850G-12PI

Industrial 12-Port GbEManaged PoE Switch with 4 GbE SFP Uplinks

User Manual

Version 2.00

Proscend Communications Inc. All rights reserved.

Table of Contents

1 Introduction 5

1.1 Features 5

1.2 Dimensions 5

1.3 Specifications 6

2 Hardware Installation 7

2.1 Connecting Power 7

2.2 Connecting I/O Ports 7

2.3 Reset Button 8

2.4 Ground Connector 8

2.5 LED Indicators 8

2.6 Console Connection 9

2.7 DIN-rail Mounting 9

2.8 Wall Mounting 10

2.9 Web Interface Connect & Login 10

2.10 Cybersecurity Warning 11

3 Using the Web 12

3.1 Using the Web Interface 12

3.2 Navigation 14

4 Status 18

4.1 System Information 18

4.2 Logging Message 18

4.3 Port 19

4.4 Link Aggregation 22

4.5 MAC Address Table 23

5 Network 24

5.1 IP Address 24

5.2 System Time 26

5.3 O'smart 28
6 Port 30
6.1 Port Setting 30
6.2 Error Disabled 32
6.3 Link Aggregation 33
6.4 EEE 39
6.5 Jumbo Frame 40
7 PoE 41
7.1 Global Setting 41
7.2 Power Show 43
7.3 PD Alive Check 44
7.4 Time Range 45
8 VLAN 47
8.1 VLAN 47
8.2 Voice VLAN 53
8.3 Protocol VLAN 56
8.4 MAC VLAN 60
8.5 Surveillance VLAN 64
8.6 GVRP 67
9 MAC Address Table 71
9.1 Dynamic Address 71
9.2 Static Address 72
9.3 Filtering Address 74
10 ERPS 75
10.1 Setting 75
10.2 Status 76
11 Spanning Tree 77
11.1 Property 77
11.2 Port Setting 79

11.3 MST Instance 81
11.4 MST Port Setting 83
11.5 Statistics 84
12 Discovery 85
12.1 LLDP 85
13 Multicast 96
13.1 General 96
13.2 IGMP Snooping 109
13.3 MLD Snooping 113
13.4 MVR 116
14 Security 121
14.1 RADIUS 121
14.2 TACACS+ 123
14.3 AAA 125
14.4 Management Access 128
14.5 Authentication Manager 133
14.6 Port Security 144
14.7 Protected Port 146
14.8 Storm Control 147
14.9 DoS 149
14.10 Dynamic ARP Inspection 152
14.11 DHCP Snooping 155
14.12 IP Source Guard 162
15 ACL 167
15.1 MAC ACL 167
15.2 MAC ACE 168
15.3 IPv4 ACL 171
15.4 IPv4 ACE 172
15.5 IPv6 ACL 176

15.6 IPv6 ACE 177
15.7 ACL Binding 181
16 QoS 193
16.1 General 193
16.2 Rate Limit 200
17 Diagnostics 203
17.1 Logging 203
17.2 Mirroring 206
17.3 Ping 208
17.4 Traceroute 209
17.5 Digital Input Detect 210
17.6 Copper Test 211
17.7 Fiber Module 212
17.8 UDLD 213
18 Management 216
18.1 User Account 216
18.2 Firmware 217
18.3 Configuration 219
18.4 SNMP 221
18.5 RMON 234
19 Loop Prevention 242
19.1 Property 242
19.2 Status 243

1 Introduction

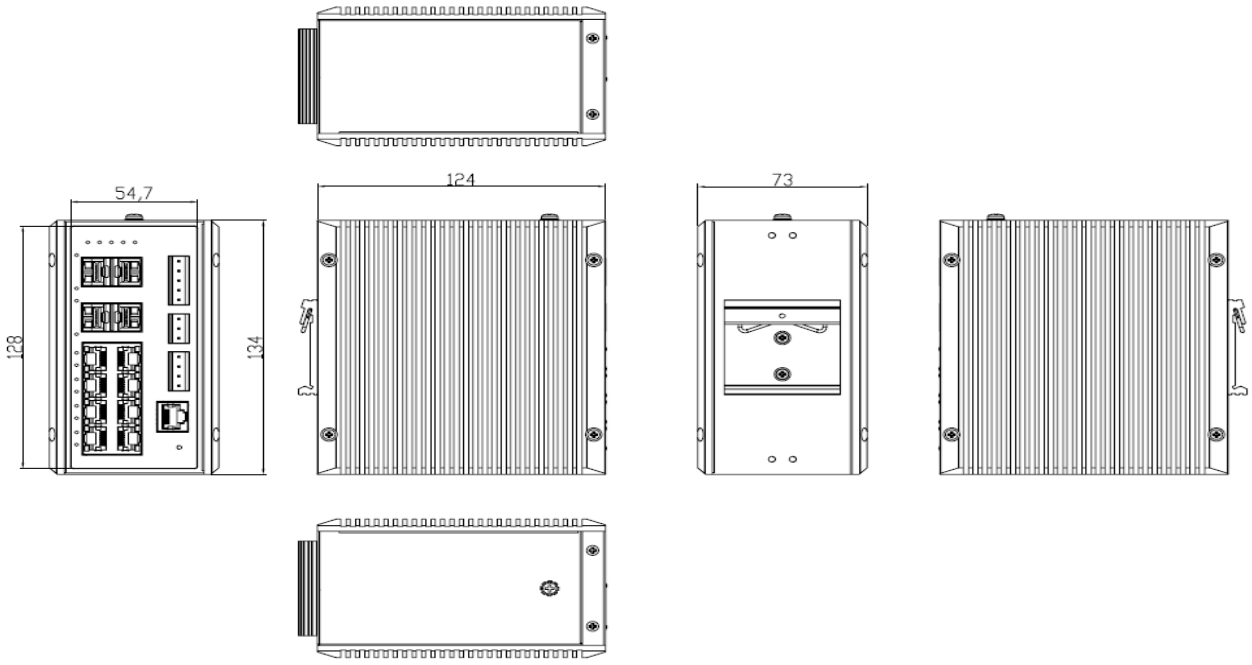
Proscend 850G-12PI Industrial Ethernet Switch features friendly manageability in full Gigabit Ethernet networks, as well as 1000Mbps Ethernet speed over copper and fiber for enabling quality of services, network security, and resilience. As a result, the 850G-12PI is the perfect solution for reducing network response time for mission-critical applications such as video security, transportation, energy, etc.

The 850G-12PI features 8 Gigabit PoE ports, each of the 10/100/1000Base-T ports with Power-over-Ethernet power source is IEEE802.3af/at compliant and provides an additional 4 SFP slots are used to work with SFP (Small form-factor pluggable) fiber transceivers to scale out modern industrial networks with the ring, daisy chain, or tree topologies.

1.1 Features

- Operating temperature -40°C ~ 75°C
- Support IEEE 802.3at/af PoE
- Support ERPS Ring failover protection
- Support Spanning Tree Protocol STP/RSTP/MSTP.
- Support IPv6 manageable
- Support Jumbo frames
- DIN-rail mounted

1.2 Dimensions



1.3 Specifications

Interfaces

- 8 x 10/100/1000BASE-T (RJ45)
- 4 x 100FX/GbE SFP
- 1 x RJ45 console port
- 1 x Reset button
- 1 x 5-pin Terminal Block for Power in
- 1 x 3-pin Terminal Block for DO
- 1 x 4-pin Terminal Block for DI

Network Resilience

- IEEE 802.1D STP, IEEE 802.1w RSTP, IEEE 802.1s MSTP
- LACP: Static trunk

Protocols & Security

- Port-based VLAN
- IEEE 802.1ab Link Layer Discovery Protocol (LLDP)
- IEEE 802.1p QoS, IGMP snooping, Port-based traffic shaping
- IP and MAC-based access control
- IEEE 802.1X authentication Network Access Control
- Multicast, Broadcast, Flooding Strom Control
- DoS, Dynamic ARP Inspection, DHCP Snooping, IP Source Guard

Mechanical

- Dimension (H x D x W): 134 x 124 x 73 mm
- Weight:1000g
- DIN-rail and Wall mounted
- Aluminum & Metal: IP40

Management

- Web-based Management, HTTP/HTTPS, Console, CLI, Telnet, SSH
- SNMP v1, v2c, v3, Syslog
- HTTP/TFTP firmware upgrade
- SNTP
- PoE scheduling, power control

Power

- Input: 48V~57VDC, 4.95A (Max)
- System power consumption: 13 W
- PoE Power Budget: 240W

LED Indicators

- Power input, System Alarm
- Ethernet LAN Port Link & Speed, SFP Port Link
- PoE power output

Environment & Regulatory Compliance

- Operation temperature: -40 to +75°C
- Storage temperature: -40 to +85 °C
- Humidity (non-condensing): 10 to 95% RH EMC Class A
- Emission (EMI/EMS): CE/FCC class A,
- EN61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN61000-4-6, EN61000-4-8
- Safety: ETL EN62368
- Shock: IEC60068-2-27
- Freefall: IEC60068-2-32
- Vibration: IEC60068-2-6
- MTBF: > 1,000,000 hours@25 degree C

Standards and Certifications

- CE&UKCA
- FCC

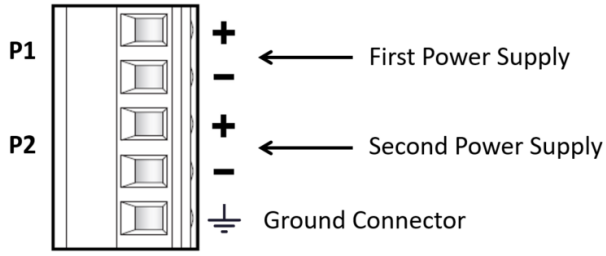
2 Hardware Installation

This chapter introduces how to install and connect the hardware.

2.1 Connecting Power

The 850G-12PI Industrial Ethernet PoE Switch can be powered from two power supplies (input range 48~57 VDC). Two power supplies are in front of the switch.

Insert the positive and negative wires (AWG 20-28) into V+ and V- contacts on the terminal block respectively and use a flat-head screwdriver to push in and open the wire clamp.

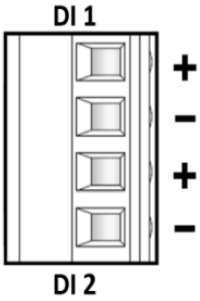


⚠ WARNING

The DC power should be connected to a well-fused power supply.

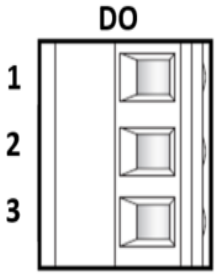
2.2 Connecting I/O Ports

There are four terminals on the terminal block for digital inputs.



Pin	Digital Input
DI 1 +	High (+13V to +30V) for “Off”
DI 1 -	
DI 2 +	Low (-30 to +3V) for “On”
DI 2 -	

There are three terminals on the terminal block for digital output.



DO	Factory default
PIN 1 PIN 2	Open
PIN 2 PIN 3	Short

NOTE: DO configuration (Open/Short) can be reversed (Short/Open) from the UI.

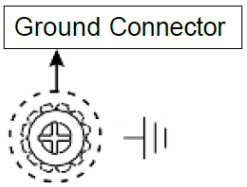
2.3 Reset Button

RESET

Function	Operation
Reboot	**Press and hold the button for less than 5 seconds.**
Reset to default setting	**Press and hold the button for at least 5 seconds.**

2.4 Ground Connector

The switch must be properly grounded for optimum system performance.



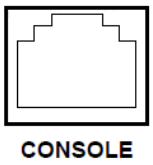
2.5 LED Indicators

The following table explains the LED indicators on the front panel.

LED	Color	Description
P1	On: Green	Power on.
	Off	Power off.
P2	On: Green	Power on.
	Off	Power off.
ALM	On: Red	One of the two powers is abnormal
	Off	The system is operating normally.
PoE	On: Green	Over PoE max power budget.
	Off	Below PoE max power budget.
SYS	On: Green	System is ready.
	Blinking	System is booting up.
	Off	No power
1~8 LAN Port Link/Act	On: Green	Ethernet LINK UP at 1000Mbps.
	On: Amber	Ethernet LINK UP at 10/100Mbps.
	Blinking	Ethernet traffic detected.
	Off	Ethernet LINK DOWN.
PoE	On: Green	PoE PD (Powered Device) connected.
	Off	PoE PD (Powered Device) disconnected.
9~12 SFP Port UPLINK	On: Green	LINK UP at 100/1000Mbps.
	Blinking	Traffic detected.
	Off	LINK DOWN.

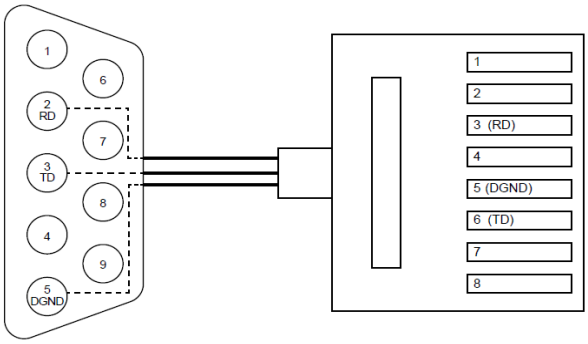
2.6 Console Connection

The console port on the front panel is for local management by using a terminal emulator or a computer with terminal emulation software.



