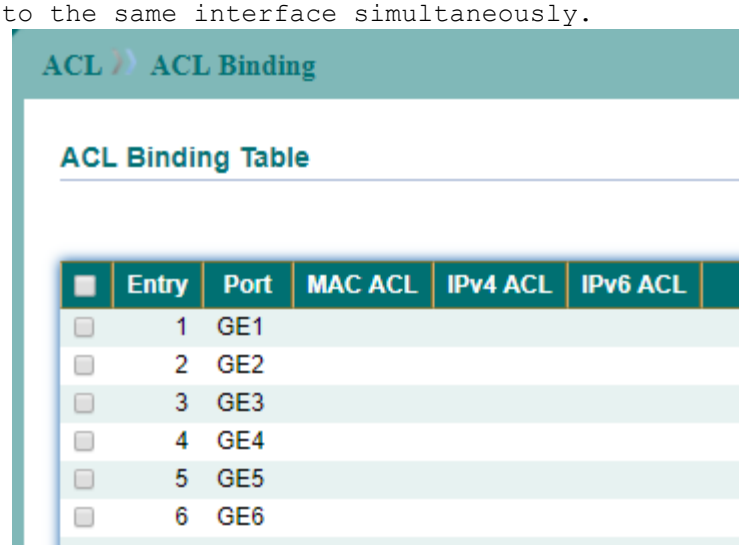


Figure 13-12 ACL Binding page

Select entry and click "Bind" button to bind ACL entries.

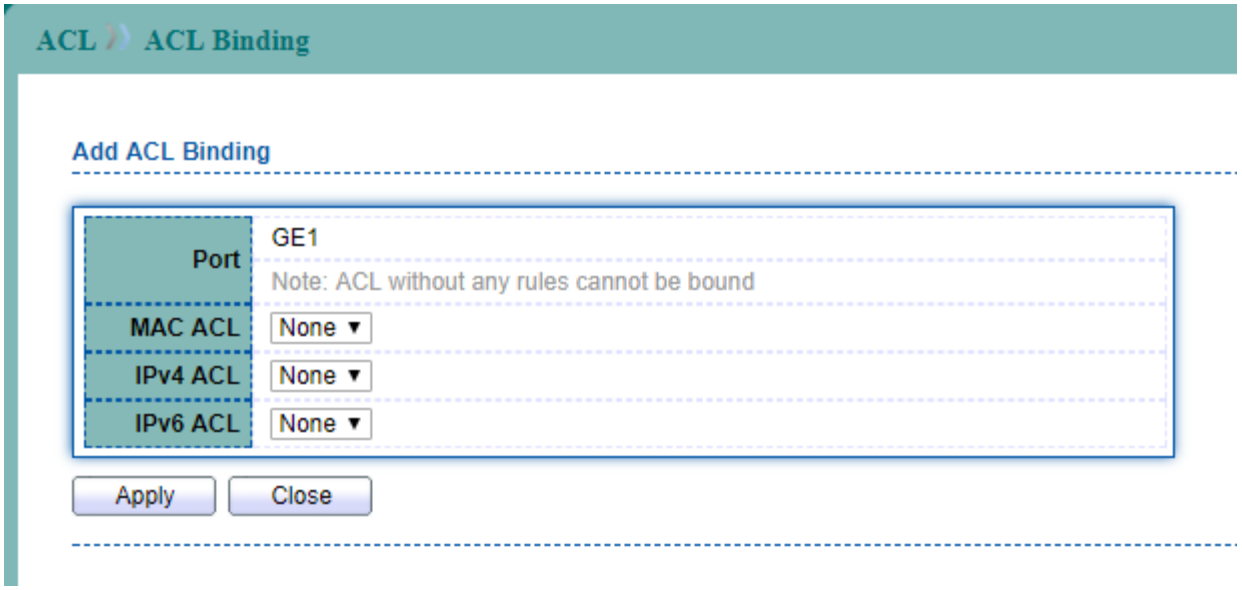


Figure 13-13 Add ACL Binding page

Field	Description
Port	The port number to bind ACL entries.
MAC ACL	The name of MAC ACL.
IPv4 ACL	The name of IPv4 ACL
IPv6 ACL	The name of IPv6 ACL

Table 13-7 IPv6 ACL fields

14 QoS

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

14.1 General

14.1.1 *Property*

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

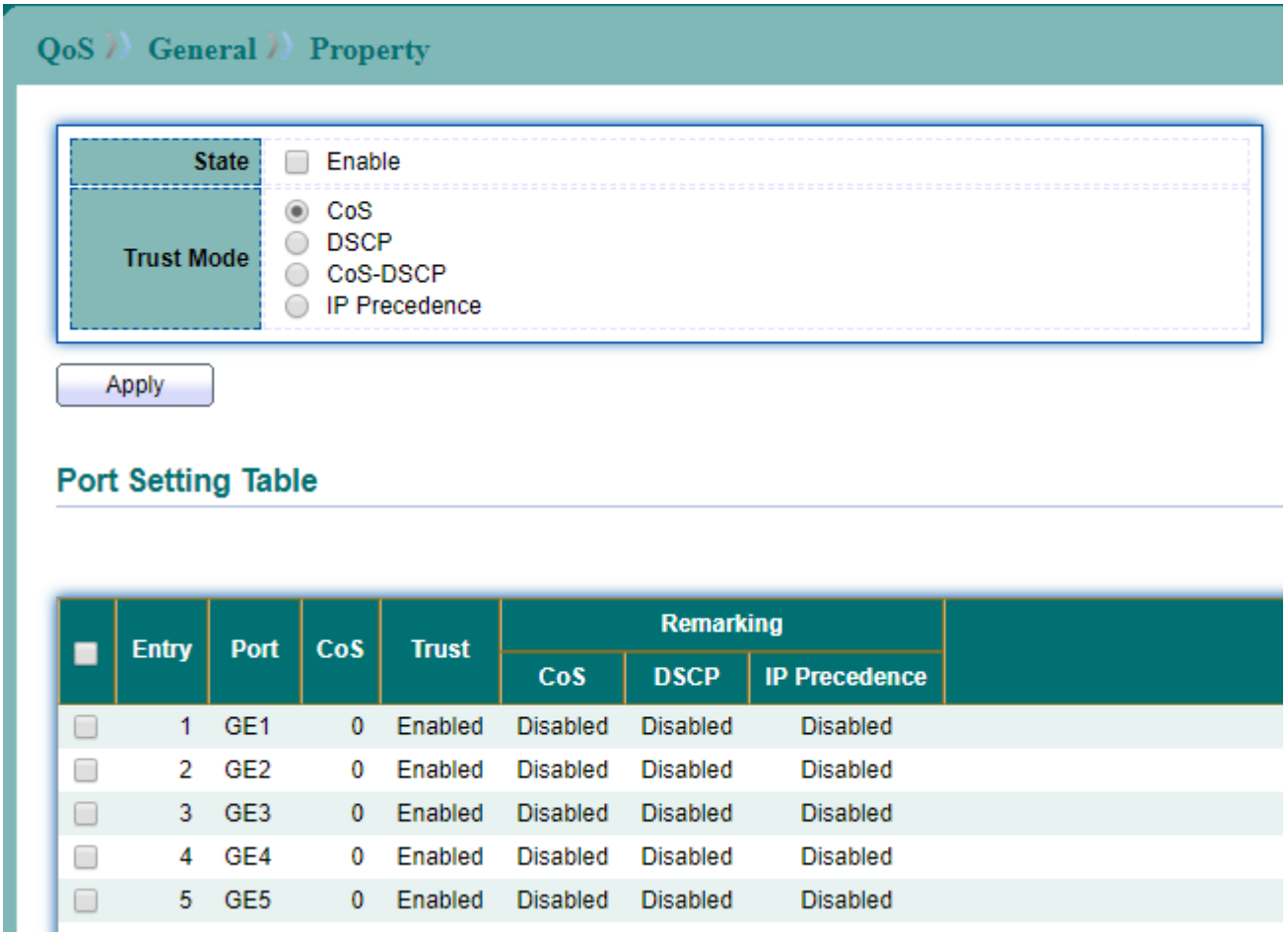


Figure 14-1 QoS Property page

Select entry and click "Edit" button to configure QoS Property Port Setting entry.

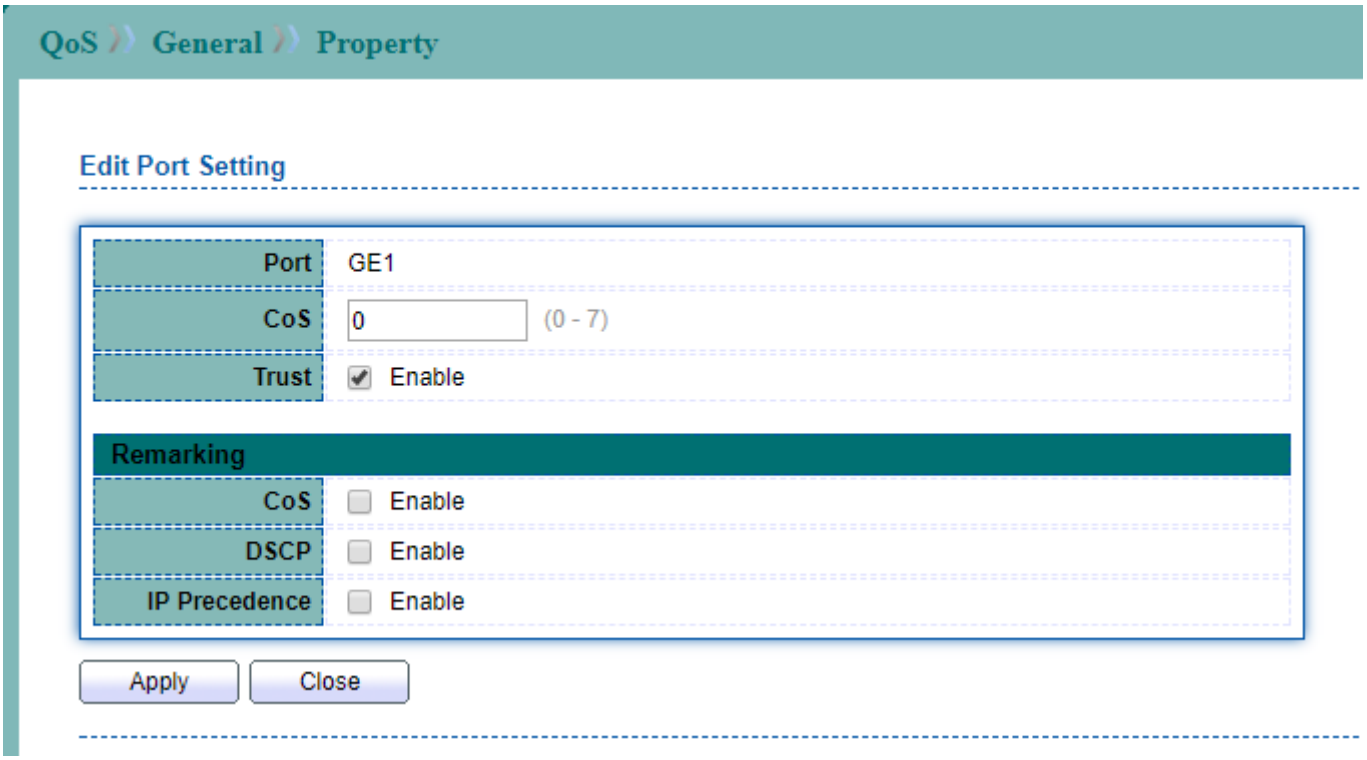


Figure 14-2 Edit QoS Property page

Field	Description
State	Enable/Disable QoS
Trust Mode	Select one type as trust mode.
Port	The port number to configure QoS property.
CoS	Specify the CoS/802.1p priority value.
Trust	Enable/Disable trust mode for the specified port.
Remarking CoS	Enable/Disable CoS remark
Remarking DSCP	Enable/Disable DSCP remark
Remarking IP Precedence	Enable/Disable IP Precedence remark

Table 14-1 QoS property fields

14.1.2 *Queue Scheduling*

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

When queue mode is 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 queue mode is WRR, queues are serviced until their quota has been used up and then another queue is serviced.