- DB9 connector connect to computer COM port
- Baud rate: 115200bps
- 8 data bits, 1 stop bit
- None Priority
- None flow control

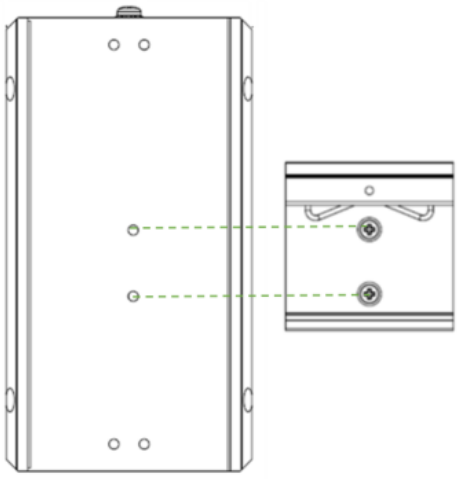
To connect the host PC to the console port, a RJ45 (male) connector-to-RS232 DB9 (female) connector cable is used. The RJ45 connector of the cable is connected to the console port of the switch, the DB9 connector of the cable is connected to the PC COM port. The pin assignment of the console cable is shown below:



NOTE: The console cable is not included in the package.

2.7 DIN-rail Mounting

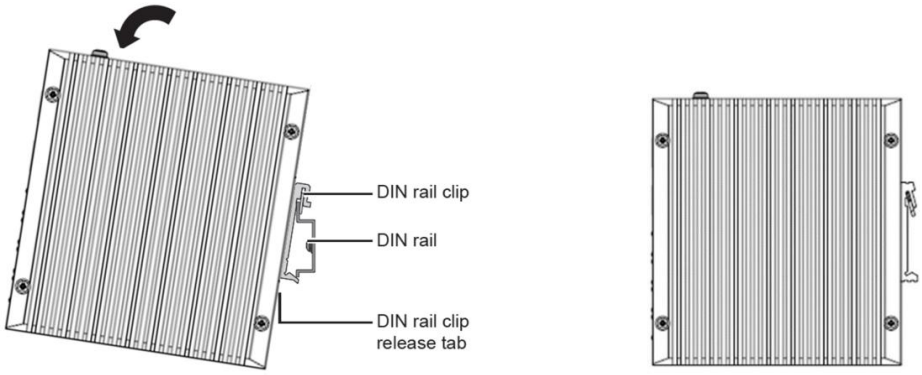
STEP 1: Use the screws to install the DIN-rail kit to attach at the rear side of the switch.



NOTE: The type of screw is flat head M3 x 6mm.

STEP 2: Hook the unit onto the DIN-rail.

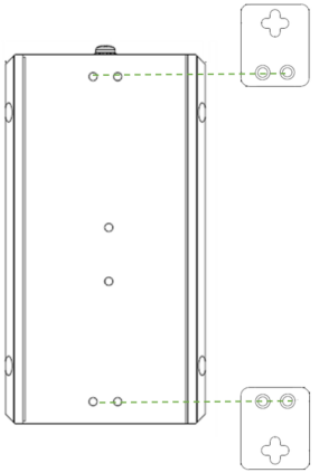
STEP 3: Push the bottom of the unit towards the DIN-rail until it locks in place.



NOTE: The DIN-rail-mounting screws are not included in the package.

2.8 Wall Mounting

Use the screws to install the wall-mounting kit to attach at the rear side of the switch.



NOTE: For all switches (Non-PoE and PoE Series), the operation of wall mounting is the same

The type of screw is flat head M3 x 6mm.

2.9 Web Interface Connect & Login

1. Factory default IP: 192.168.1.1
2. Login with default account and password.

   Username: root

   Password: 2wsx#EDC

2.10 Cybersecurity Warning

Change the default password immediately upon first login. HTTP and SNMP management services are enabled by default. Disable unused services and interfaces to reduce the attack surface. Use secure protocols such as SSH and HTTPS for remote management whenever possible.

3 Using the Web

3.1 Using the Web Interface

The object of this document “Web Configuration Tool Guide” is to address the web feature, design layout and descript how to use the web interface.

3.1.1 Web Browser Support

Firefox with the following default settings is recommended:

Web page font	Times New Roman
Encoding	Unicode (UTF-8)
Text size	16

Google Chrome with the following default settings is recommended:

Web page font	Times New Roman
Encoding	Unicode (UTF-8)
Text size	Medium

3.1.2 Navigation

All main screens of the web interface can be reached by clicking on hyperlinks in the four menu boxes on the left side of the screen:

- **Status**
- **Network**
- **Port**
- **PoE**
- **VLAN**
- **MAC Address Table**
- **ERPS**
- **Spanning Tree**
- **Discovery**
- **Multicast**
- **Security**
- **ACL**
- **QoS**
- **Diagnostics**
- **Management**
- **Loop Prevention**

3.1.3 Title Bar Links



Save

If any unsaved change has been made to the *configuration* (by you during this or a prior session, or by any other administrator using the web interface or the Command Line Interface), a Save icon appears in the title line. To save the running configuration to the startup configuration:

1. Click on the Save link. The Message box appears.
2. Click on OK to save the running configuration to the startup configuration.

Logout

Disconnect your current session and need to enter the username/password to login again.

Reboot

Reboot the system and unsaved change in the configuration will be lost.

Login

This section provide instruction to login

Operation	1. Open Browser and enter default IP address http://192.168.1.1. 2. Fill Username and Password. 3. Click “LOGIN”
Field	Description
Username	Login user name. The maximum length is 32. Default: root
Password	Login user password. The maximum length is 32. Default: 2wsx#EDC



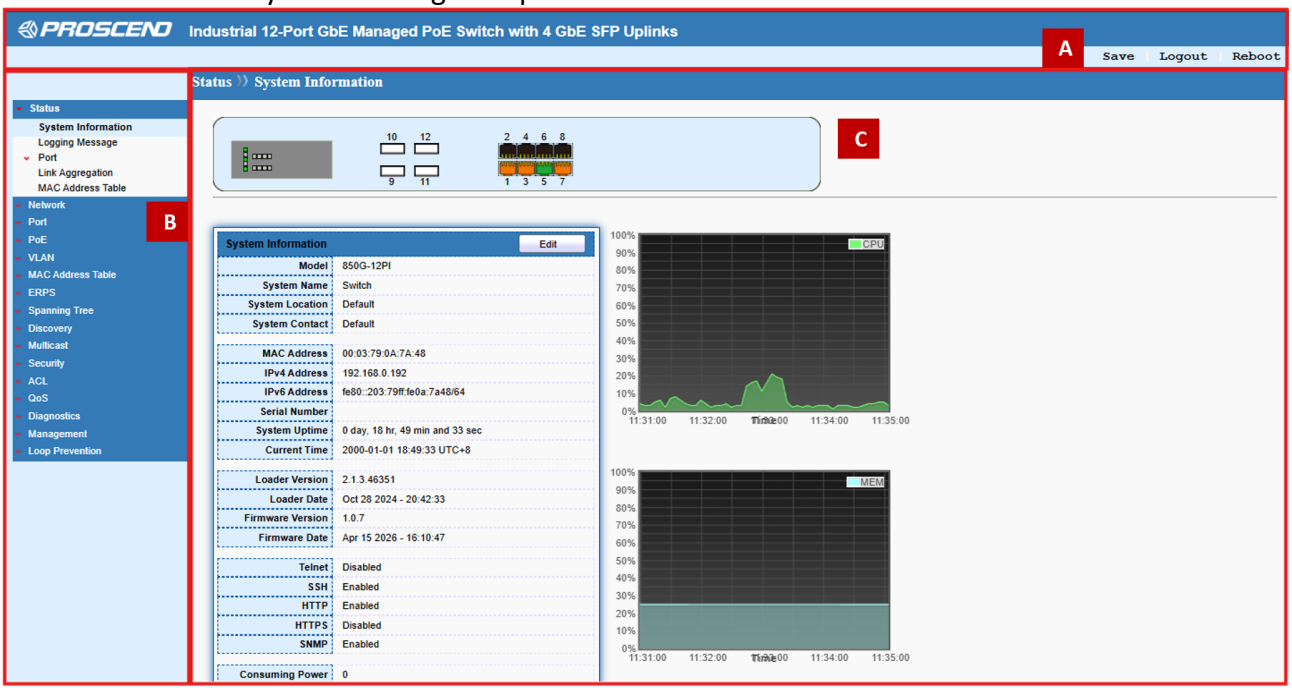
Item	Description
Username	Login username. The maximum length is 32. Default: root
Password	Login user password. The maximum length is 32. Default: 2wsx#EDC

3.2 Navigation

The main screen is divided into three parts as below.

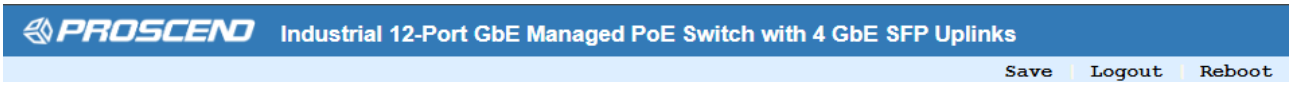
A - Title Bar, B - Navigation Panel and C - Main Window.

The menu items are divided into main and sub menu to configure the settings and get the status of connectivity on the navigation panel.



(1) A : Title Bar

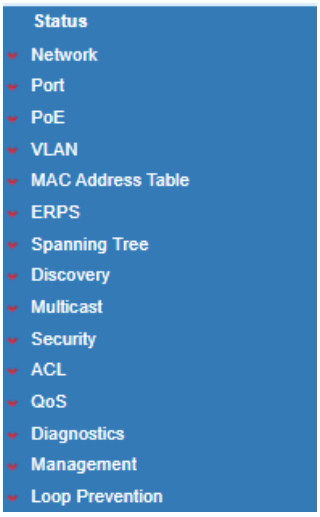
The title bar provides Save, Logout and reboot.



Item	Description
Save	All configuration should be saved in order to prevent reset after switch reboot.
Logout	Logout from the switch.
Reboot	Reboot the system and unsaved change in the configuration will be lost.

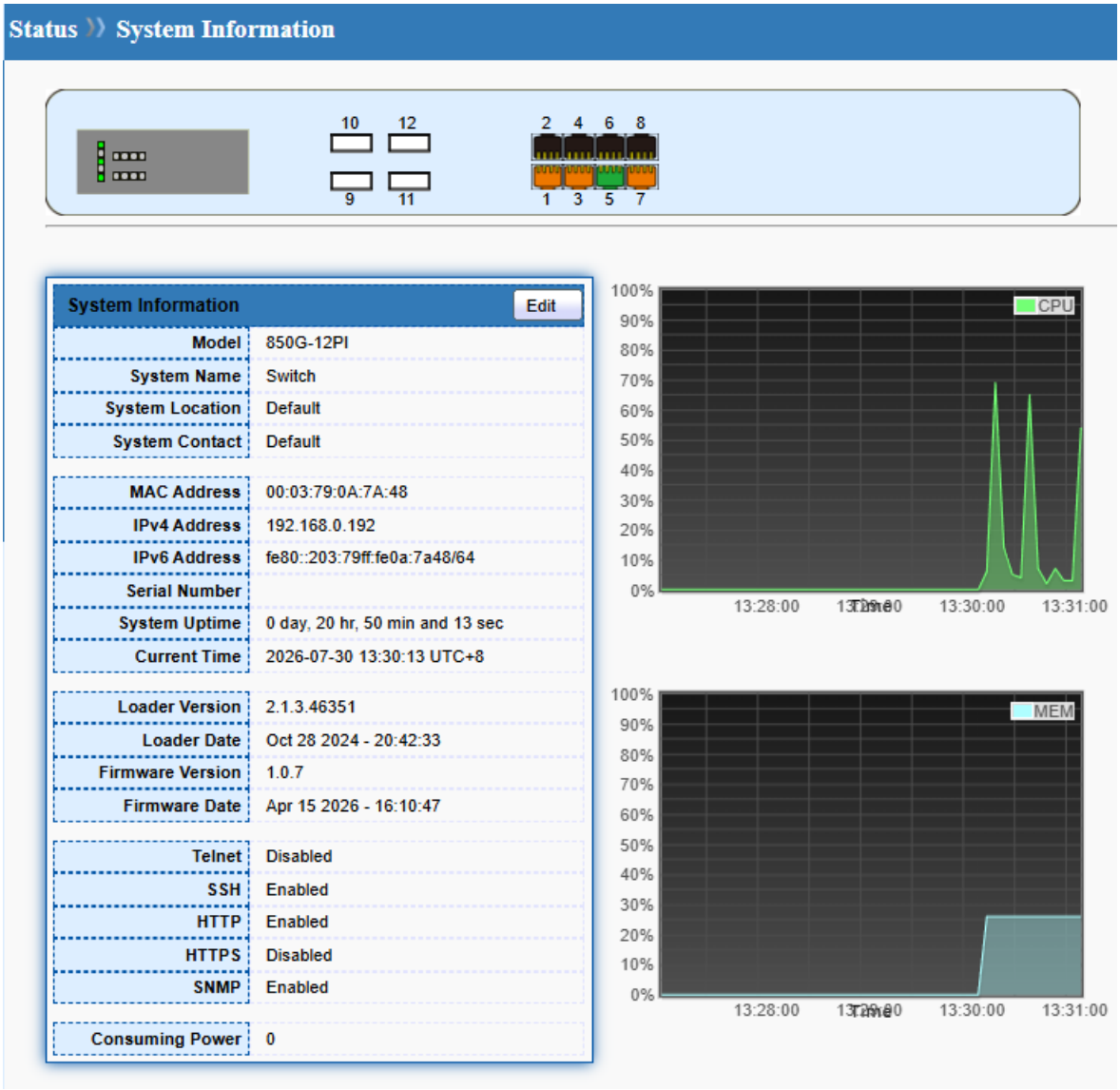
(2) B : Navigation Panel-Main Menu and Sub Menu

The menu items are divided into main and sub menu to configure the settings and get the status of connectivity on the navigation panel.



(3) C : Main Window

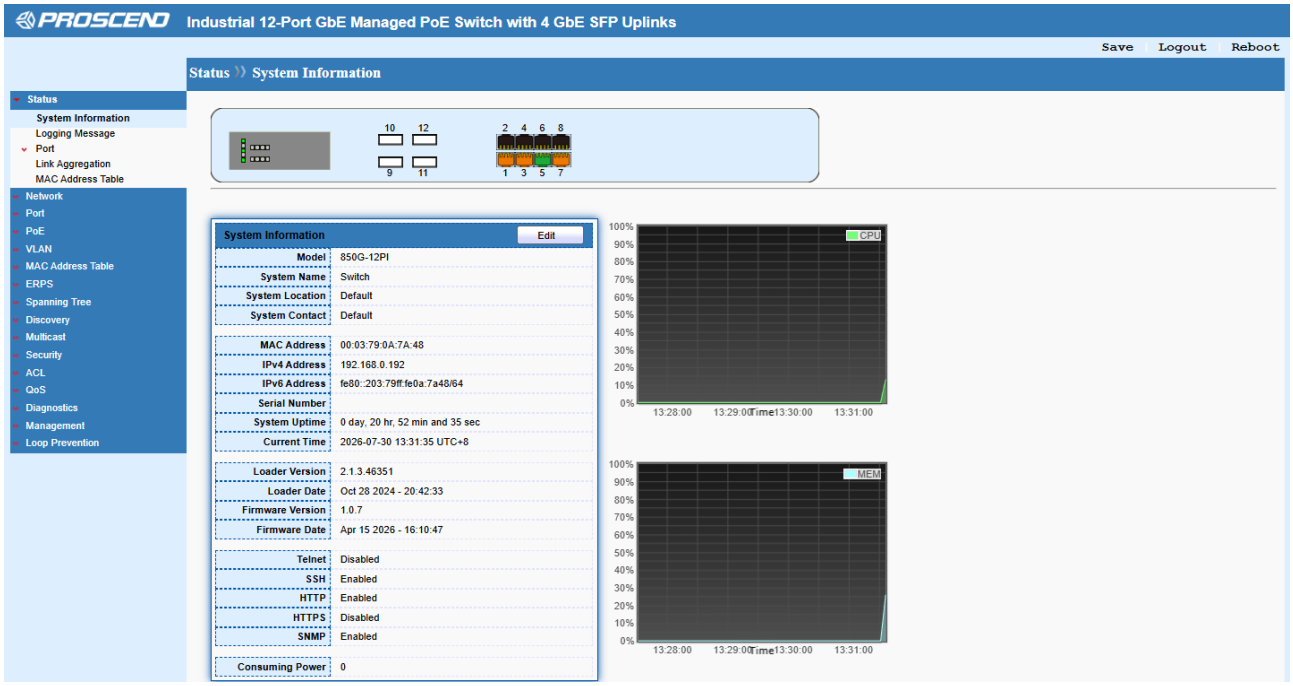
This section shows the information or setting fields from main menu and sub menu.



4 Status

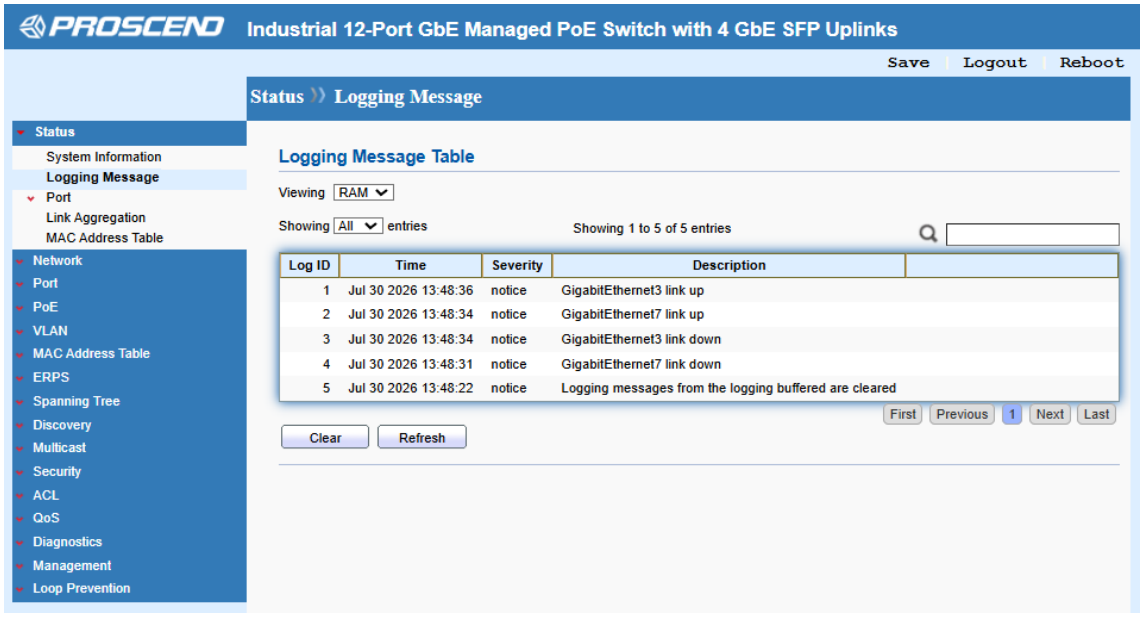
4.1 System Information

This page displays detailed information of system, port status and CPU/Memory utilization.



4.2 Logging Message

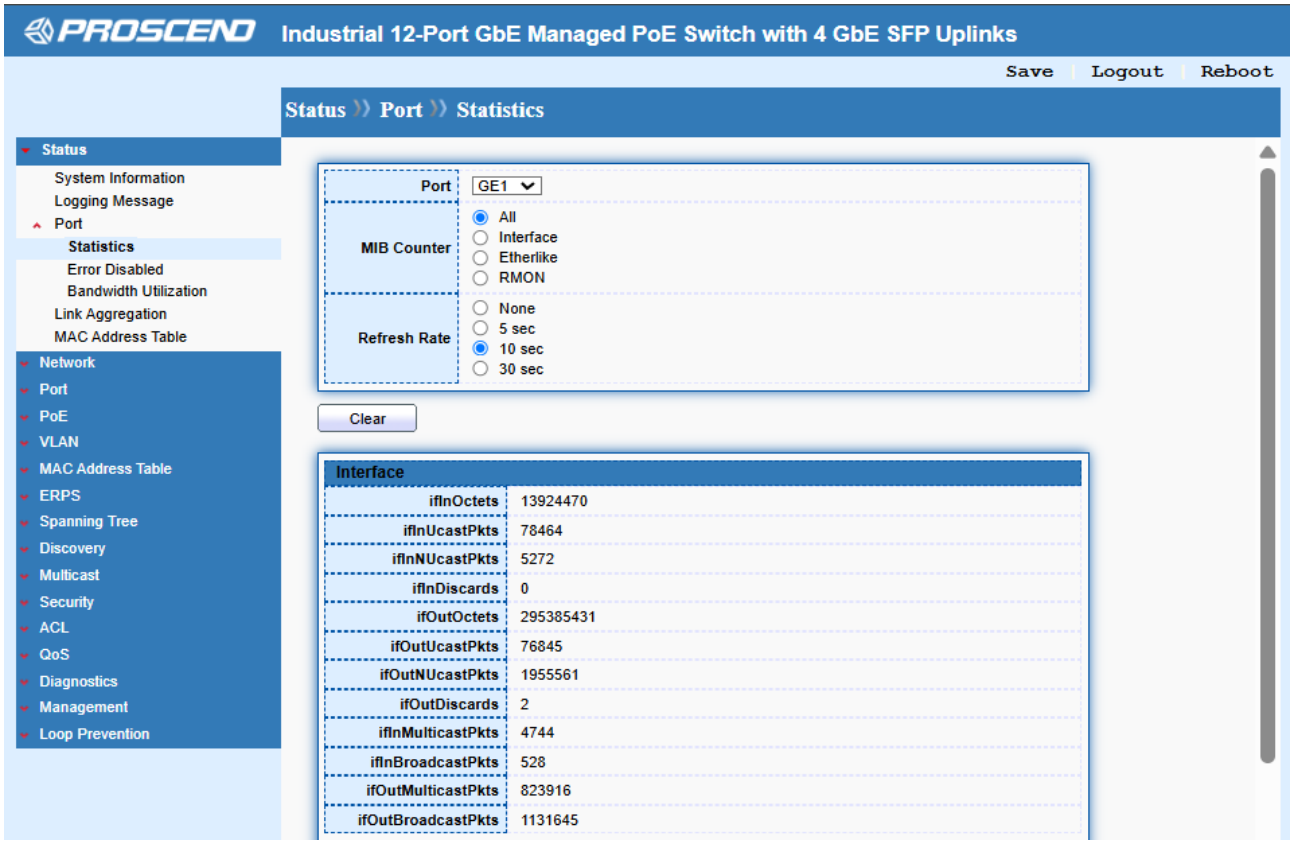
This page provides the system log for all events.