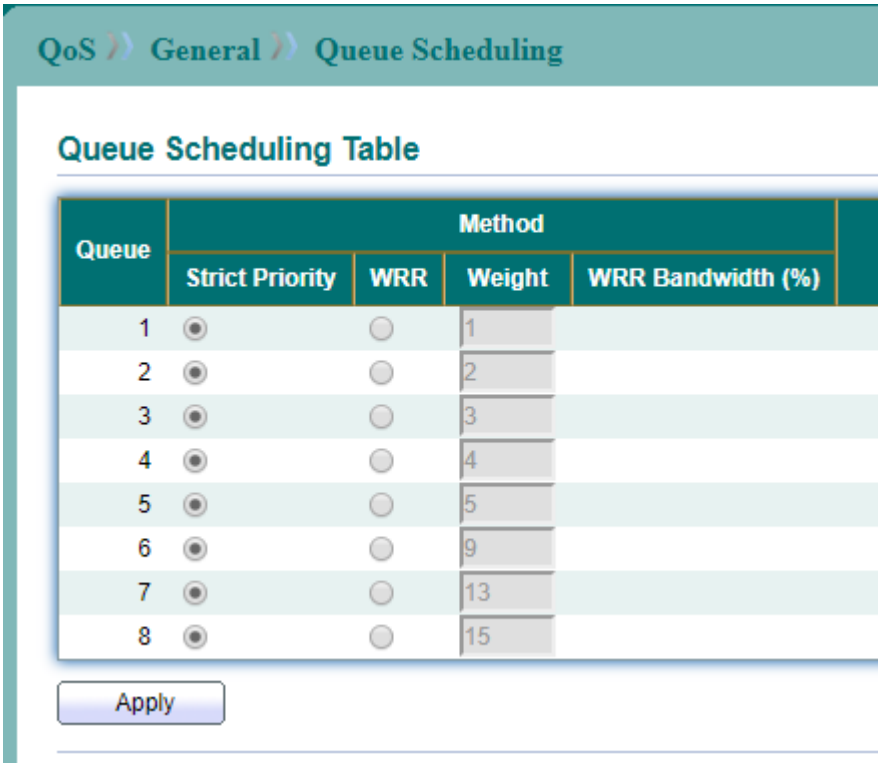


Figure 14-3 QoS Scheduling page

Field	Description
Queue	Specify queue ID
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	The bandwidth when the queue type is WRR.

Table 14-2 QoS scheduling fields

14.1.3 *CoS Mapping*

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

The CoS to Queue table determines the egress queues of the incoming packets based on the 802.1p priority in the VLAN tags.
Use the Queues to CoS table to remark the CoS/802.1p priority for egress traffic from each queue.

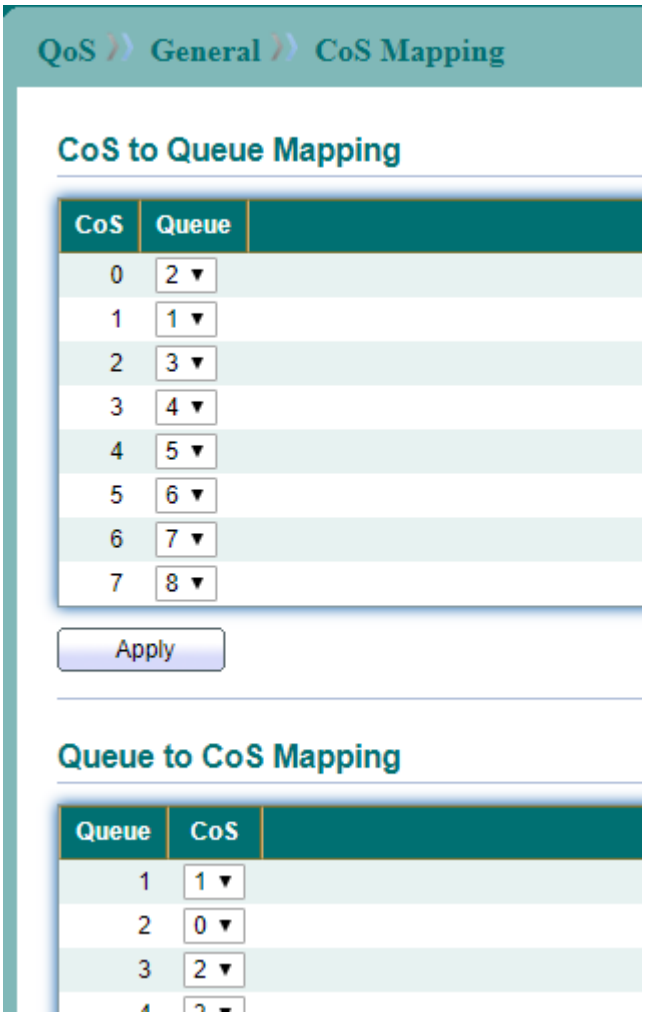


Figure 14-4 CoS Mapping page

Field	Description
CoS	CoS value
Queue	Queue ID

Table 14-3 CoS Mapping fields

14.1.4 *DSCP Mapping*

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

The DSCP to Queue table determines the egress queues of the incoming IP packets based on the DSCP value.
Use the Queues to DSCP table to remark the DSCP value for egress traffic from each queue.

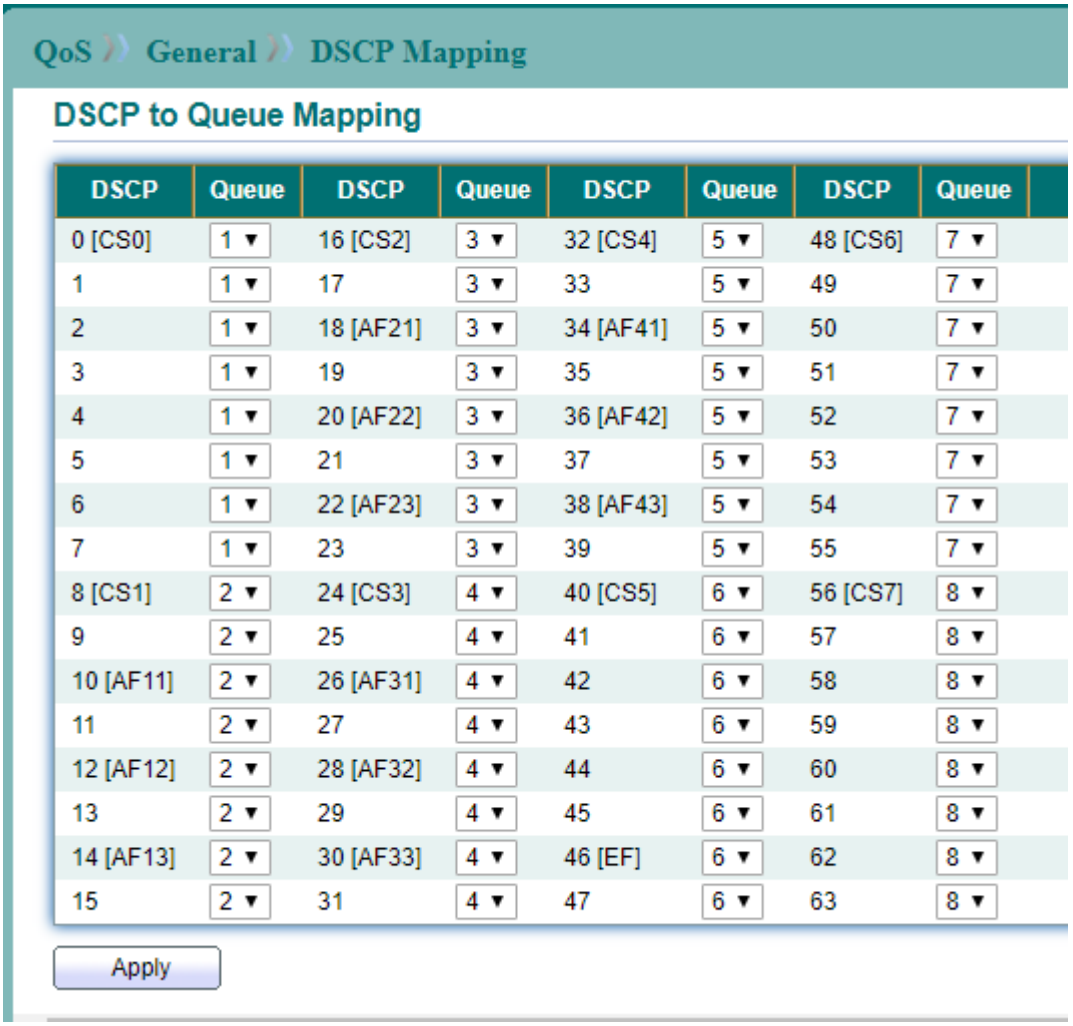


Figure 14-5 DSCP to Queue Mapping page

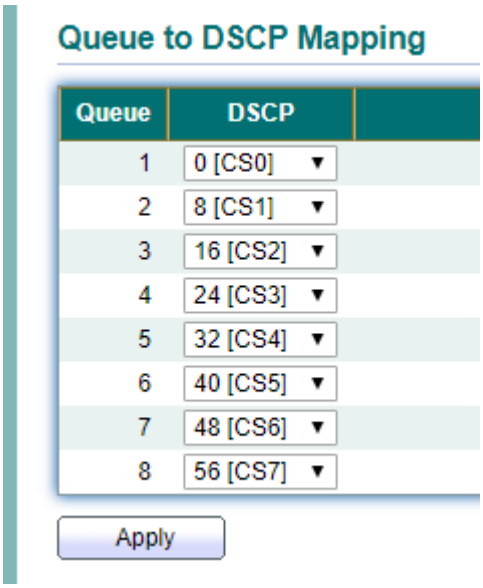


Figure 14-6 Queue to DSCP Mapping page

Field	Description
DSCP	DSCP value
Queue	Queue ID

Table 14-4 DSCP Mapping fields

14.1.5 *IP Precedence Mapping*

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

The IP Precedence to Queue table determines the egress queues of the incoming IP packets based on the IP Precedence value.
Use the Queues to IP Precedence table to remark the IP Precedence value for egress traffic from each queue.

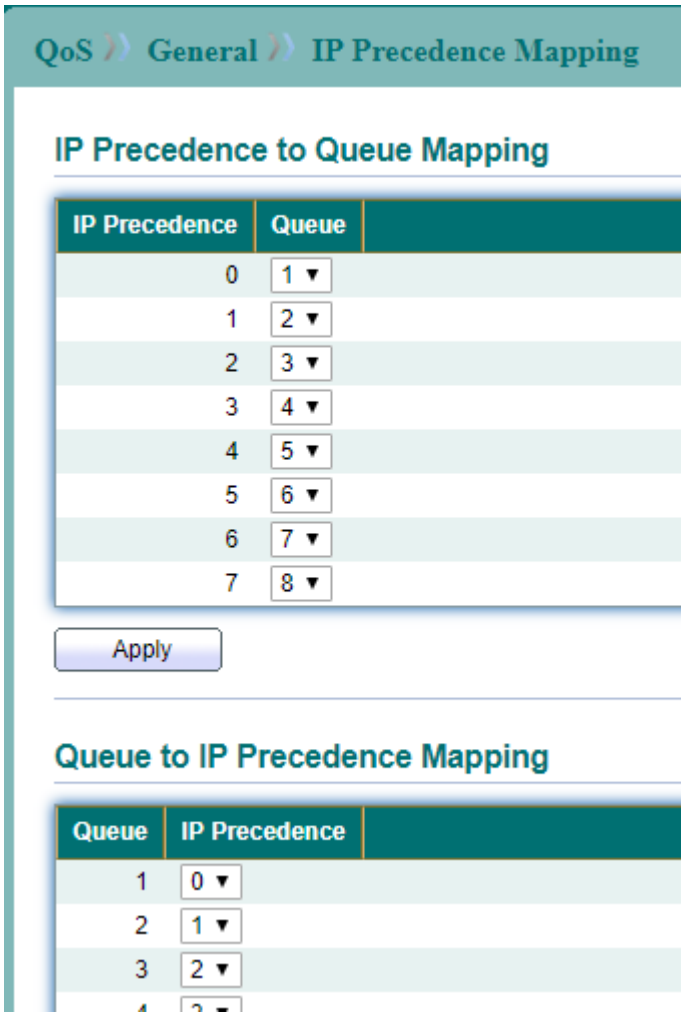


Figure 14-7 IP Precedence Mapping page

Field	Description
IP Precedence	IP Precedence value
Queue	Queue ID

Table 14-5 IP Precedence Mapping fields

14.2 Rate Limit

14.2.1 *Ingress/Egress Port*

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

Use the Ingress/Egress Port pages to define values that determine how much traffic the switch can receive and send.
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.
Egress rate limiting is performed by shaping the output load.