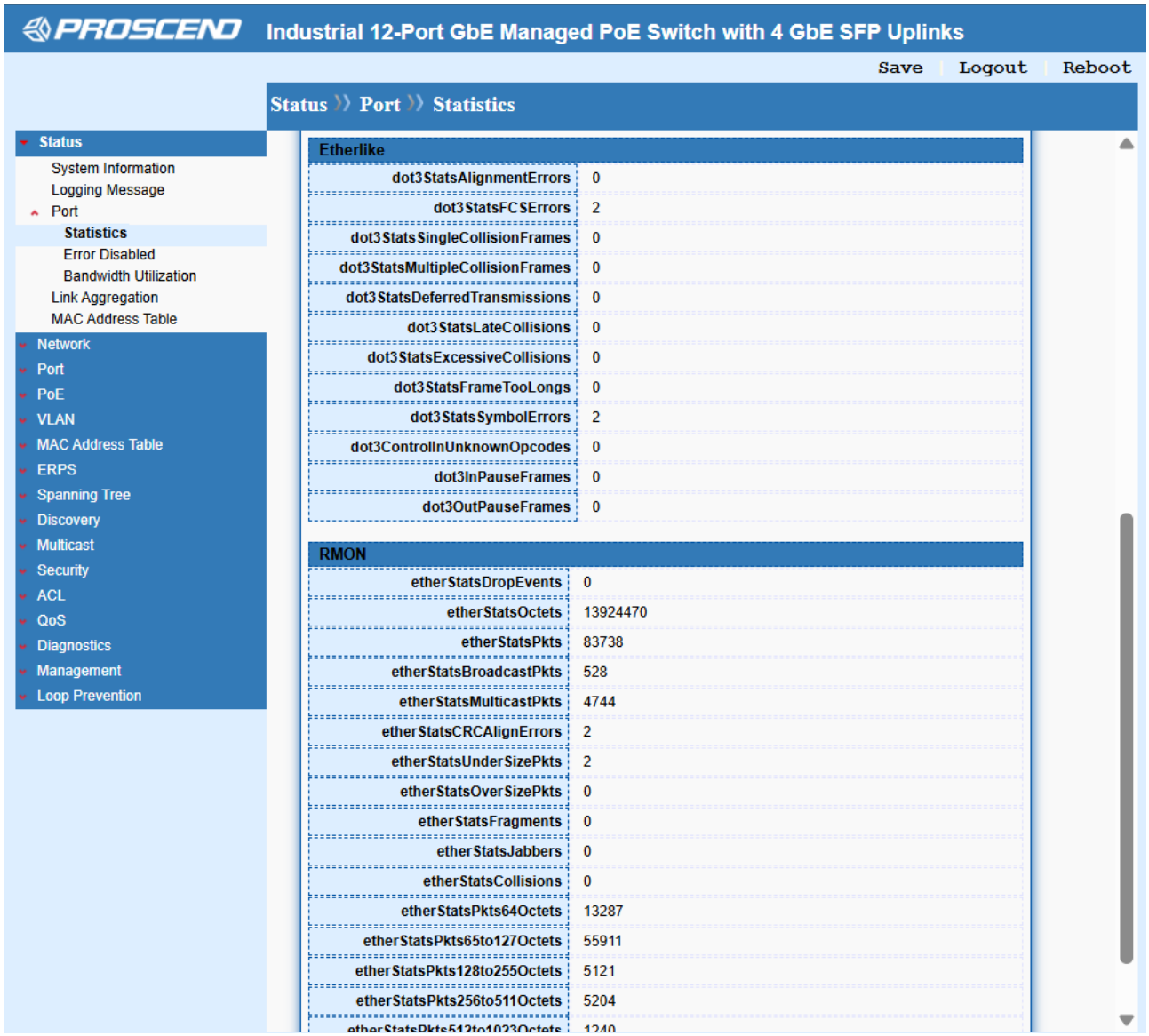


4.3 Port

4.3.1 Statistics

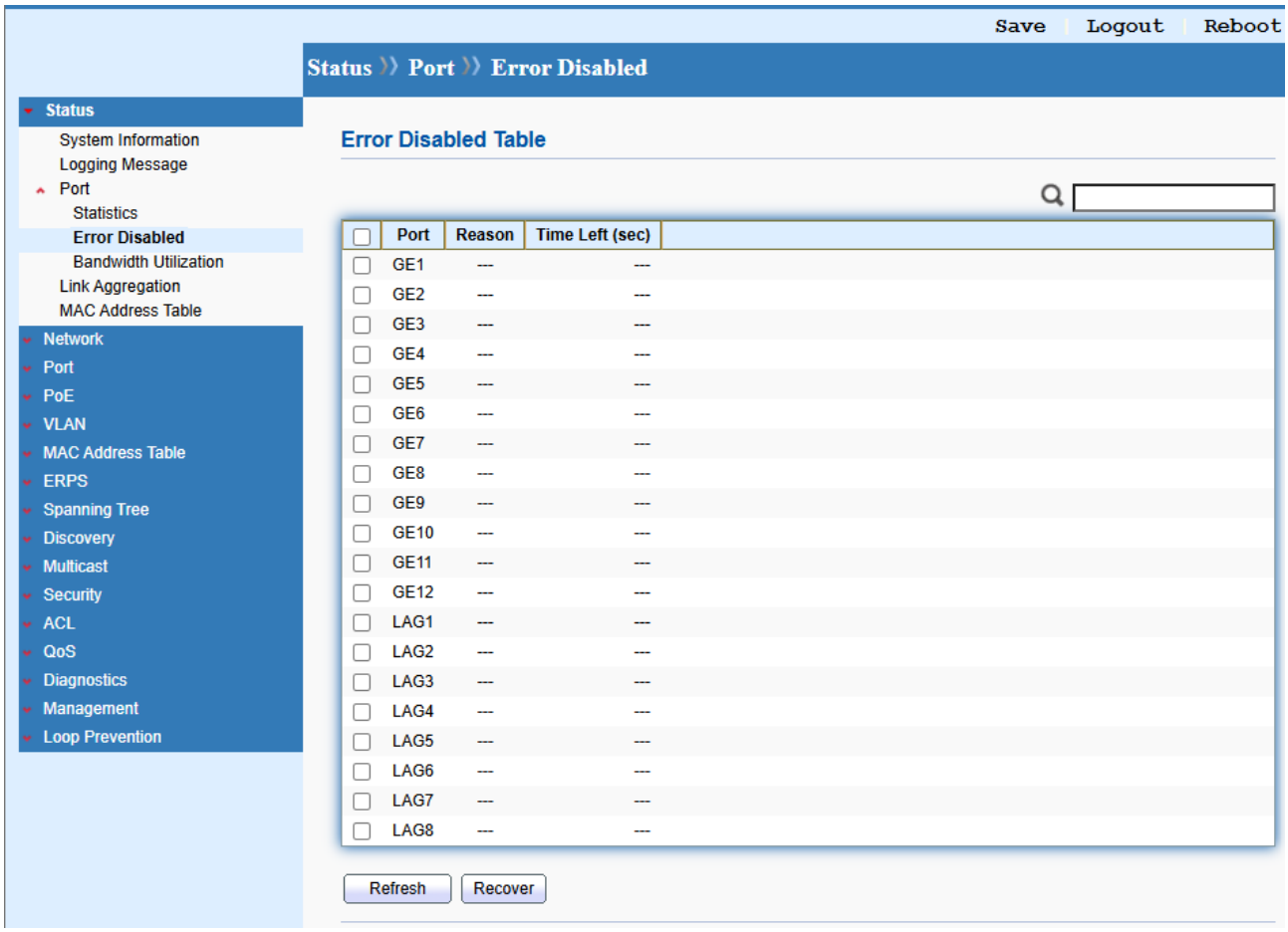
This page displays statistics for GE/10GE/LAG ports.




PROSCEND
Industrial 12-Port GbE Managed PoE Switch with 4 GbE SFP Uplinks
Save | Logout | Reboot
Status » Port » Statistics
Status
System Information
Logging Message
Port
Statistics
Error Disabled
Bandwidth Utilization
Link Aggregation
MAC Address Table
Network
Port
PoE
VLAN
MAC Address Table
ERPS
Spanning Tree
Discovery
Multicast
Security
ACL
QoS
Diagnostics
Management
Loop Prevention
Etherlike
dot3StatsAlignmentErrors 0
dot3StatsFCSErrors 2
dot3StatsSingleCollisionFrames 0
dot3StatsMultipleCollisionFrames 0
dot3StatsDeferredTransmissions 0
dot3StatsLateCollisions 0
dot3StatsExcessiveCollisions 0
dot3StatsFrameTooLongs 0
dot3StatsSymbolErrors 2
dot3ControlInUnknownOpcodes 0
dot3InPauseFrames 0
dot3OutPauseFrames 0
RMON
etherStatsDropEvents 0
etherStatsOctets 13924470
etherStatsPkts 83738
etherStatsBroadcastPkts 528
etherStatsMulticastPkts 4744
etherStatsCRCAlignErrors 2
etherStatsUnderSizePkts 2
etherStatsOverSizePkts 0
etherStatsFragments 0
etherStatsJabbers 0
etherStatsCollisions 0
etherStatsPkts64Octets 13287
etherStatsPkts65to127Octets 55911
etherStatsPkts128to255Octets 5121
etherStatsPkts256to511Octets 5204
etherStatsPkts512to1023Octets 1240

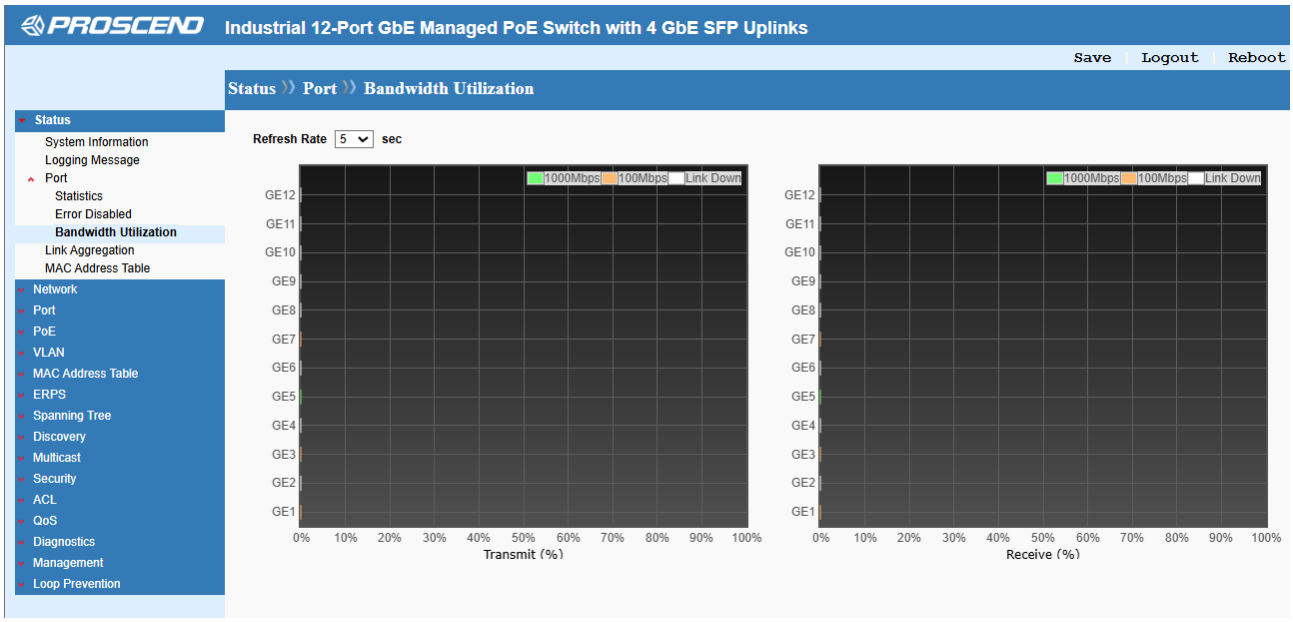
4.3.2 Error Disabled

This page displays “Error Disabled” status of port and can recover it on this page, too.



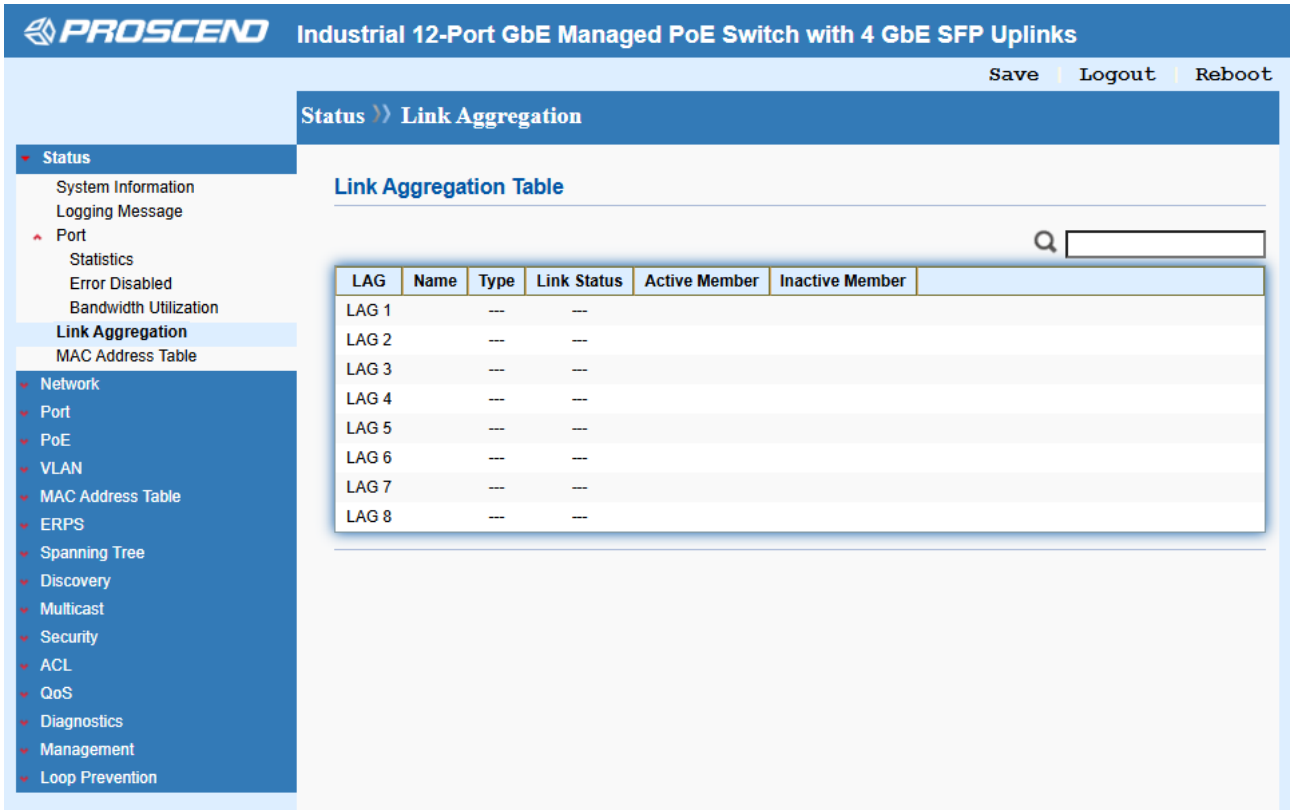
4.3.3 Bandwidth Utilization

This page displays bandwidth utilization for both transmitting and receiving.



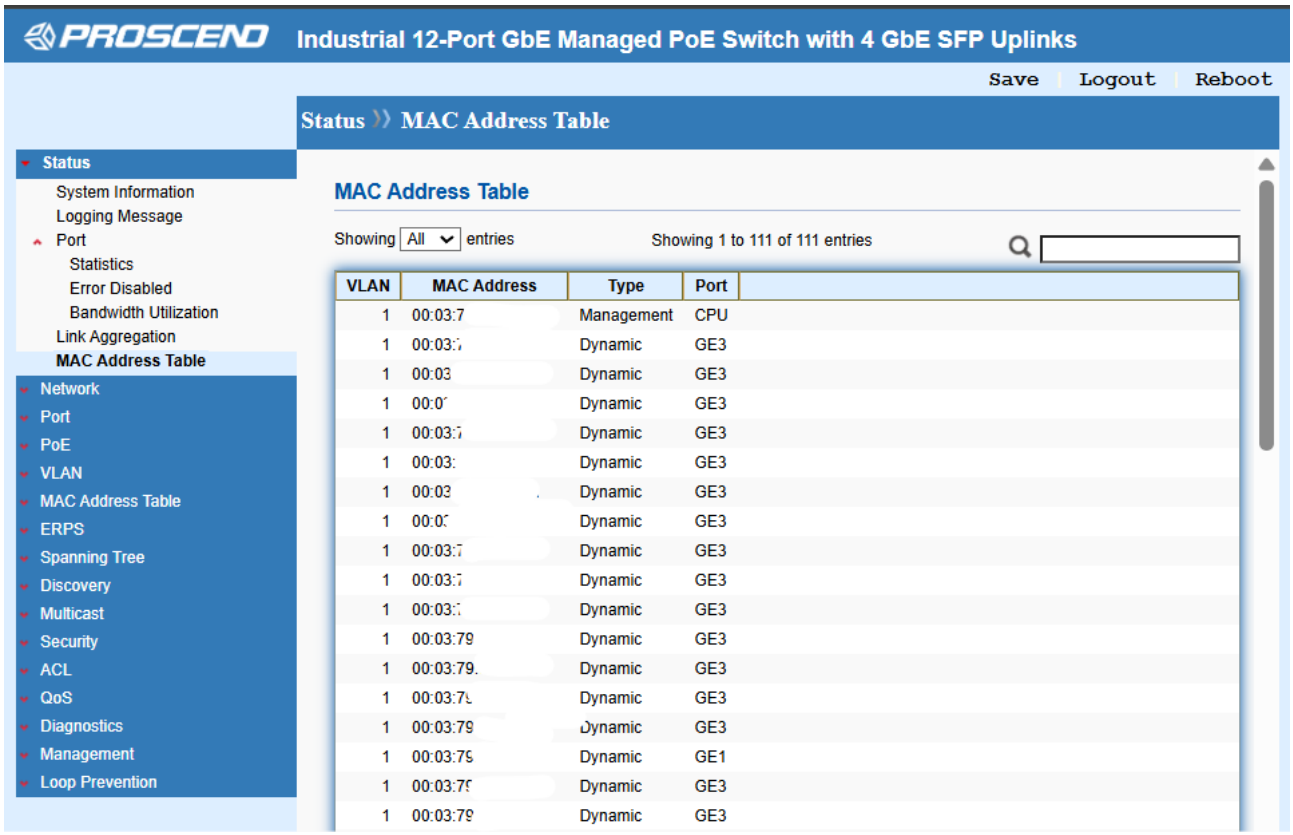
4.4 Link Aggregation

This page displays status of each Link Aggregation port.