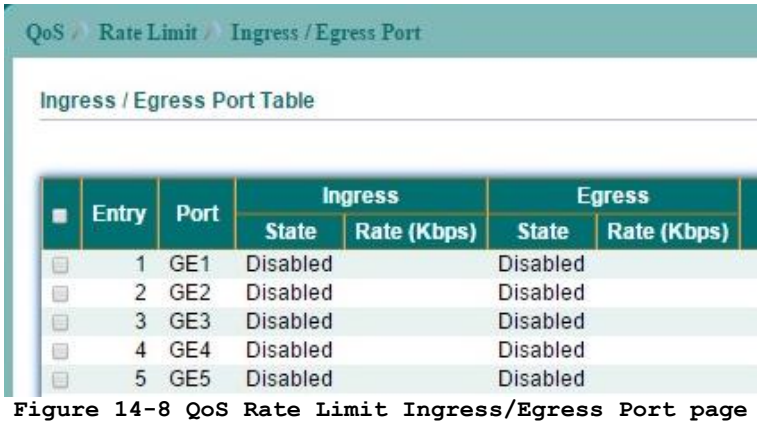


Figure 14-8 QoS Rate Limit Ingress/Egress Port page

Select entry and click "Edit" button to configure Rate Limit Ingress/Egress Port entry.

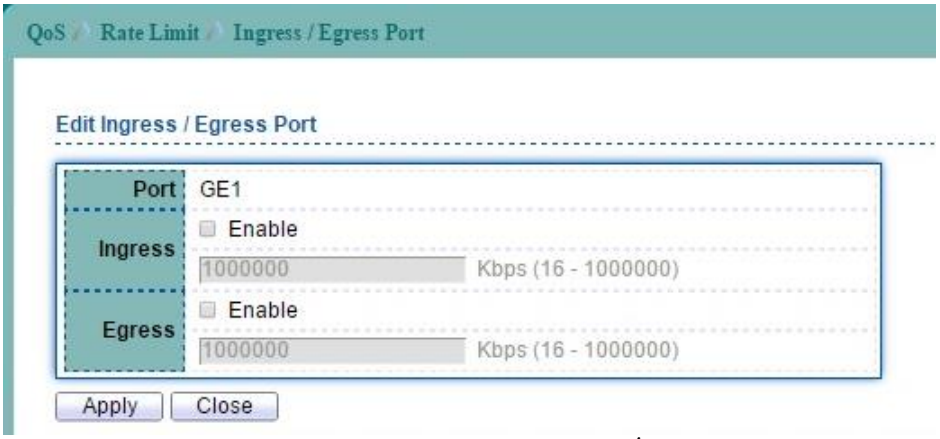


Figure 14-9 Edit QoS Rate Limit Ingress/Egress Port page

Field	Description
Port	Selected ports.
Ingress	**Enable:** Enable ingress bandwidth control. **Rate:** Rate value,<16-1000000>,unit:16 Kbps, if input rate is not multiple of 16, it will change it to multiple of 16 automatically
Egress	**Enable:** Enable egress bandwidth control. **Rate:** Rate value,<16-1000000>,unit:16 Kbps, if input rate is not multiple of 16, it will change it to multiple of 16 automatically

Table 14-6 QoS Rate Limit Ingress/Egress Port fields

14.2.1 Egress Queue

To display Egress Queue Control web page, click **QoS** > **Rate Limit** > **Egress Queue.**

The switch can limit the transmission rate of selected egressing frames on a per-queue per-port basis.

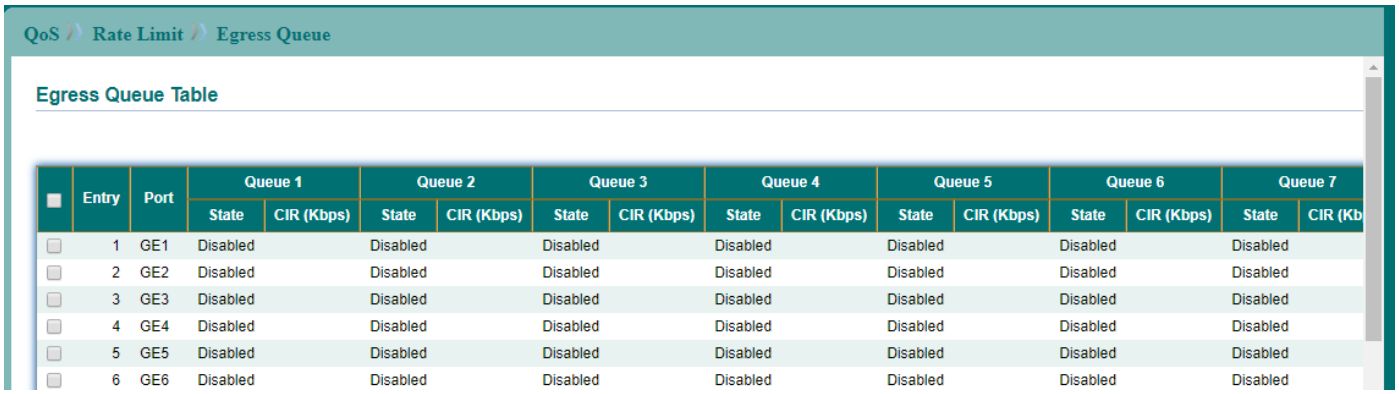


Figure 14-10 Egress Queue page

Select entry and click "Edit" button to configure Rate Limit Egress Queue entry.

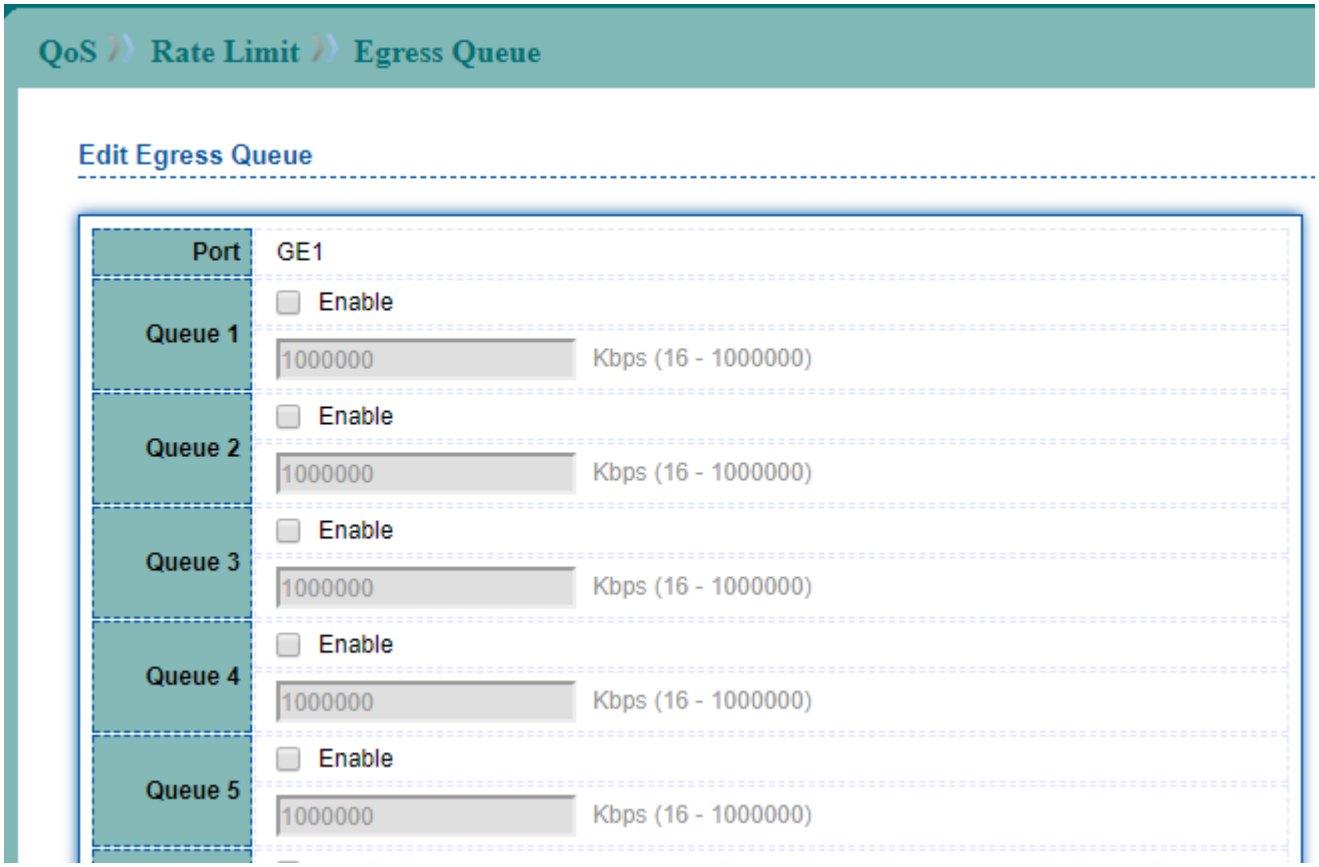


Figure 14-11 Edit Egress Queue page

Field	Description
Port	Selected ports.
Queue	Selected queue.
State	Enable/Disable ingress bandwidth control for the port and queue.
CIR	Rate value,<16-1000000>,unit:16 Kbps, if input rate is not multiple of 16, it will change it to multiple of 16

	automatically

Table 14-7 Egress Queue fields

15 Diagnostics

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

15.1 Logging

15.1.1 *Logging Property*

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

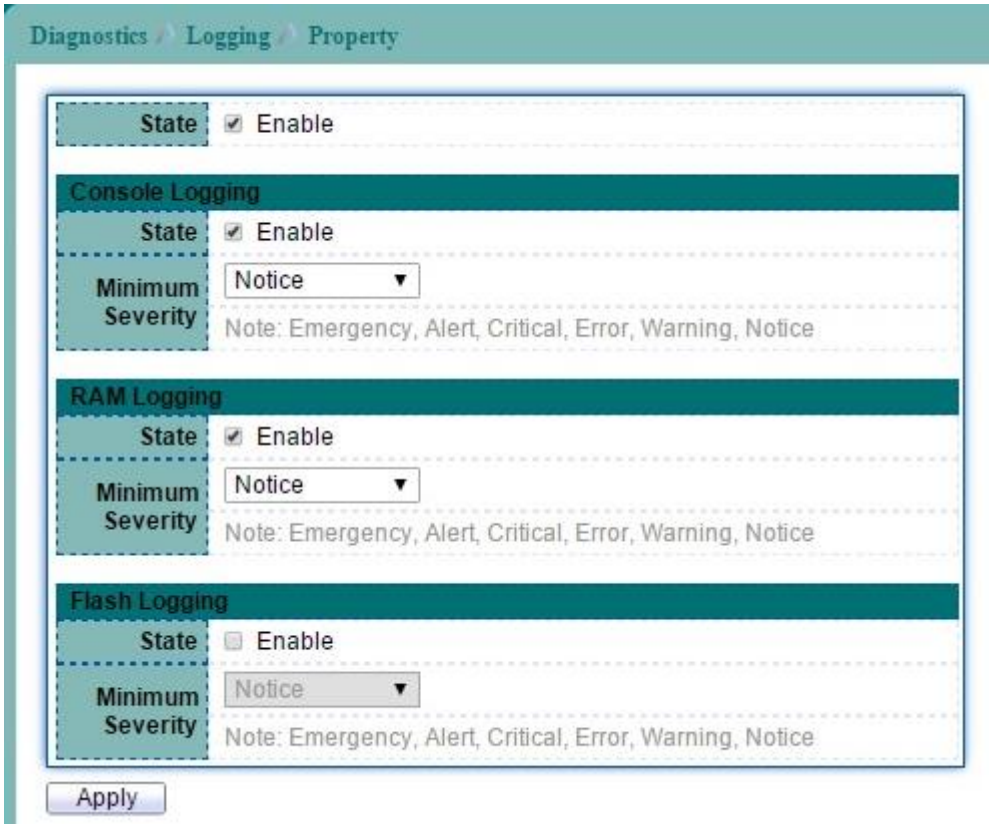


Figure 15-1 Logging Property page

Field	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	**Enable:** Print the logging messages on the console. **Minimum Severity:** Specify the minimum severity of the logging messages. ● **Emergency:** 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. ● **Information:** Device information. ● **Debug:** Provides detailed information about an event.
RAM Logging	**Enable:** Store the logging messages on the RAM. **Minimum Severity:** Specify the minimum severity of the logging messages.

	• **Emergency:** 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. • **Information:** Device information. • **Debug:** Provides detailed information about an event.
Flash Logging	**Enable:** Store the logging messages on the Flash. **Minimum Severity:** Specify the minimum severity of the logging messages. • **Emergency:** 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. • **Information:** Device information. • **Debug:** Provides detailed information about an event.

Table 15-1 Logging Property fields

15.1.2 Remote Server

To configure the remote logging service, click **Diagnostics** > **Logging** > **Remote Server**.

Figure 15-2 Logging Remote Server page

Click "Add" button to create a new Logging Remote Server entry.

Figure 15-3 Add Logging Remote Server page

Field	Description
Address Type	IPv4/IPv6 address or hostname of the remote logging server.
Server Address	Logging Server IP address or hostname.
Server Ports	Specify the port number of the remote logging server. The valid range is from 0 to 65535, and the default value is 514.
Facility	Specify the facility of the logging messages. It can be one of the following value: local0, local1, local2, local3, local4, local5, local6, and local7.
Minimum Severity	Specify the minimum severity of the logging messages. ● **Emergency:** 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. ● **Information:** Device information. ● **Debug:** Provides detailed information about an event.

Table 15-2 Logging Remote Server fields

15.2 Mirroring Setting

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

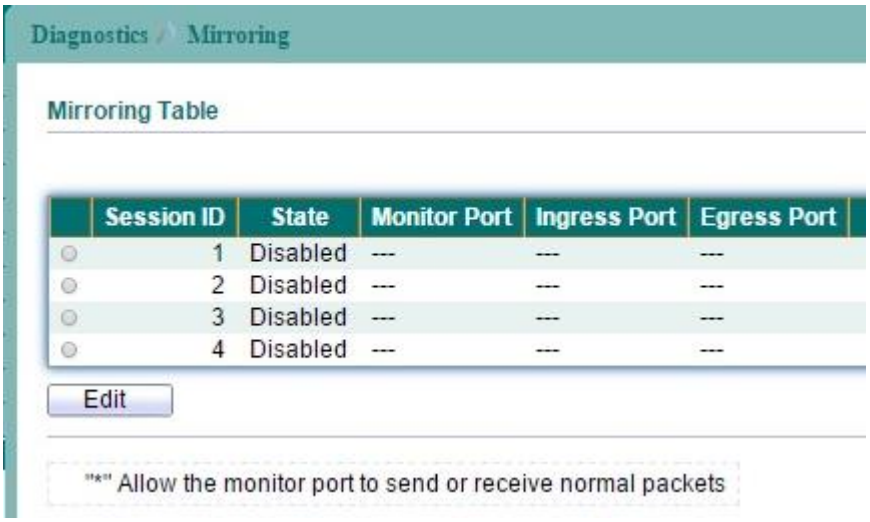


Figure 15-4 Mirroring page

Select entry and click "Edit" button to configure Mirroring entry.

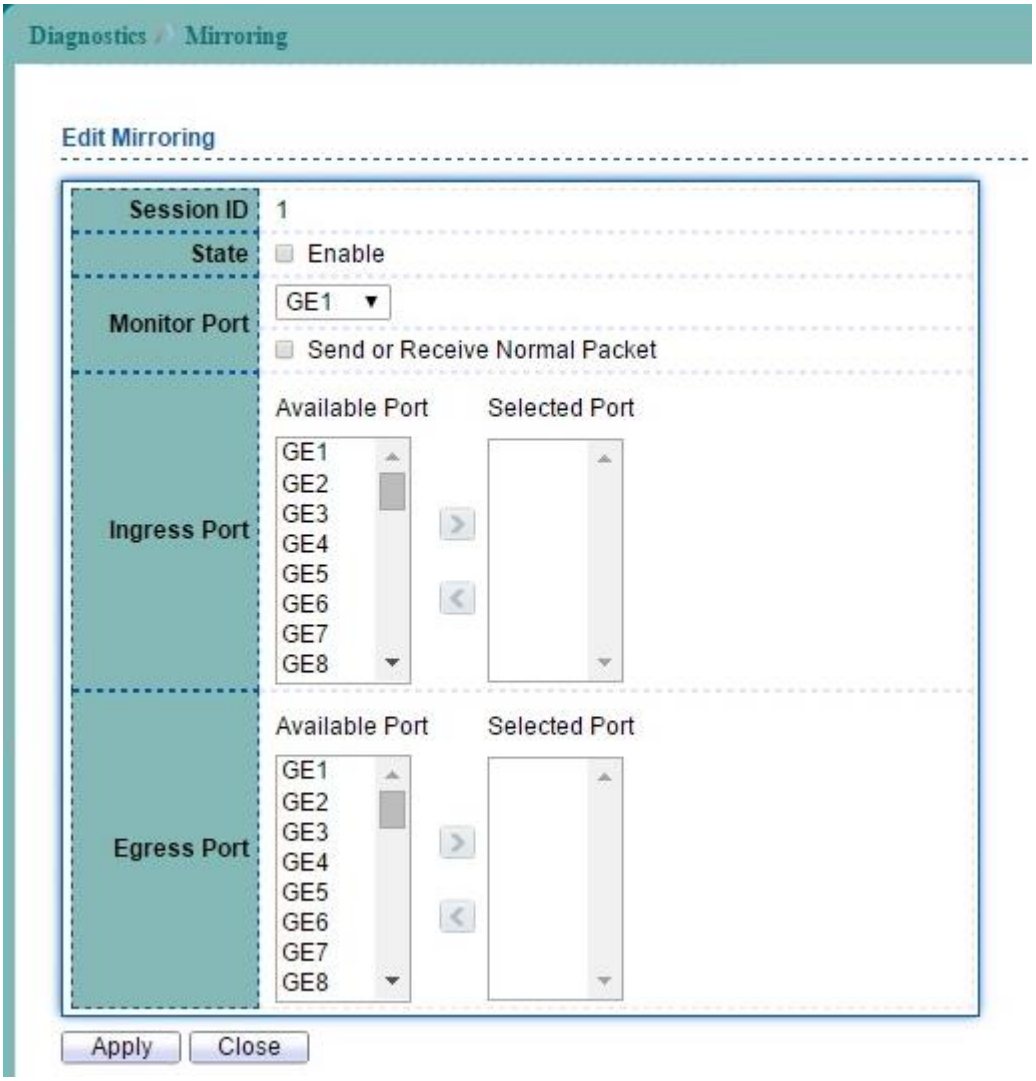


Figure 15-5 Edit Mirroring page

Field	Description
Session ID	Select mirror session ID
State	Enabled: Enable port based mirror
Monitor Port	Select mirror session destination port
Ingress ports	Select mirror session source Ingress (rx) ports.
Egress ports	Select mirror session source Egress (tx) ports

Table 15-3 Mirroring fields

15.3 Ping

To use the ping test functionality, click **Diagnostics** > **Ping**.

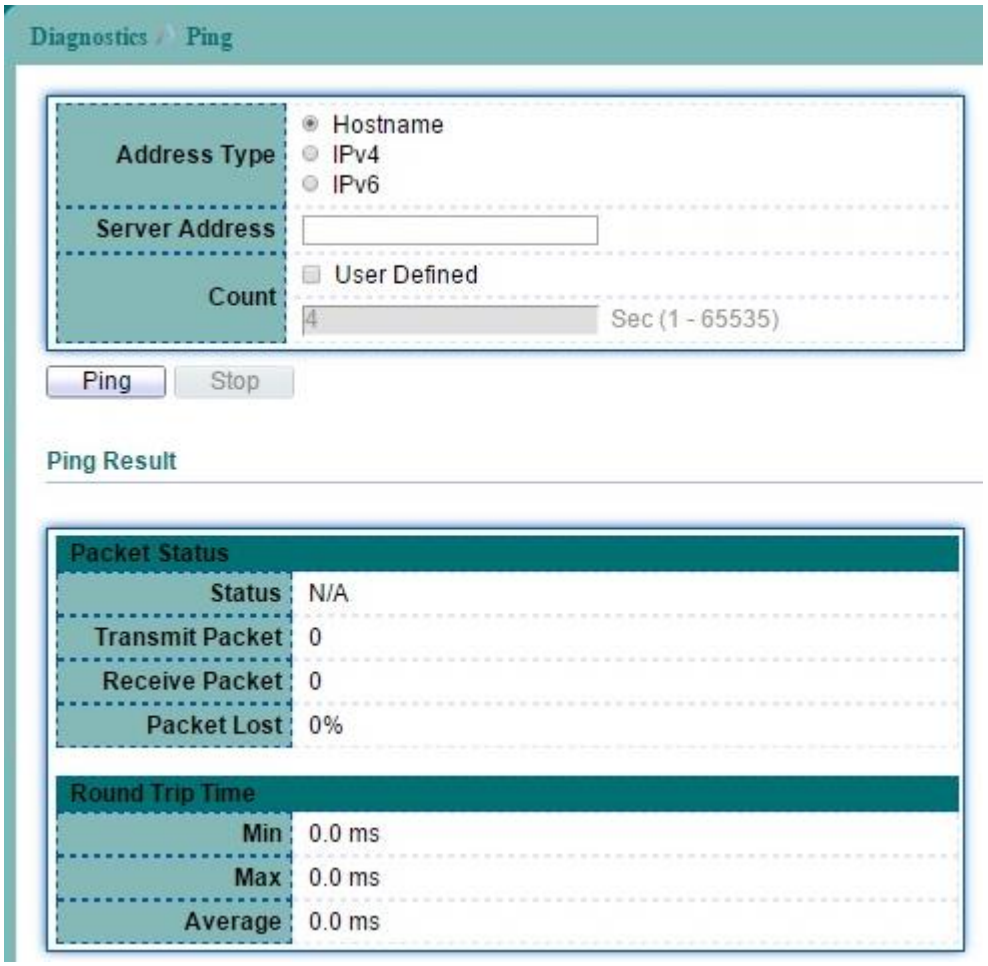


Figure 15-6 Ping page

Field	Description
Address Type	Specify the IP Type.
Server Address	Specify the IPv4/IPv6 address or Hostname.
Count	User Define: Specify the total numbers of ICMP ping packets to be sent.
Ping Results	The field for the result of the ICMP ping test.

Table 15-4 Ping fields

15.4 Traceroute

To use the trace route functionality, click **Diagnostics** > **Traceroute.**

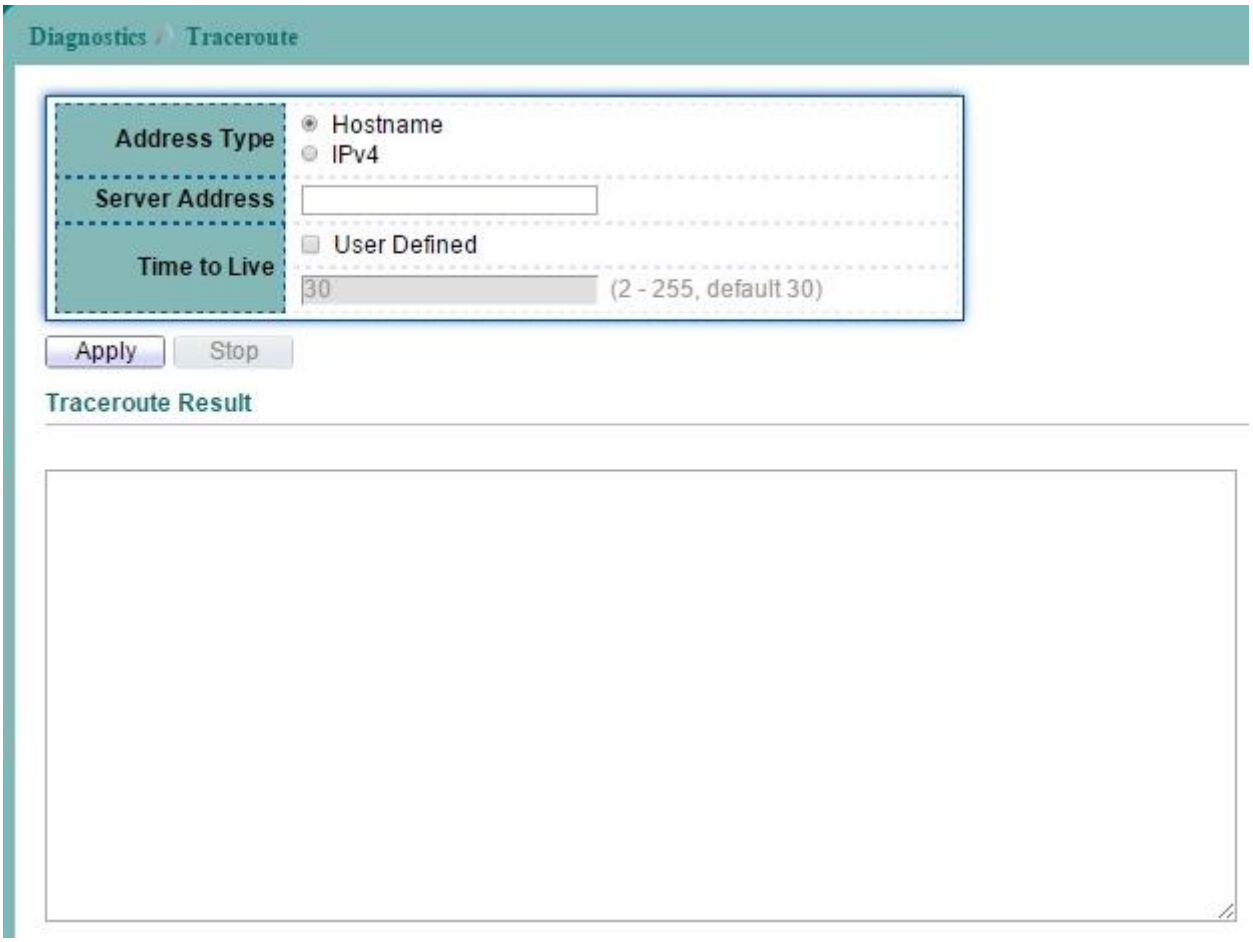


Figure 15-7 Traceroute page

Field	Description
Address Type	Specify the IP Type of IPv4or Hostname.
Server Address	Specify the IPv4/IPv6 address or the hostname.
Time to Live	Specify the Time to Live of hosts for trace route.