4.5 MAC Address Table

This page displays all MAC addresses that through the Switch.

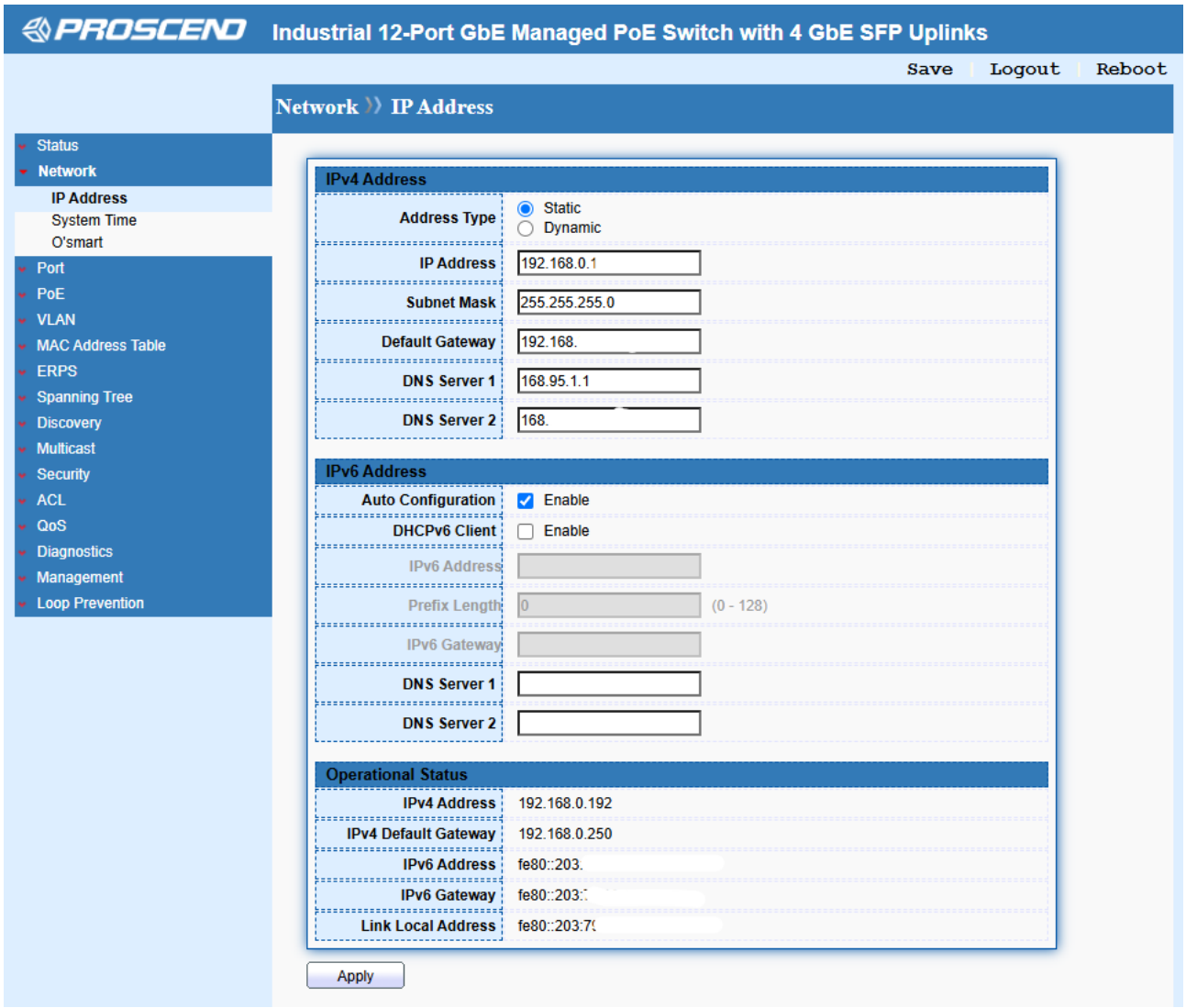


5 Network

This section allows you to setup map settings, neighbor devices and topology map.

5.1 IP Address

The switch needs an IP address for it to be managed over the network. The **factory default IP address is 192.168.1.1/24**. This page allows to configure IP basic settings.

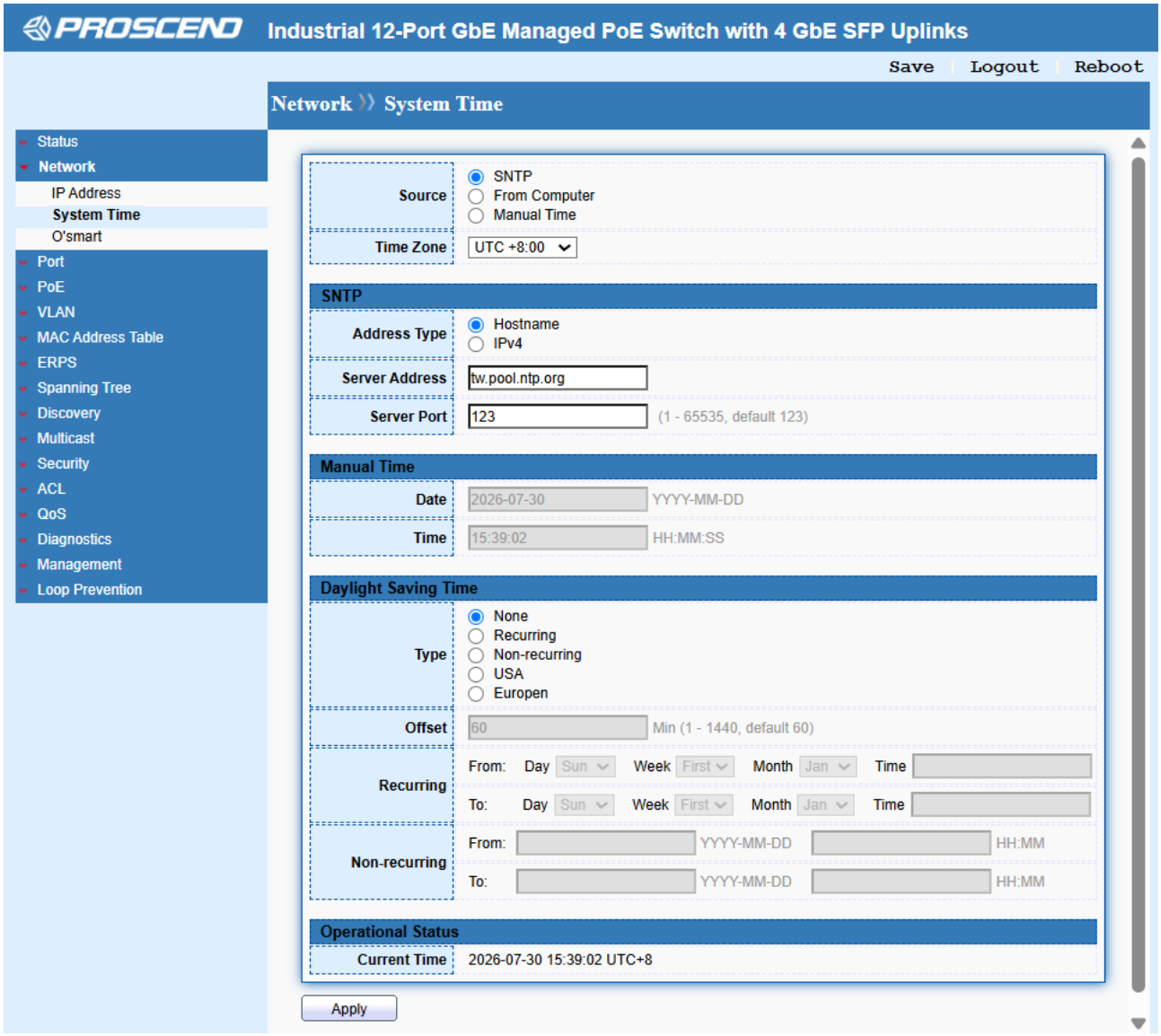


Item	Description
IPv4 Address	
Address Type	Select the type of network connection. **Static**: Use static IPv4 address. **Dynamic**: Use DHCP provisioned IP address and Gateway if feasible.

IP Address	Fill in the IPv4 address.
Subnet Mask	Fill in the IPv4 mask.
Default Gateway	Fill in the IPv4 Gateway address.
DNS Server 1	Enter primary IPv4 DNS server address in this field.
DNS Server 2	Enter second IPv4 DNS server address in this field.
IPv6 Address	
Auto Configuration	The option to let switch automatically configure IPv6 address.
DHCPv6 Client	Enable this feature if there is a DHCPv6 server on your network for assigning IPv6 Address, instead of using Router Advertisement.
IPv6 Address	Fill in the IPv6 address
Prefix Length	Specify the prefix length of the IPv6 address.
IPv6 Gateway	Fill in the IPv6 Gateway address.
DNS Server 1	Enter primary IPv6 DNS server address in this field.
DNS Server 2	Enter second IPv6 DNS server address in this field.
Operational Status	
IPv4 Address	Current IPv4 address.
IPv4 Default Gateway	Current IPv4 Default Gateway address.
IPv6 Address	Current IPv6 address.
IPv6 Gateway	Current IPv6 Gateway address.
Link Local Address	Current Link Local address.

5.2 System Time

This page allows a user to specify where the time of Switch should be inquired from.

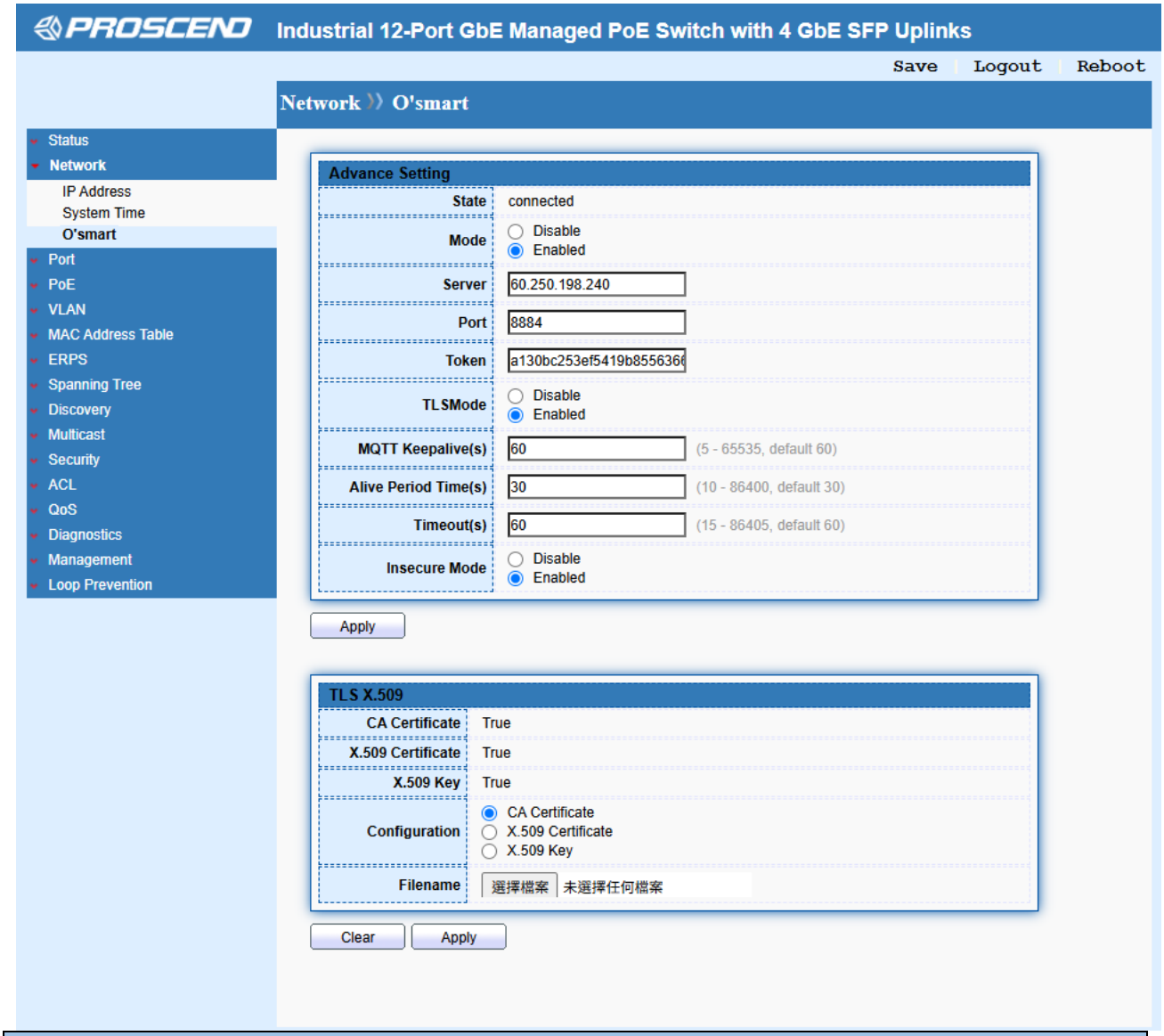


Network > IP Address	
Item	Description
Source	**SNTP**: Click it to get time and date from SNTP Server **From Computer**: Click it to get time and date from connected PC. **Manual Time**: Specify static time and date manually.
Tim Zone	Specify the time zone of your area.
SNTP	

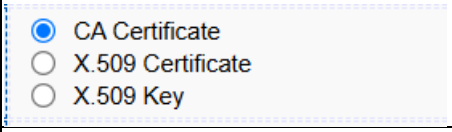
Address Type	Specify the address type of SNTP server.
Server Address	Enter the SNTP server IP address or hostname.
Server Port	Specify the service port of SNTP server.
Manual Time	
Date	Enter the date.
Time	Enter the time.
Daylight Saving Time	
Type	Select the type of daylight saving time. **None**: Disable daylight saving time. **Recurring**: Using recurring mode of daylight saving time. **Non-Recurring**: Using non-recurring mode of daylight saving time. **USA**: Using daylight saving time in the United States that starts on the second Sunday of March and ends on the first Sunday of November. **European**: Using daylight saving time in the Europe that starts on the last Sunday.
Offset	Specify the adjust offset of daylight saving time.
Recurring	**From**: Specify the starting time of recurring daylight saving time. **To**: Specify the ending time of recurring daylight saving time.
Non-recurring	**From**: Specify the starting time of non-recurring daylight saving time. **To**: Specify the ending time of non-recurring daylight saving time.
Operational Status	
Current Time	Display the current time and date of Switch.