Table 15-5 Traceroute fields

15.5 Copper Test

To perform the copper length diagnostic, click **Diagnostics** > **Copper Test.**

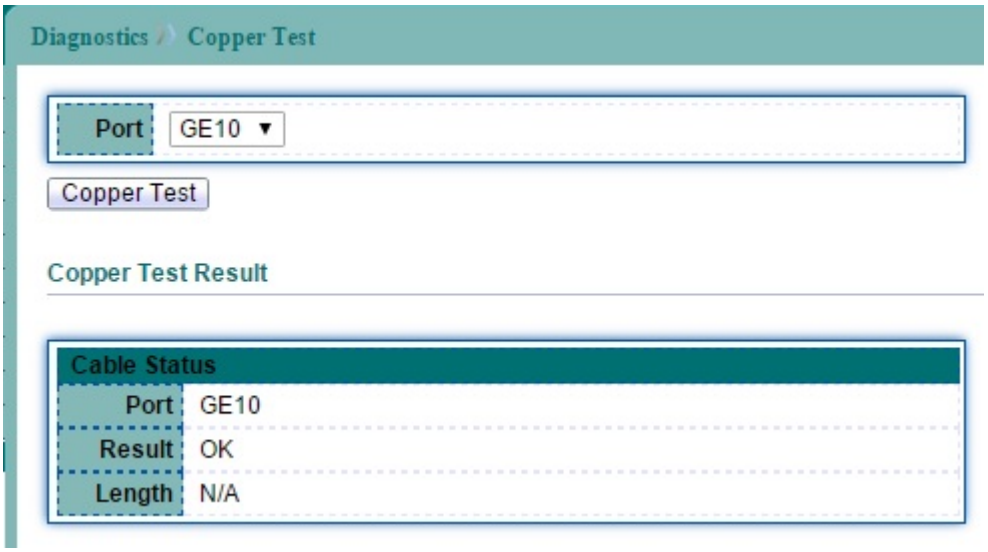


Figure 15-8 Copper Test page

Field	Description
Port	Interface or port number.
Cooper Test Result	
Port	Selected Port.
Result	Display whether port test is Pass or Fail. ● **OK:** cable is normal. ● **Short Cable:** A short is detected on the cable. ● **Open Cable:** An opening is detected on the cable. One scenario is the cable doesn't plug to the line partner. ● **Impedance Mismatch:** The impedance is mismatched. ● **Line Drive:** The high impedance is detected. One scenario is the cable plug to a power down link partner.
Length	Distance in meter from the port to the location on the cable where the fault was discovered.

Table 15-6 Copper Test fields

15.6 Fiber Module

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

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

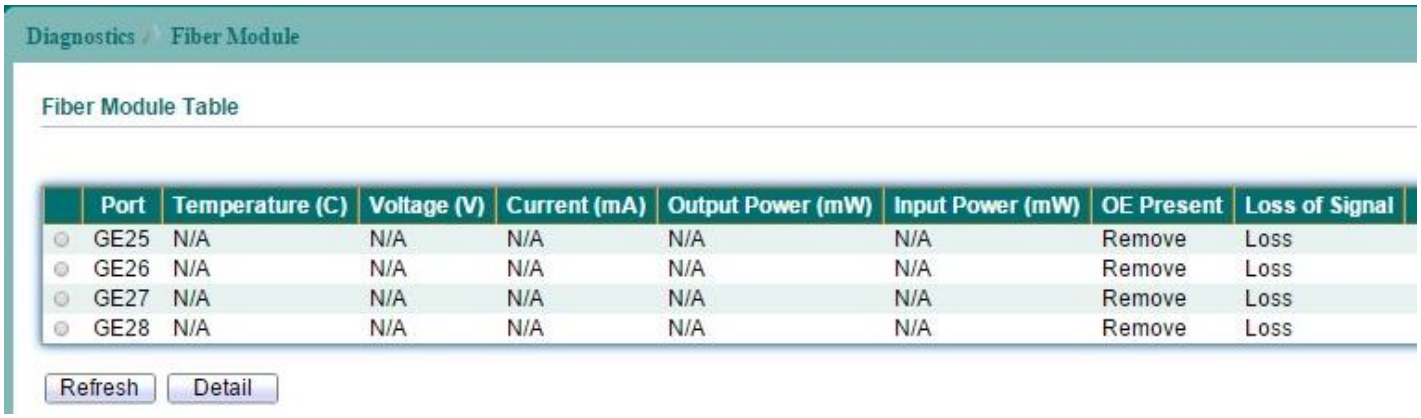


Figure 15-9 Fiber Module page

Field	Description
Port	Interface or port number.
Temperature	Internally measured transceiver temperature.
Voltage (V)	Internally measured supply voltage.
Current (mA)	Measured TX bias current.
Output Power (mW)	Measured TX output power in milliwatts.
Input Power (mW)	Measured RX received power in milliwatts.
Data Ready	Indicate transceiver has achieved power up and data is ready.
Transmitter Fault	State of TX fault.
Loss of Signal	Loss of signal.

Table 15-7 Fiber Module fields

15.7 UDLD

15.7.1 UDLD Property

To configure the Unidirectional Link Detection (UDLD), click **Diagnostics** > **UDLD** > **Property**.

User can UDLD function to detect the unidirectional link exits on the network. All connected devices must support UDLD protocol to make this function successfully.

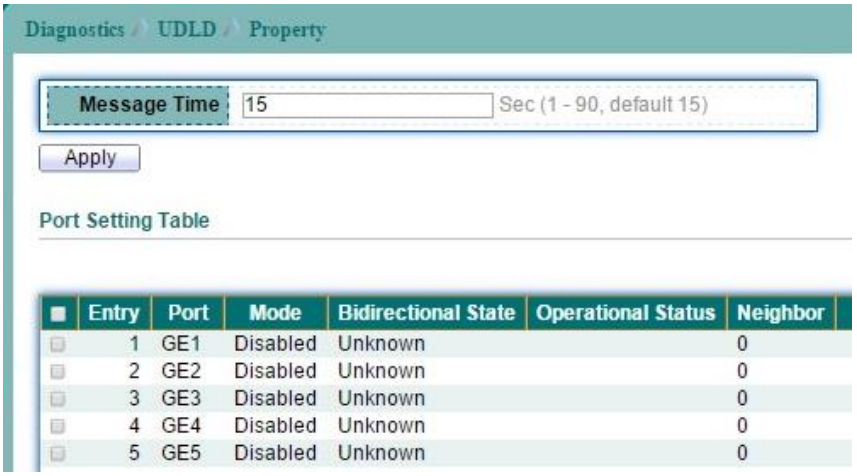


Figure 15-10 UDLD Property page

Select entry and click "Edit" button to configure UDLD Port Setting entry.

Figure 15-11 Edit UDLD Property page

Field	Description
Port	Port number.
Mode	UDLD Mode.
Bidirectional State	Bidirectional State information.
Operational Status	Operational State information.
Neighbor	UDLD Neighbor information.
Edit Port Setting	
Port	Selected port.
Mode	Select one of UDLD Modes or disable it. • **Normal**: UDLD Normal mode; use to detect unidirectional links due to misconnected interface on fiber-optical connection. • **Aggressive**: UDLD Aggressive mode: use to detect unidirectional links due to misconnected interface on fiber-optical connection and unidirectional links due to one-way traffic on fiber-optic and twisted-pair links.

Table 15-8 UDLD Property fields

15.7.2 UDLD Neighbor

To display the Unidirectional Link Detection (UDLD) Neighbor information, click **Diagnostics** > **UDLD** > **Neighbor**.

Figure 15-12 UDLD Neighbor page

16 Management

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

16.1 User Account

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

The default username/password is switch/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.

Figure 16-1 User Account page

Click "Add" button to create a new User Account entry.

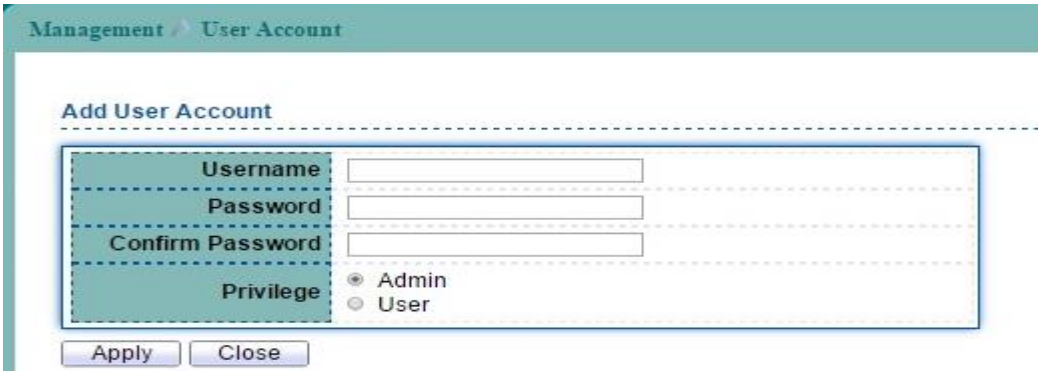


Figure 16-2 Add User Account page

Field	Description
User Name	User name for new account.
Password	Specify a password for the user account.
Confirm Password	Retype password to make sure the password is exactly you typed before in "Password" field.
Privilege	Select privilege level for new account. • **Admin:** Allow to change switch settings. • **User:** See switch settings only. Not allow to change it.

Table 16-1 Add User Account fields

16.2 Firmware

16.2.1 Upgrade/Backup

To display Upgrade/Backup Manager web page, click **Management** > **Firmware** > **Upgrade/Backup**.

This page allow user to Upgrade/backup the firmware image on the switch to remote TFTP server or host file system through HTTP protocol.

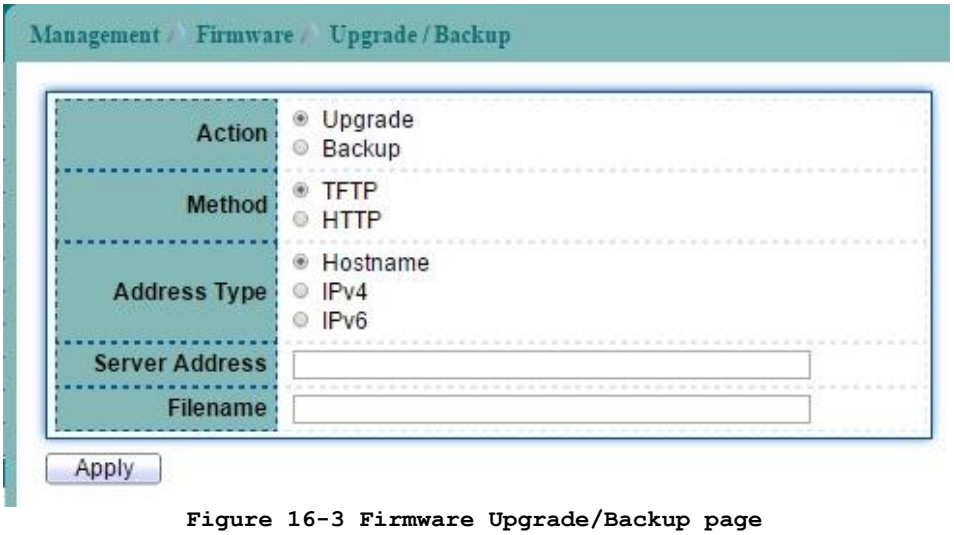


Figure 16-3 Firmware Upgrade/Backup page

Figure 16-4 Firmware Upgrade/Backup page

Field	Description
Action	Select an Action to Upgrade or Backup the firmware.
Method	Select upgrade/backup method. ● **TFTP:** Use TFTP to upgrade/backup. ● **HTTP:** Use HTTP to upgrade/backup.
TFTP	
Address Type	Server Address Type ● **Host name:** Use host name as server address. ● **IPv4 address:** Use IPv4 address as server address. ● **IPv6 address:** Use IPv6 address as server address.
Server Address	IP address of the TFTP server. If the TFTP backup method is selected, the IP address of the TFTP server must be assigned.
Filename	Firmware image or configuration file name on remote TFTP server. If the TFTP upgrade method is selected, the file name must be specified.
HTTP	
Filename	If the HTTP upgrade method is selected, the browse file field allow you to select any file on host operating system.

Table 16-2 Firmware Upgrade/Backup fields

16.3 Configuration

16.3.1 Upgrade/Backup

To display Upgrade/Backup Manager web page, click **Management** > **Configuration** > **Upgrade/Backup**.

This page allow user to copy running configuration, startup configuration or backup configuration to startup configuration or backup configuration.

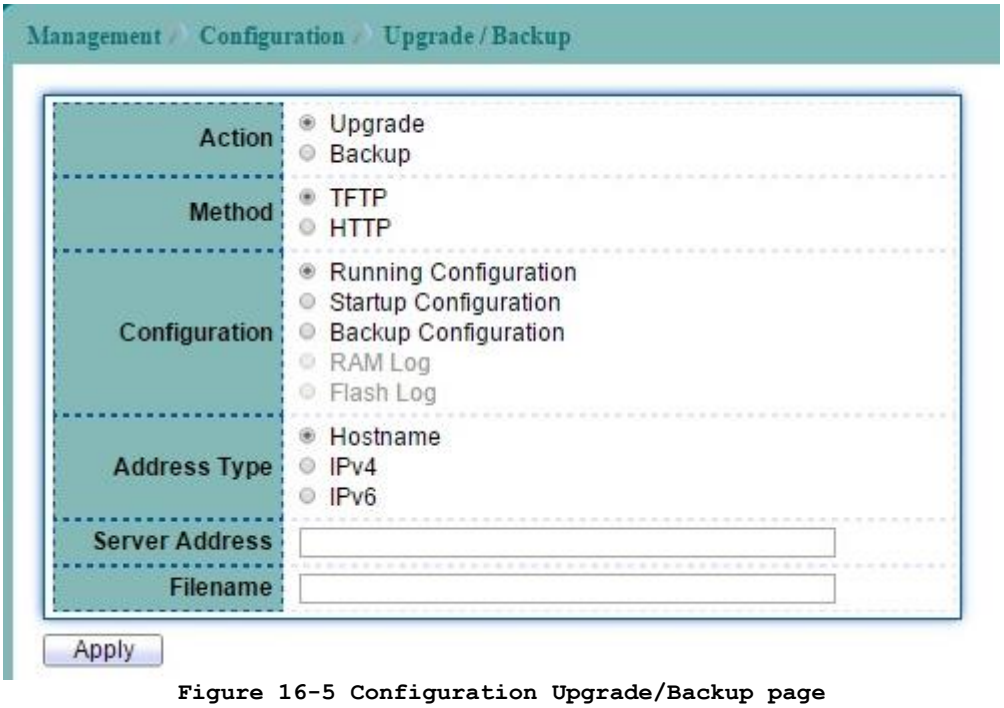


Figure 16-5 Configuration Upgrade/Backup page

Figure 16-6 Configuration Upgrade/Backup page

Field	Description
Action	Select an Action to Upgrade or Backup the configuration file.
Method	Select upgrade/backup method. ● **TFTP:** Use TFTP to upgrade/backup. ● **HTTP:** Use HTTP to upgrade/backup.
Configuration	Select source file type.

	• **Running configuration:** Running configuration file. • **Startup configuration:** Startup configuration file. • **Backup configuration:** Backup configuration file. • **RAM Log:** Backup RAM Log. • **Flash Log:** Backup Flash Log.
TFTP	
Address Type	Server Address Type • **Host name:** Use host name as server address. • **IPv4 address:** Use IPv4 address as server address. • **IPv6 address:** Use IPv6 address as server address.
Server Address	IP address of the TFTP server. If the TFTP backup method is selected, the IP address of the TFTP server must be assigned.
Filename	Configuration file name on remote TFTP server. If the TFTP upgrade method is selected, the file name must be specified.
HTTP	
Filename	If the HTTP upgrade method is selected, the browse file field allow you to select any file on host operating system.

Table 16-3 Configuration Upgrade/Backup fields

16.3.2 Save Configuration

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

This page allow user to copy running configuration, startup configuration or backup configuration to startup configuration or backup configuration. And restore the switch factory default setting.

Figure 16-7 Save Configuration page

Field	Description
Source File	Select source file type. ● **Running configuration:** Running configuration file. ● **Startup configuration:** Startup configuration file. ● **Backup configuration:** Backup configuration file.
Destination File	Select destination file type. ● **Startup Configuration:** Startup configuration file. ● **Backup Configuration:** Backup configuration file.

Table 16-4 Save Configuration fields

16.4 SNMP

16.4.1 SNMP View

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

Figure 16-8 SNMP View page

Click "Add" button to create a new SNMP View entry.

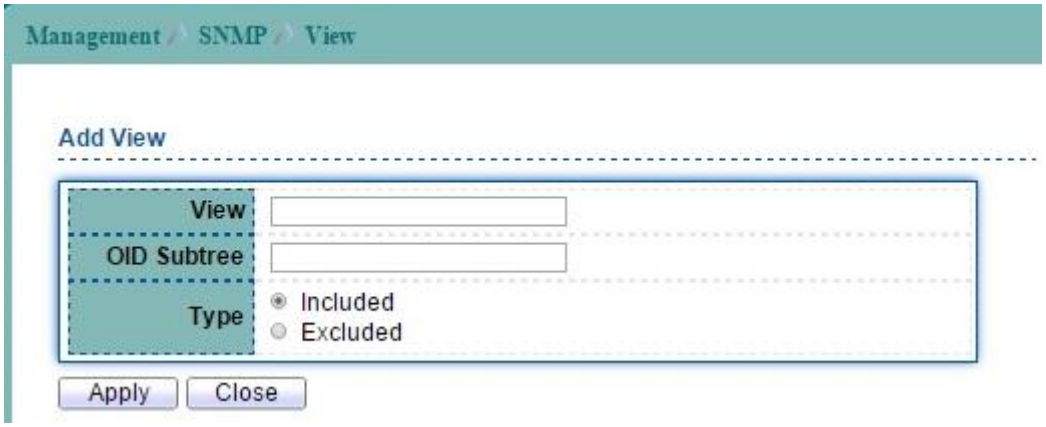


Figure 16-9 Add SNMP View page

Field	Description
View Name	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.

Table 16-5 SNMP View fields

16.4.2 SNMP Group

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

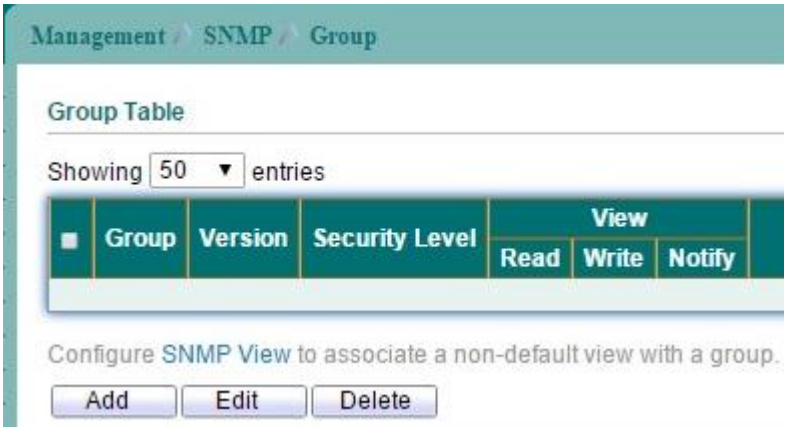


Figure 16-10 SNMP Group page

Click "Add" button to create a new SNMP Group entry.

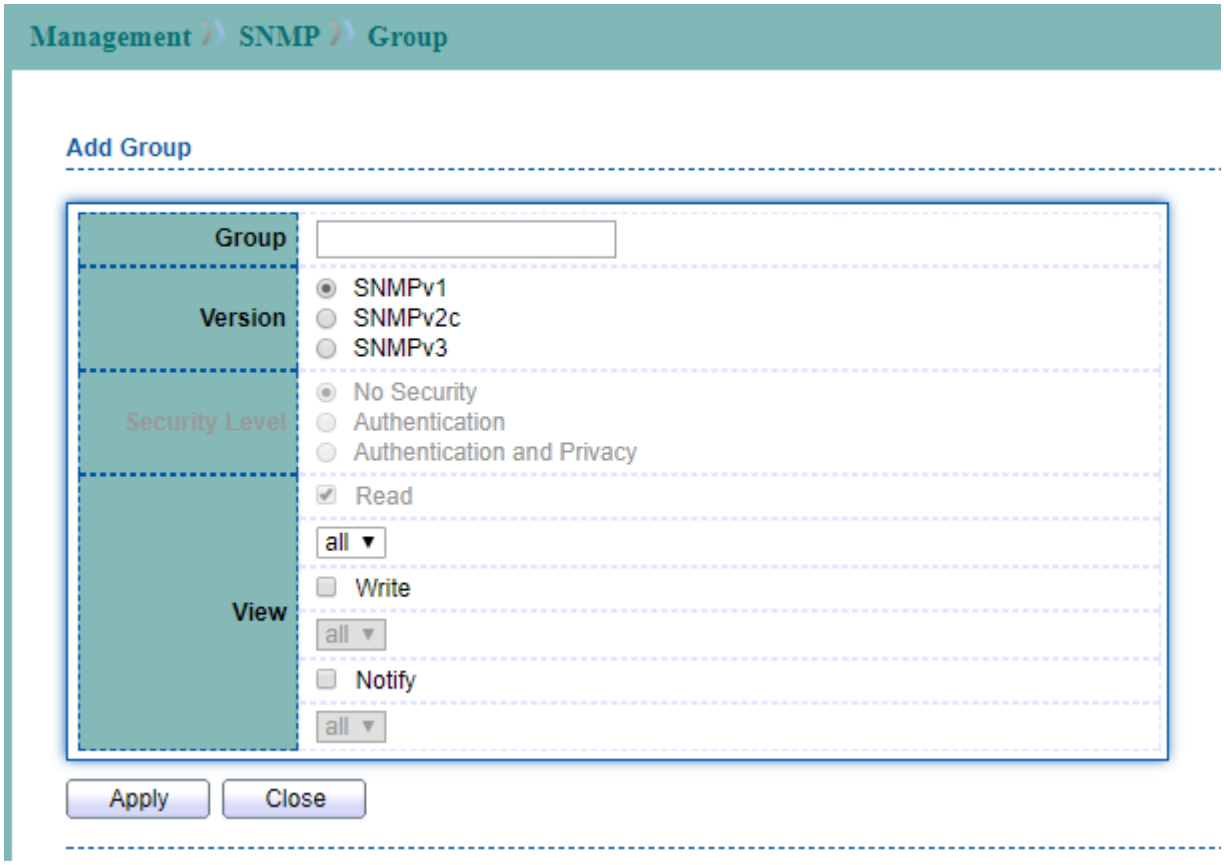


Figure 16-11 Add SNMP Group page

Field	Description
Group Name	Specify SNMP group name, and the maximum length is 30 characters.
Version	Specify SNMP version. ● **SNMPv1:** SNMP version 1. ● **SNMPv2c:** SNMP version 2. ● **SNMPv3:** 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 the view name and enables viewing only. • **Write:** Select the view name and enables configuring the agent. • **Notify:** Select view name that sends only traps with contents that is included in SNMP view selected for notification.

Table 16-6 SNMP Group fields

16.4.3 SNMP Community

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

Figure 16-12 SNMP Community page

Click "Add" button to create a new SNMP Community entry.