5.3 O’smart

Remote management platform using MQTT.



Network > O’smart	
Advance Setting	Description
State	The status between device and O’smart server
Mode	Enable or disable the connection with O’smart server.
Server	Enter the O’smart server IP address or domain name.
Port	Enter the listen port of O’smart server.
Token	Enter the token that generated by O’smart server.

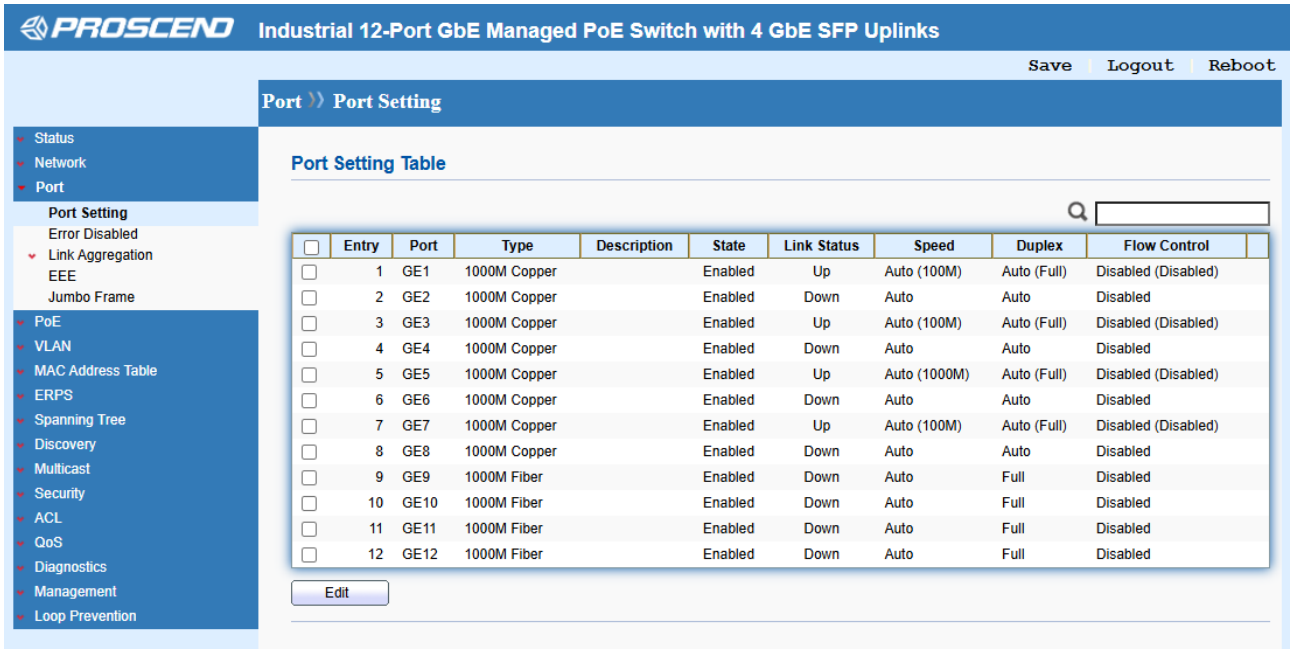
TLS mode	Enable or disable the secure connection with O'smart server.
MQTT Keepalive(s)	How much time the first keepalive packet will be sent on an apparently idle connection
Alive Period Time(s)	The duration between two successive keepalive retransmissions before the previous keepalive transmission is not received.
Timeout(s)	Keep alive session is not connected until overtime.
Insecure Mode	Allows the establishment of a secure encrypted connection by accepting SSL/TLS certificate issues, including expired certificates, invalid certificates, self-signed certificates, or incomplete/untrusted certificate chains.
Operational Status	
CA Certificate	True/False **True**:The image uploaded successfully; **False**:Null
X.509 Certificate	True/False **True**:The image uploaded successfully; **False**:Null
X.509 Key	True/False **True**:The image uploaded successfully; **False**:Null
Configuration	Choose an upload option 
Filename	Choose the file to up load.

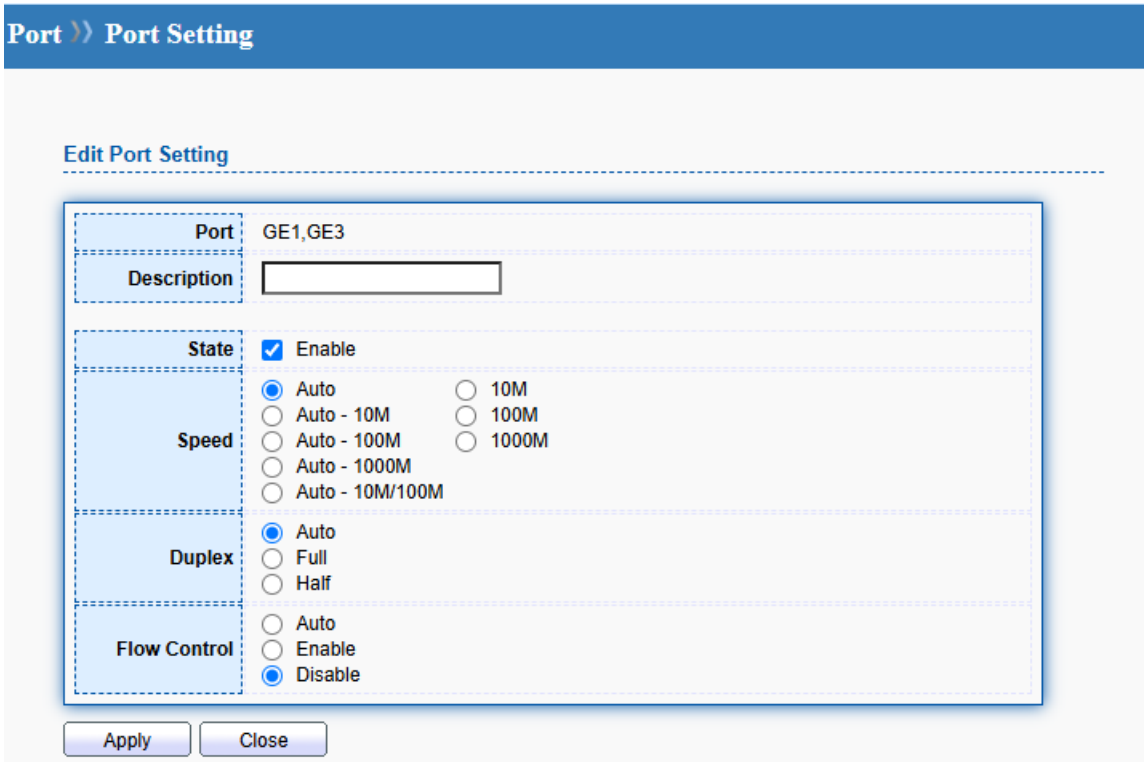
6 Port

Port Setting is used to configure settings for the switch ports, trunk, Layer 2 protocols and other switch features.

6.1 Port Setting

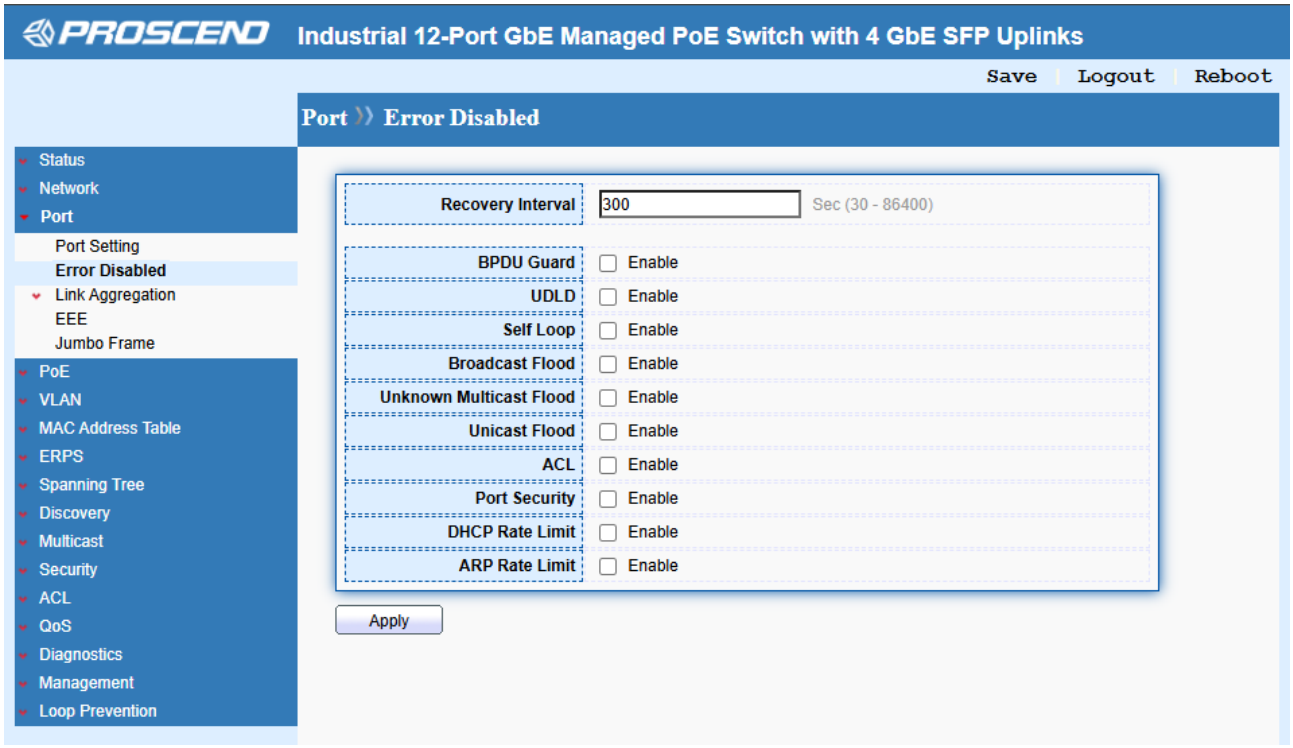
Available settings are explained as follows.





Item	Description
Edit	Edit specified port settings.
Port	The port number that you are doing setting now.
Description	Enter the description of this port.
State	Click it to enable/disable the port.
Speed	Specify the port speed, default is Auto. For SFP fiber module, you might need to **manually** configure the speed to match fiber module speed.
Duplex	Port duplex capabilities: **Auto**: Auto duplex with all capabilities. **Full**: Auto speed with 10/100/1000M ability only. **Half**: Auto speed with 10/100M ability only.
Flow Control	Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port. Click it to enable/disable Flow Control.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

6.2 Error Disabled



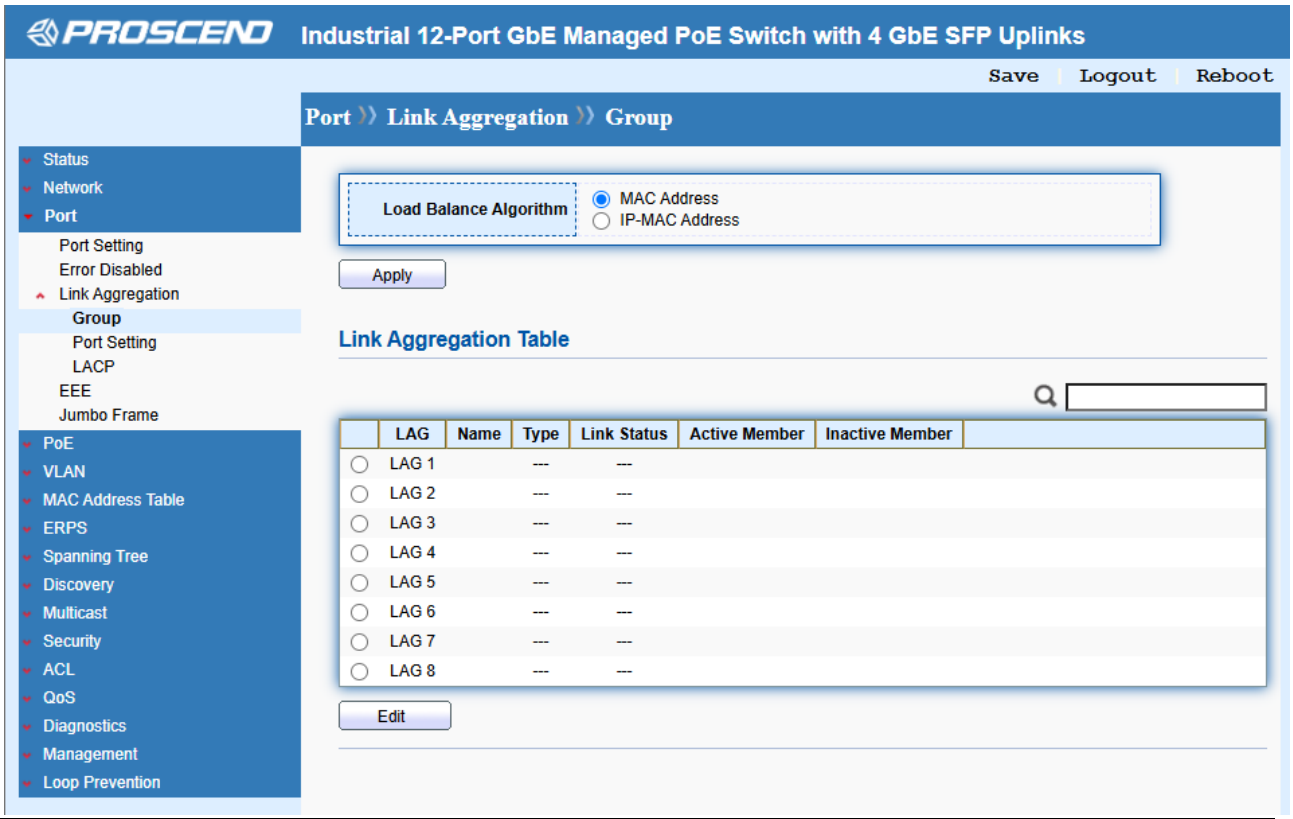
Item	Description
Recovery Interval	The port being blocked will be able to receive and send traffic after the time period configured here.
BPDU Guard	Recover the port being blocked by BPDU Guard after the time set in Recovery Interval.
UDLD	Check it to enable UniDirectional Link Detection (UDLD) function.
Self Loop	Recover the port being blocked by self loop Guard after the time set in Recovery Interval.
Broadcast Flood	Recover the port being blocked by broadcast flood after the time set in Recovery Interval.
Unknown Multicast Flood	Recover the port being blocked by unknown multicast flood after the time set in Recovery Interval.
Unicast Flood	Recover the port being blocked by unicast flood after the time set in Recovery Interval.
ACL	Recover the port being blocked by ACL after the time set in Recovery Interval.
Port Security	Recover the port being blocked by port security after the time set in Recovery Interval.

DHCP Rate Limit	Recover the port being blocked by DHCP rate limit after the time set in Recovery Interval.
ARP Rate Limit	Recover the port being blocked by ARP rate limit after the time set in Recovery Interval.
Apply	Apply the settings to the switch.

6.3 Link Aggregation

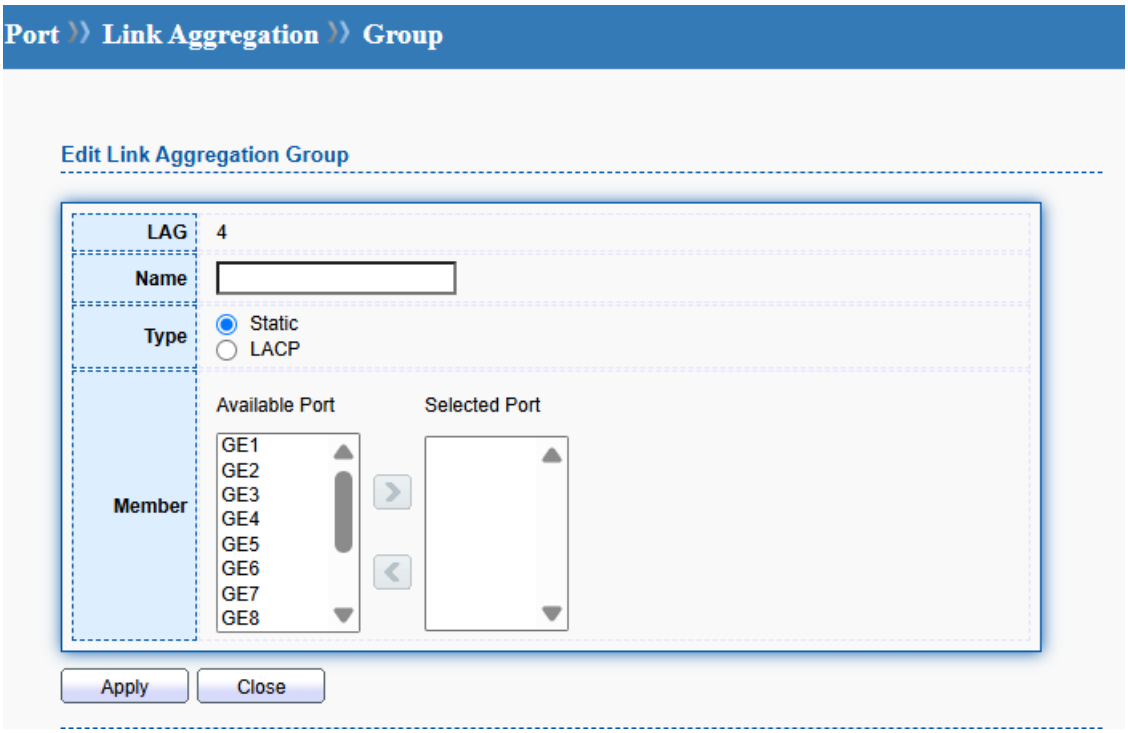
6.3.1 Group

Link Aggregation Group which groups some physical ports together to make a single high-bandwidth data path. Thus, it can implement traffic load sharing among the member ports in a group to enhance the connection reliability.



Item	Description
Load Balance Algorithm	Select Load balance algorithm. **MAC address**: Aggregated group will balance the traffic based on different MAC addresses. Therefore, the packets from different MAC addresses will be sent to different links. **IP-MAC Address**: Aggregated group will balance the traffic

	based on MAC addresses and IP addresses. Therefore, the packets from same MAC addresses but different IP addresses will be sent to different links.
Apply	Apply the settings to the switch.
Edit	Edit the profile of Link Aggregation group. There are eight LAG profiles allowed to group different physical ports. The system will assign certain port(s) as Active Member and Standby Member according to the port selections.

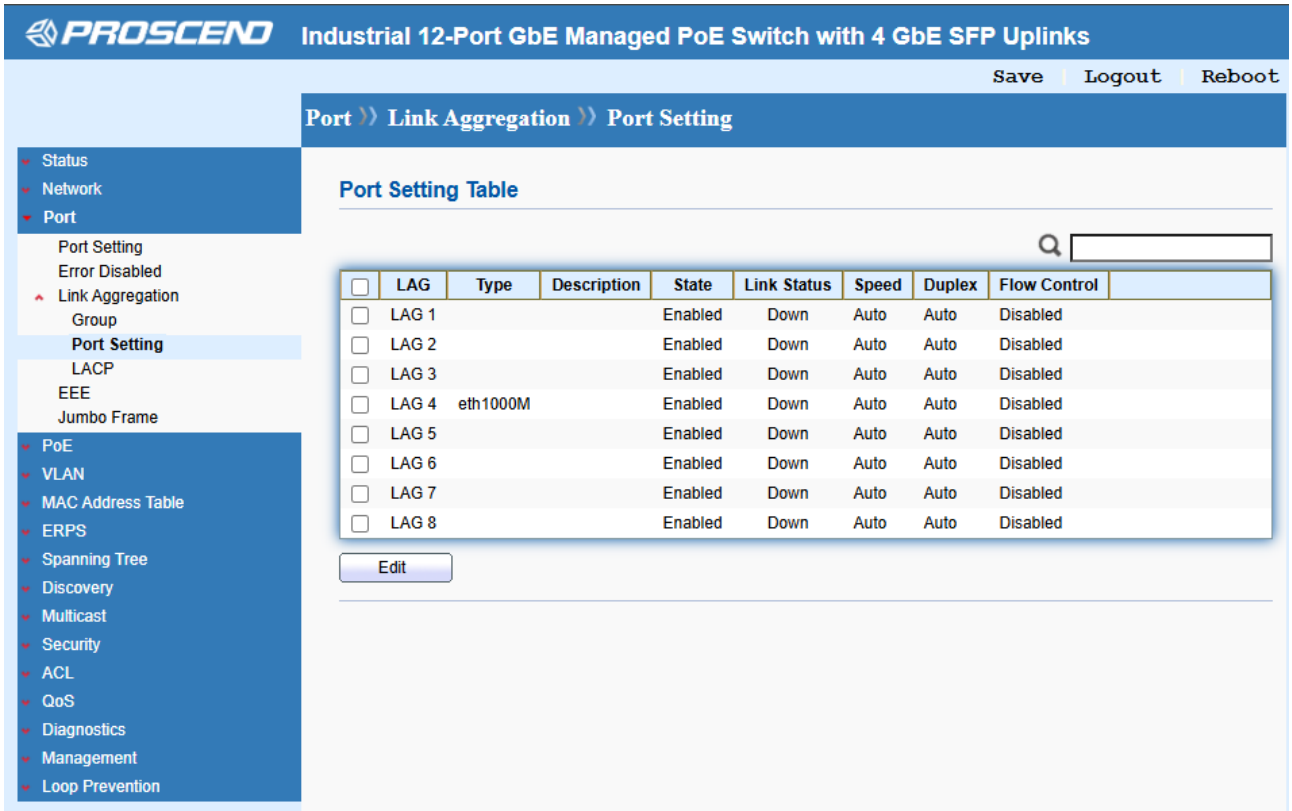


Item	Description
LAG	The index number of LAG group.
Name	Enter the name of the current LAG group.
Type	Select the type for current LAG group. **Static**: The static aggregated port sends packets over active member without detecting or negotiating with remote aggregated port. **Active**: The interface is in an active negotiating state. LACP runs on

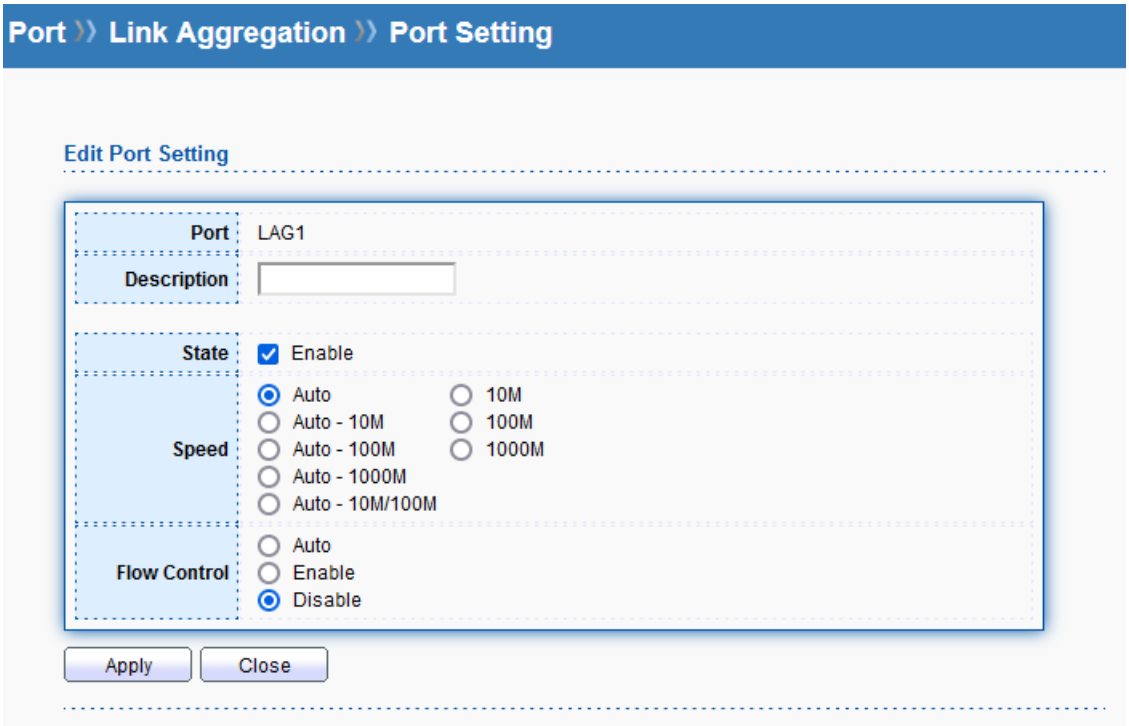
	any link that is configured to be in the active state. The port in an active mode also automatically initiates negotiations with other ports by initiating LACP packets.
Member	Select the member of the current LAG group.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

6.3.2 Port Setting

This page defines port setting for each LAG profile (LAG1 to LAG8), including data speed and enabling/disabling the flow control.