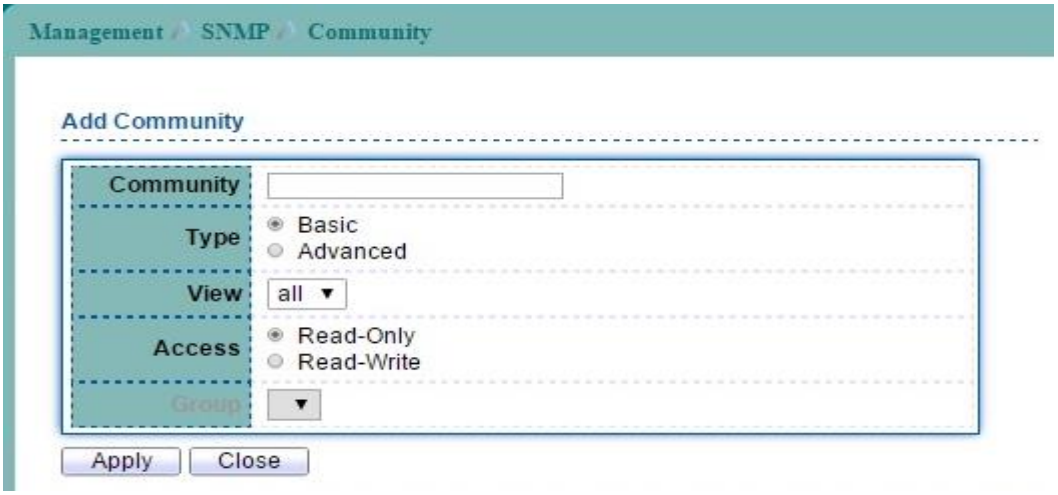


Figure 16-13 Add SNMP Community page

Field	Description
Community Name	The SNMP community name. Its maximum length is 20 characters.
Type	SNMP Community Type. • **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 Right	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.

Table 16-7 SNMP community fields

16.4.4 SNMP User

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

Figure 16-14 SNMP User page

Click "Add" button to create a new SNMP User entry.

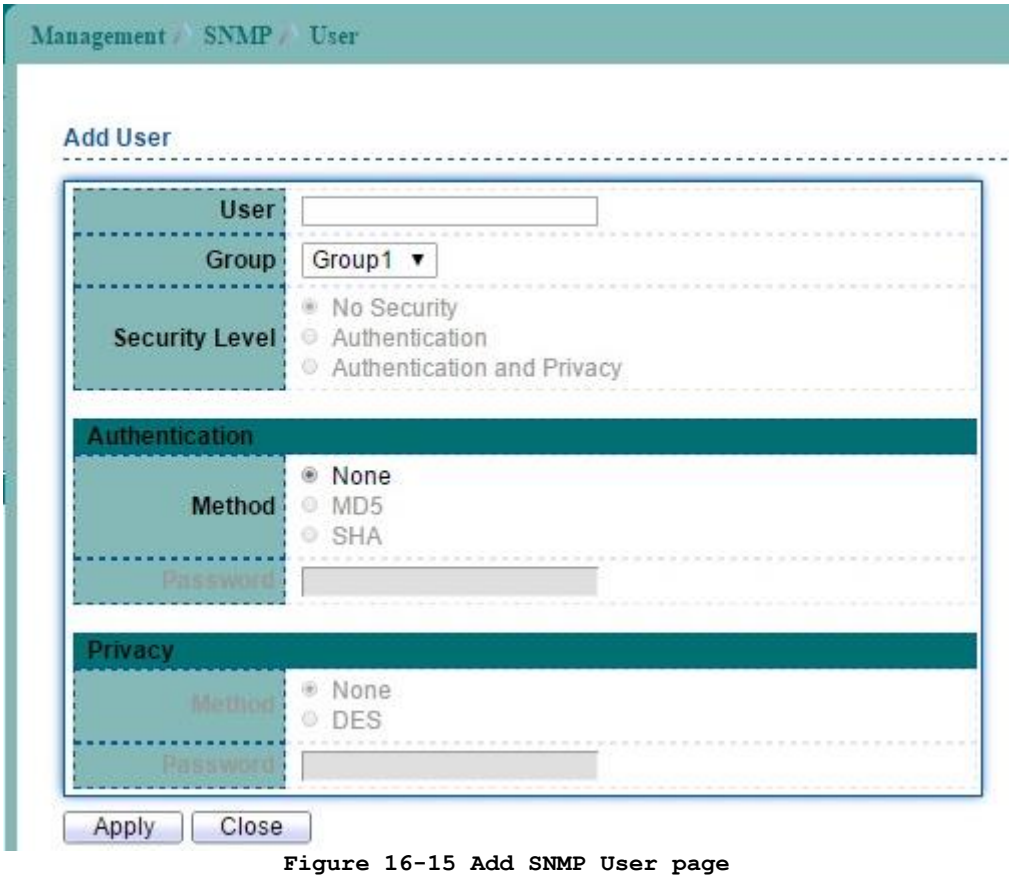


Figure 16-15 Add SNMP User page

Field	Description
User	Specify the SNMP user name on the host that connects to the SNMP agent. The max character is 30 characters. For the SNMP v1 or v2c, the user name must match the community name.
Group	Specify the SNMP group to which the SNMP user belongs.
Authentication	
Method	Authentication Protocol which is available when Privilege Mode is Authentication or privacy. • **None:** No authentication required. • **MD5:** Specify the HMAC-MD5-96 authentication

	protocol. • **SHA**: Specify the HMAC-SHA-96 authentication protocol.
Password	The password for authentication and the range of length is from 8 to 32 characters.
Privacy	
Method	Encryption Protocol • **None**: No privacy required. • **DES**: DES algorithm.
Password	Encryption password. The range of length is from 8 to 64 characters.

Table 16-8 SNMP User fields

16.4.5 SNMP Engine ID

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

Figure 16-16 SNMP Engine ID page

Click "Add" button to create a new SNMP Engine ID entry.

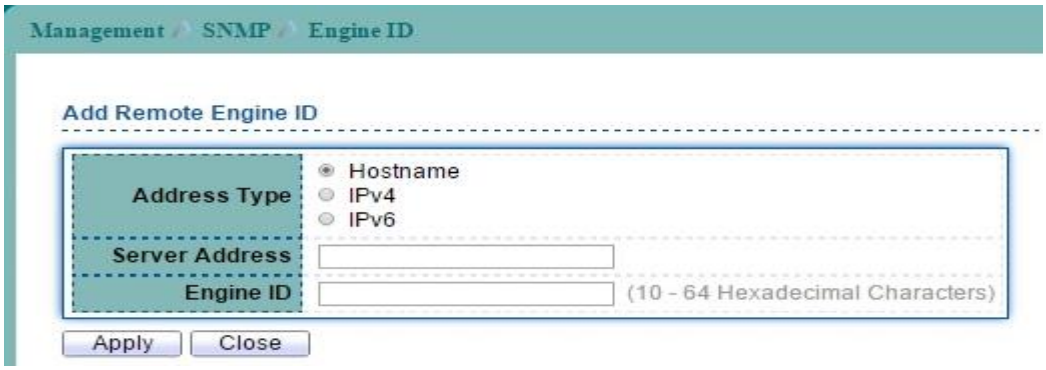


Figure 16-17 Add SNMP Engine ID page

Field	Description
Engine ID	User Defined: Specify SNMP engine ID. The engine ID is the 10 to 64 hexadecimal characters.
Add Remote Engine ID	
Address Type	Server Address Type • **Host name:** Use host name as server address. • **IPv4 address:** Use IPv4 address as server address. • **IPv6 address:** Use IPv6 address as server address.
Server Address	The IP address or the hostname of the SNMP trap recipients.
Engine ID	Specify SNMP engine ID. The engine ID is the 10 to 64 hexadecimal character.

Table 16-9 SNMP Engine ID fields

16.4.6 SNMP Trap Event

To configure SNMP Trap Event, click **Management** > **SNMP** > **Trap Event.**
Switch will send the trap message when one of following condition selected and occurred.

Figure 16-18 SNMP Trap Event page

Field	Description
Authentication Failure	Send the trap message when authentication failed.
Link UP/Down	Send the trap message when port is link up/down.
Cold Start	Send the trap message when system cold start occurred.
Warm Start	Send the trap message when system warm start occurred.

Table 16-10 SNMP Trap Event fields

16.4.7 SNMP Notification

To configure the hosts to receive SNMP notifications, click **Management** > **SNMP** > **Notification.**

Figure 16-19 SNMP Notification page

Click "Add" button to create a new SNMP Notification entry.

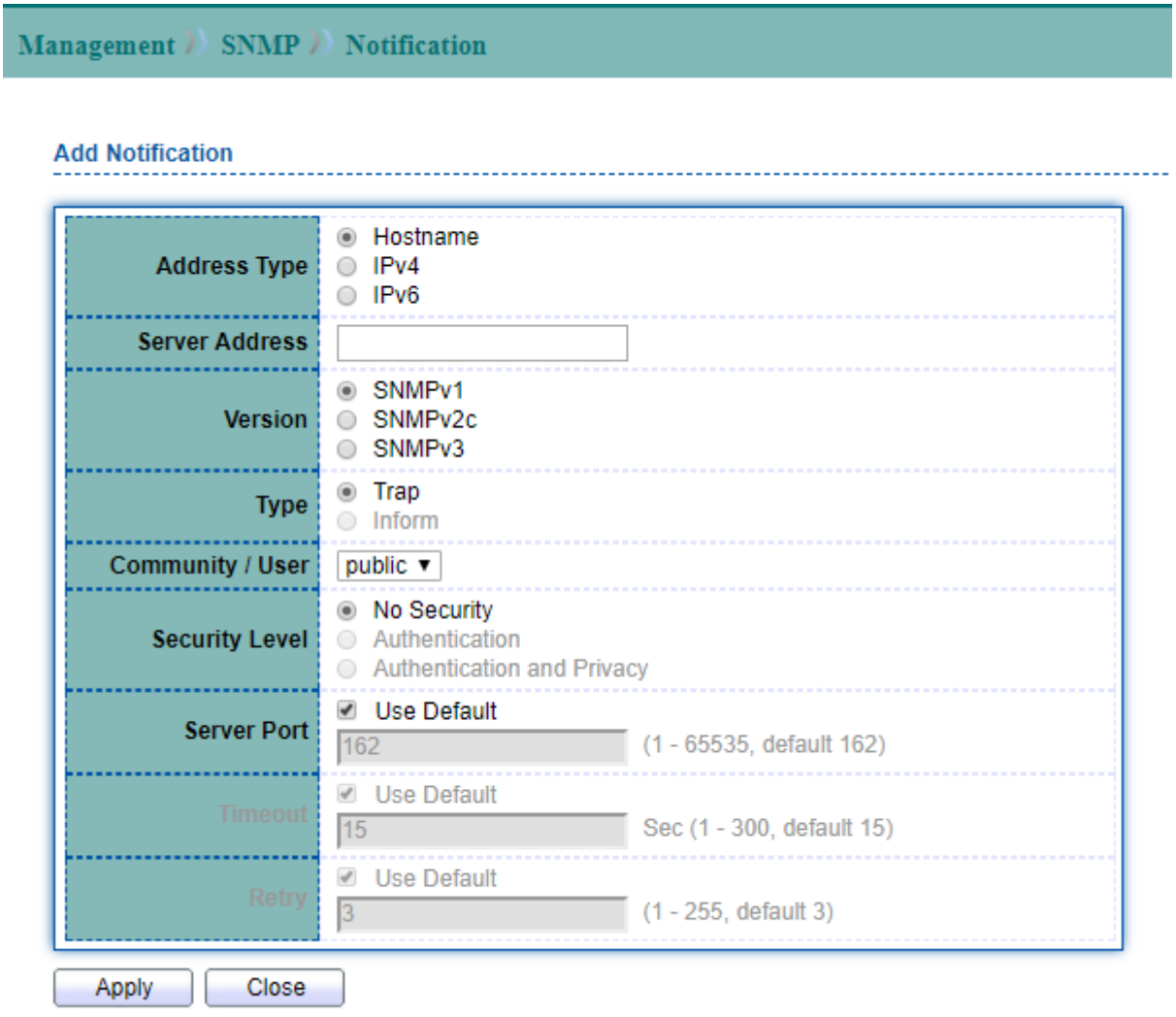


Figure 16-20 Add SNMP Notification page

Field	Description

Address Type	Server Address Type ● **Host name:** Use host name as server address. ● **IPv4 address:** Use IPv4 address as server address. ● **IPv6 address:** Use IPv6 address as server address.
Server Address	IP address or the hostname of the SNMP trap recipients.
Version	Specify SNMP version. ● **SNMPv1:** SNMP Version 1 notification. ● **SNMPv2c:** SNMP Version2 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 name for notification.
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.
Server Port	Specify the Server UDP port number.
Timeout	Specify the SNMP informs timeout.
Retry	Specify the retry counter of the SNMP informs.

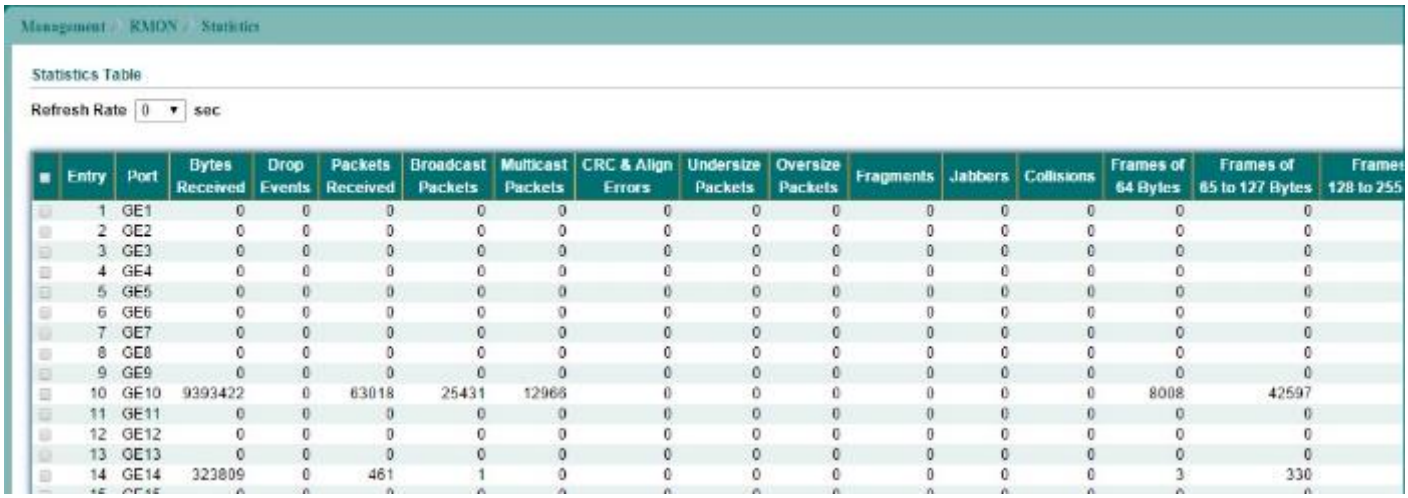
Table 16-11 SNMP Notification fields

16.5 RMON

16.5.1 RMON Statistics

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

This page allow user to browser RMON Ether Statistics Table statistics for each port.



■	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 128 to 255
□	1	GE1	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	
□	3	GE3	0	0	0	0	0	0	0	0	0	0	0	0	0	
□	4	GE4	0	0	0	0	0	0	0	0	0	0	0	0	0	
□	5	GE5	0	0	0	0	0	0	0	0	0	0	0	0	0	
□	6	GE6	0	0	0	0	0	0	0	0	0	0	0	0	0	
□	7	GE7	0	0	0	0	0	0	0	0	0	0	0	0	0	
□	8	GE8	0	0	0	0	0	0	0	0	0	0	0	0	0	
□	9	GE9	0	0	0	0	0	0	0	0	0	0	0	0	0	
□	10	GE10	9393422	0	63018	25431	12966	0	0	0	0	0	0	8008	42597	
□	11	GE11	0	0	0	0	0	0	0	0	0	0	0	0	0	
□	12	GE12	0	0	0	0	0	0	0	0	0	0	0	0	0	
□	13	GE13	0	0	0	0	0	0	0	0	0	0	0	0	0	
□	14	GE14	323809	0	461	1	0	0	0	0	0	0	0	3	330	

Figure 16-21 RMON Statistics page

Field	Description
Port	Select port to browser RMON ether statistics.
Received Bytes (Octets)	Number of octets received, including bad packets and FCS octets, but excluding framing bits.
Drop Events	Number of packets that were dropped.
Received Packets	Number of packets received, including bad packets, Multicast packets, and Broadcast packets.
Broadcast Packets Received	Number of good Broadcast packets received. This number does not include Multicast packets.
Multicast Packets Received	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.

Table 16-12 RMON Statistics fields

	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.
Frame of 64 Bytes	Number of frames, containing 64 bytes that were received.
Frame of 65 to 127 Bytes	Number of frames, containing 65 to 127 bytes that were received.
Frame of 128 to 255 Bytes	Number of frames, containing 128 to 255 bytes that were received.
Frame of 256 to 511 Bytes	Number of frames, containing 256 to 511 bytes that were received.
Frame 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.

16.5.2 RMON History

To display RMON History web page, click **Management** > **RMON** > **History**.

This page allow user to add or delete RMON History Entry.

Figure 16-22 RMON History page

Click "Add" button to create a new RMON History entry.

Figure 16-23 Add RMON History page

Field	Description
Entry	Select entry to configure.
Port	Select a port for sampling
Max Sample	The maximum amount of sampling.
Interval	Select sample interval
Owner	Owner name of this entry.

Table 16-13 RMON History fields

Click "View" button to display RMON History sample data.

Figure 16-24 View RMON History page

Field	Description
Sample No.	Sample Numbers.
Drop Events	Number of packets that were dropped.
Bytes Received	Number of bytes received, including bad packets and FCS octets, but excluding framing bits
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.
Utilization	Percentage of current interface traffic compared to the maximum traffic that the interface can handle.

Table 16-14 View RMON History fields

16.5.3 RMON Event

To display RMON Event web page, click **Management** > **RMON** > **Event**.

This page allow user to add or delete RMON Event Entry.

Figure 16-25 RMON Event page

Click "Add" button to create a new RMON Event entry.

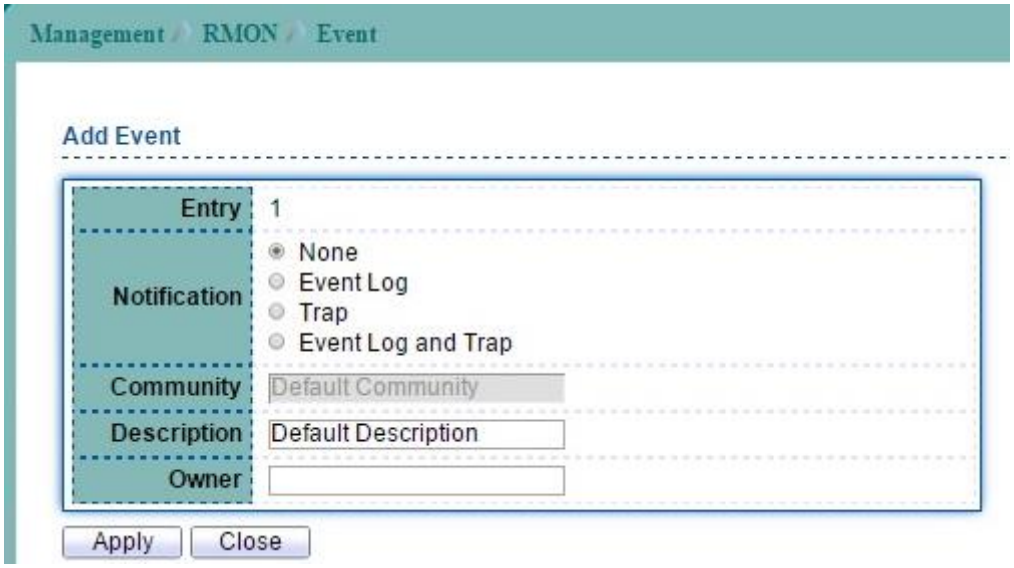


Figure 16-26 Add RMON Event page

Click "View" button to display RMON Event log.

Figure 16-27 View RMON Event page

Field	Description
Select Entry	Select index to configure.
Entry	Input an Index when select create a new entry.
Notification	Select Notification Type:

	• **None:** Do not inform. • **Event Log:** Log Event in Event. • **Trap:** Send a SNMP trap message. • **Even Log and Trap:** Do log and trap.
Community	Select SNMP community when send trap message has selected.
Description	Description of log.
Owner	Owner name of this entry.

Table 16-15 RMON Event fields

16.5.4 RMON Alarm

To display RMON Alarm web page, click **Management** > **RMON** > **Alarm**

This page allow user to add or delete RMON Alarm Entry.

Figure 16-28 RMON Alarm page

Click "Add" button to create a new RMON Alarm entry.

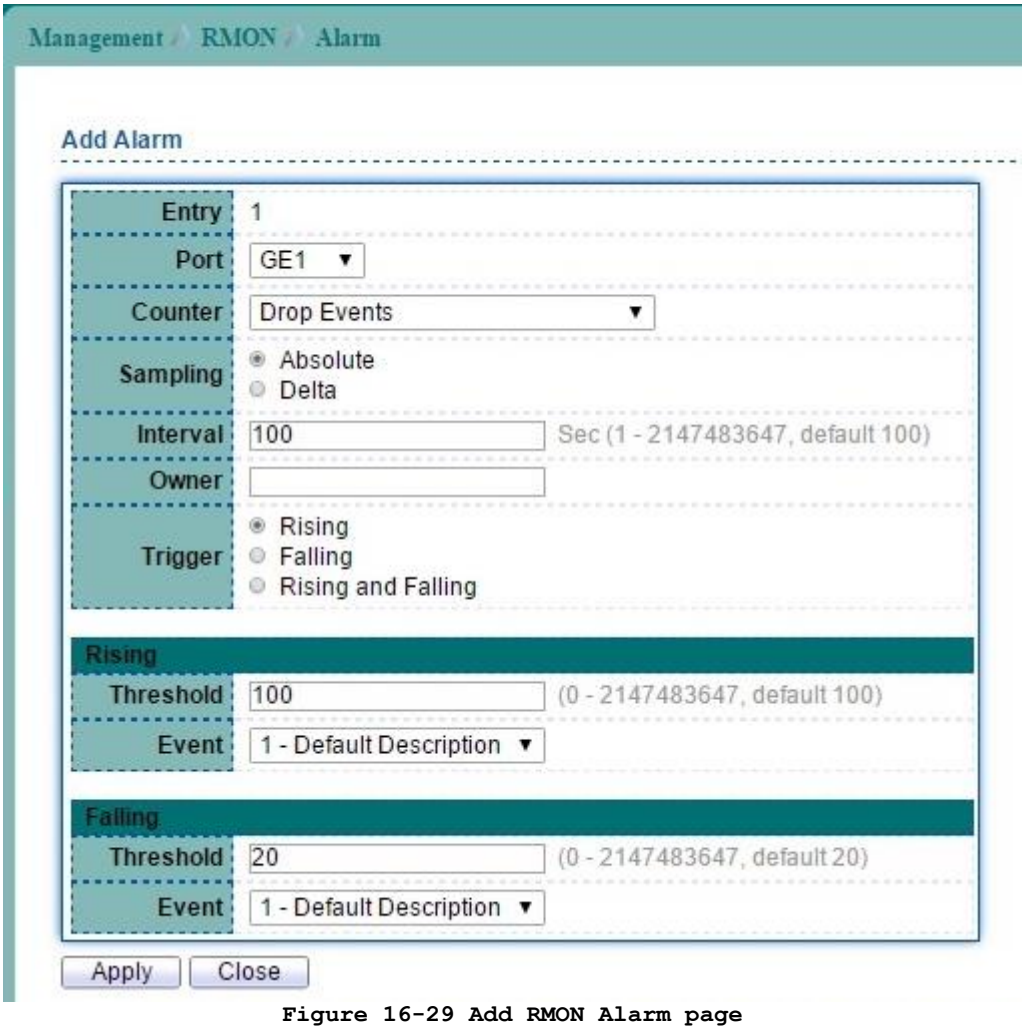


Figure 16-29 Add RMON Alarm page

Field	Description
Select Index	Select index to configure.
Entry	Alarm Table entry number.
Port	Select a port for sampling

Counter	Select an variable for sampling • **Drop Events**: Total number of events received in which the packets were dropped. • **Received Bytes (Octets)**: Number of bytes received • **Received Packets**: Number of packets. • **Broadcast Packets Received**: Broadcast packets. • **Multicast Packets Received**: Multicast packets. • **CRC & Align Errors**: 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 Bytes to 127 Bytes**: Number of packets size 65 to 127 octets. • **Frames of 128 Bytes to 255 Bytes**: Number of packets size 128 to 255 octets. • **Frames of 256 Bytes to 511 Bytes**: Number of packets size 256 to 511 octets. • **Frames of 512 Bytes to 1023 Bytes**: Number of packets size 512 to 1023 octets. • **Frames of 1024 Bytes to 1518 Bytes**: Number of packets size 1024 to 1518 octets.
Sampling	Select type for sampling • **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	Input sample interval
Owner	Owner of the Alarm.
Trigger	Rising: Trigger on firing rising event. Falling: Trigger on firing falling event Rising and Falling: Trigger on both rising and falling events.
Rising	
Rising Threshold	Threshold for firing rising event.
Falling Threshold	Threshold for firing falling event.
Falling	
Rising Event	Index of rising event when alarm fired.
Falling Event	Index of falling event when alarm fired.

Table 16-16 RMON Alarm fields