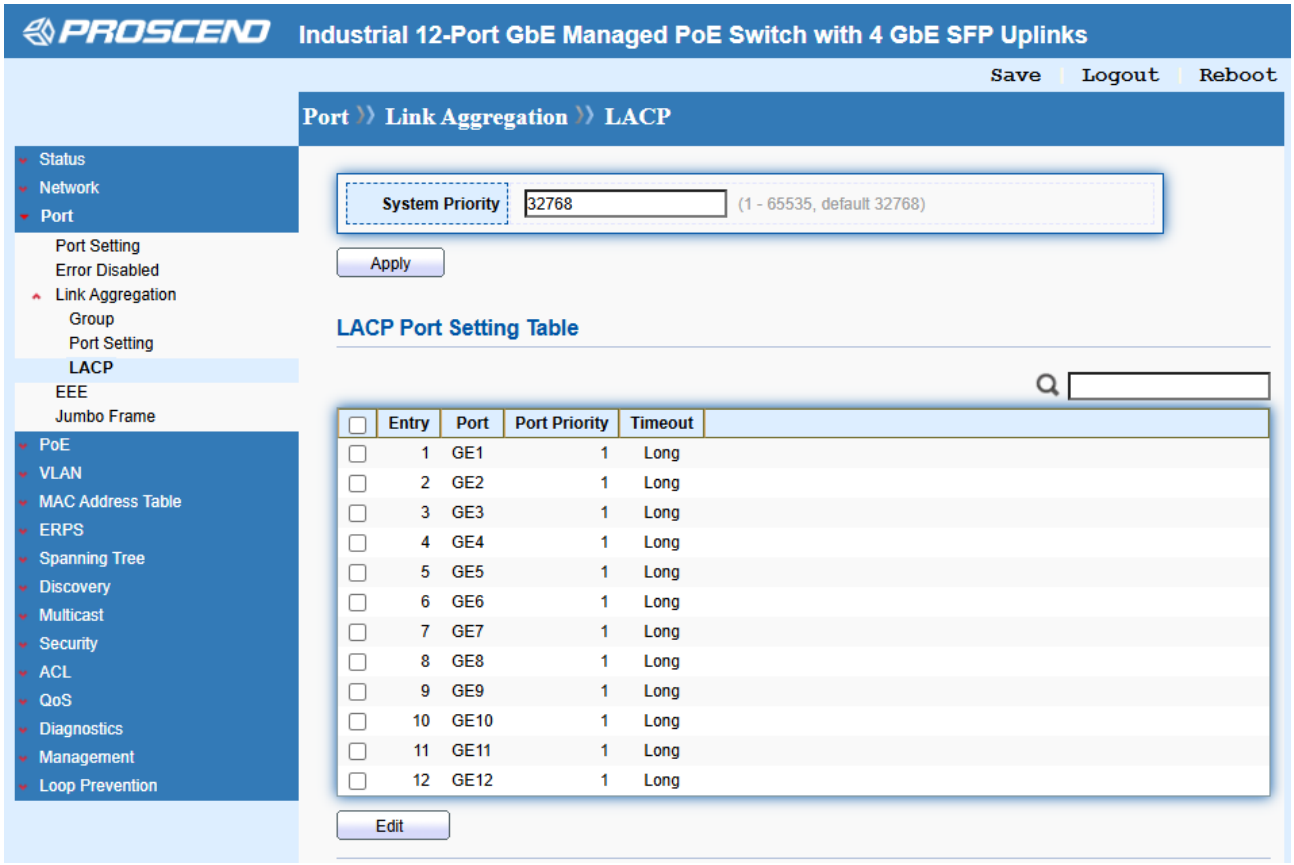
Item	Description
Edit	Edit the settings of LAG port.



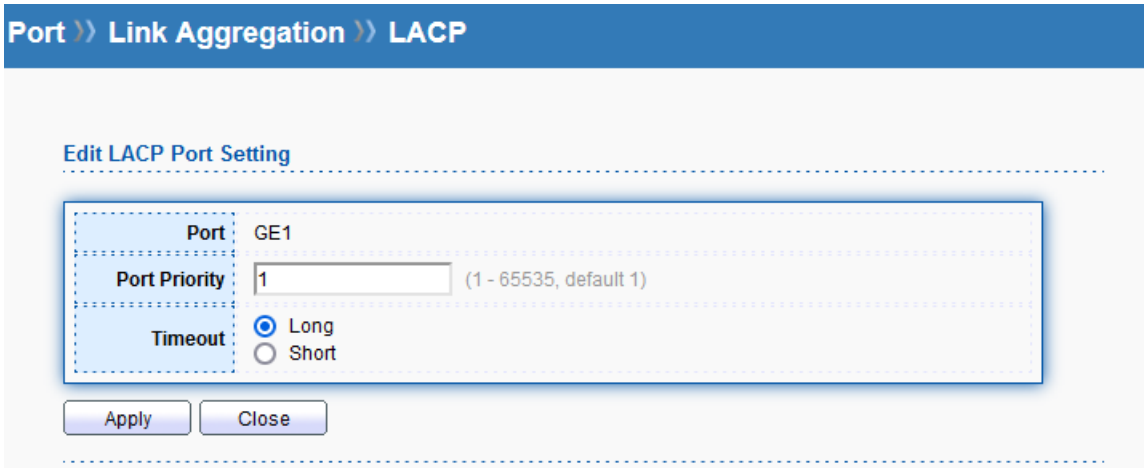
Item	Description
Port	The index number of current LAG port.
Description	Enter the description of the current LAG port.
State	Enable or disable the LAG port.
Speed	Select the specified speed for LAG port.
Flow Control	Flow control is based on IEEE 802.3x and is effective only when the connected device supports compatible flow control settings. Auto: Negotiates the flow control mode automatically with the link partner Enable: Enable Ethernet flow control. Disable: Disables Ethernet flow control.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

6.3.3 LACP

This page allows the network administrator to change system priority of the LACP function.



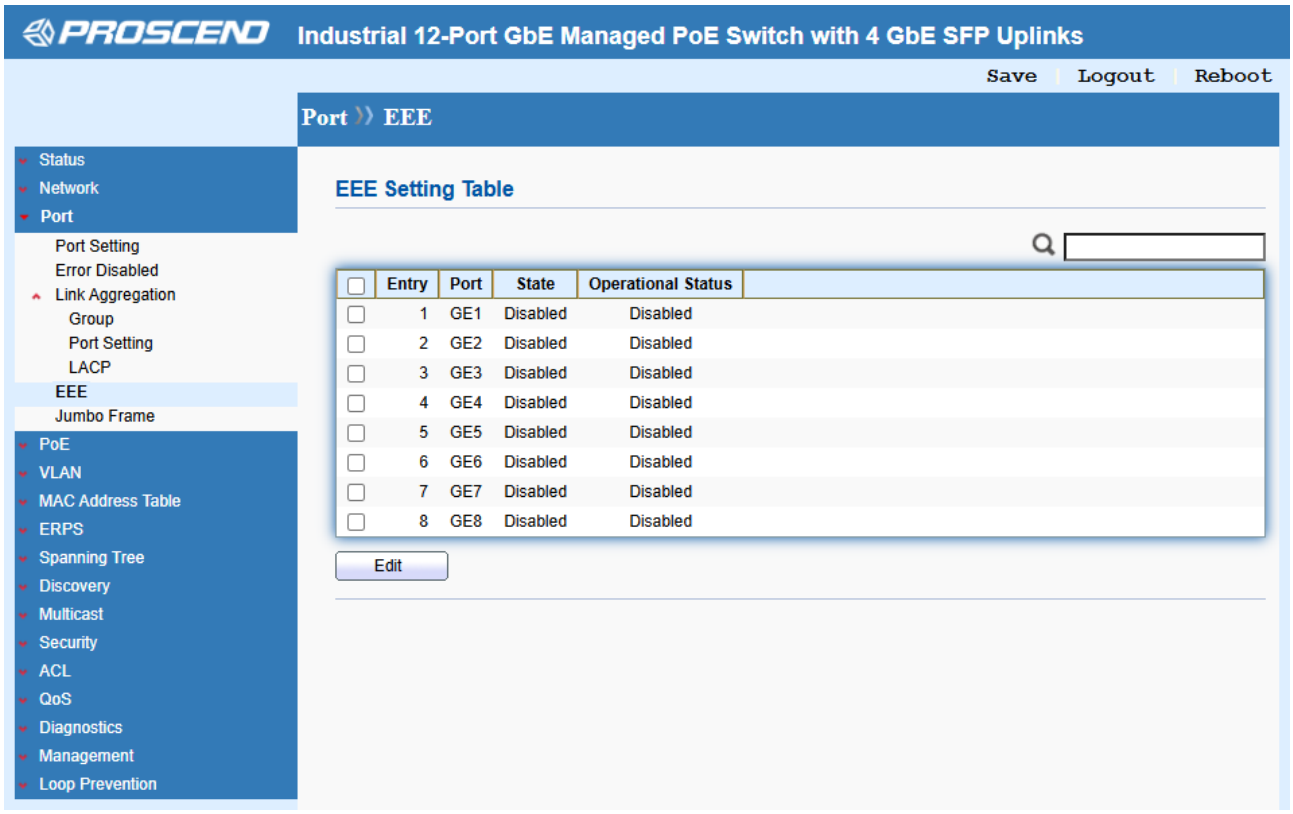
Item	Description
System Priority	The priority is used to determine which switch (local or remote) on the LAG connection is able to decide LACP activities.
Apply	Apply the settings to the switch.
Edit	Edit the settings of LACP port.

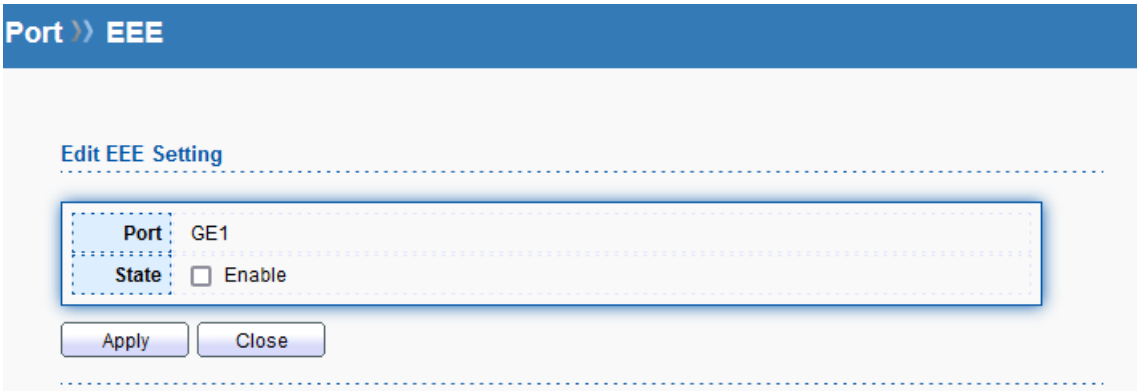


Item	Description
Port	The index number of LACP port.
Port Priority	Enter the priority number for the port.
Timeout	The timeout option decides how local switch of LAG connection determines connection to be lost. Switch would also notify the remote switch about this setting value, so that remote switch can send LACP PDU in correct timing. **Long**: LACP PDU will be sent every 30 seconds. If port member is not seen over 90 seconds, it will cause port member timeout. **Short**: LACP PDU will be sent per second. If port member is not seen over 3 seconds, it will cause port member timeout.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

6.4 EEE

This page allows a user to enable or disable port EEE (Energy Efficient Ethernet) function.



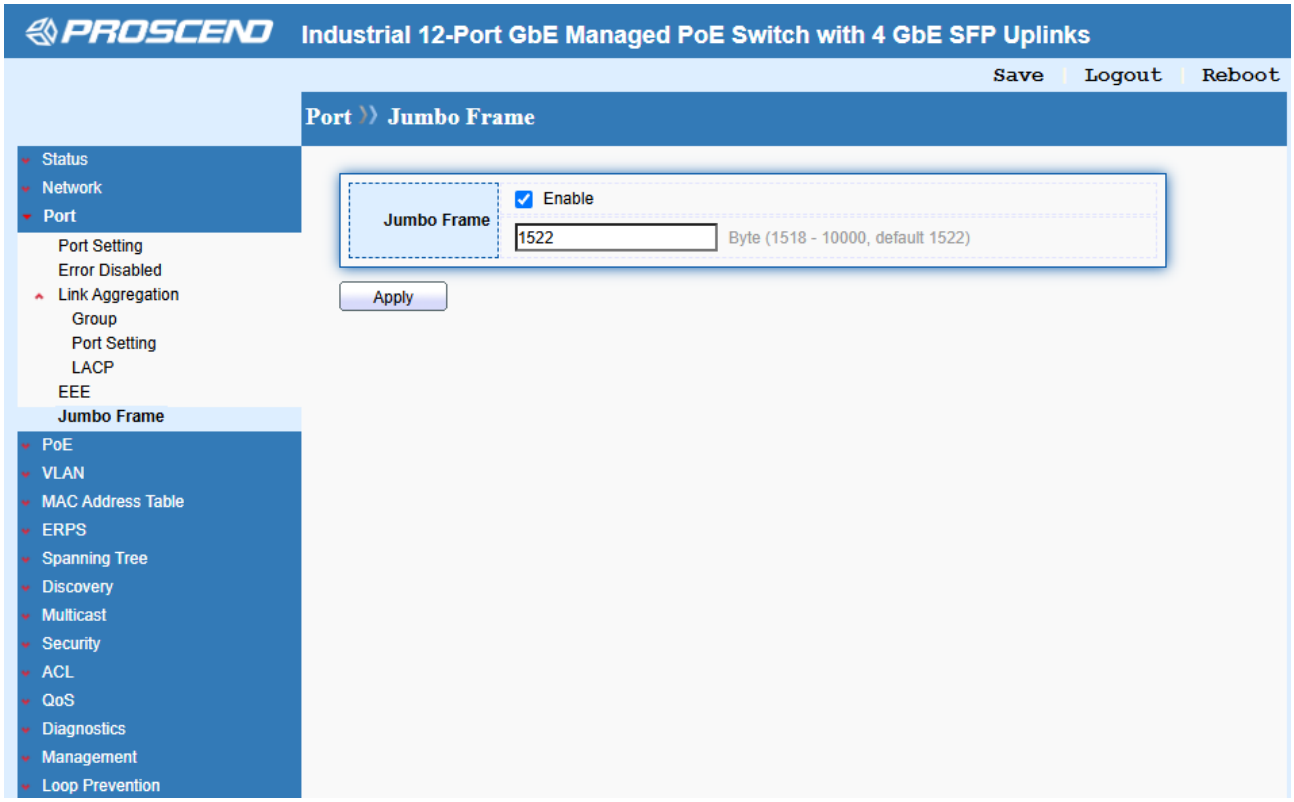


Item	Description
Edit	Edit the settings of the EEE.
Port	The index number of the port

State	Enable or disable the EEE function of the port.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

6.5 Jumbo Frame

This page allows a user to configure switch port jumbo frame settings.

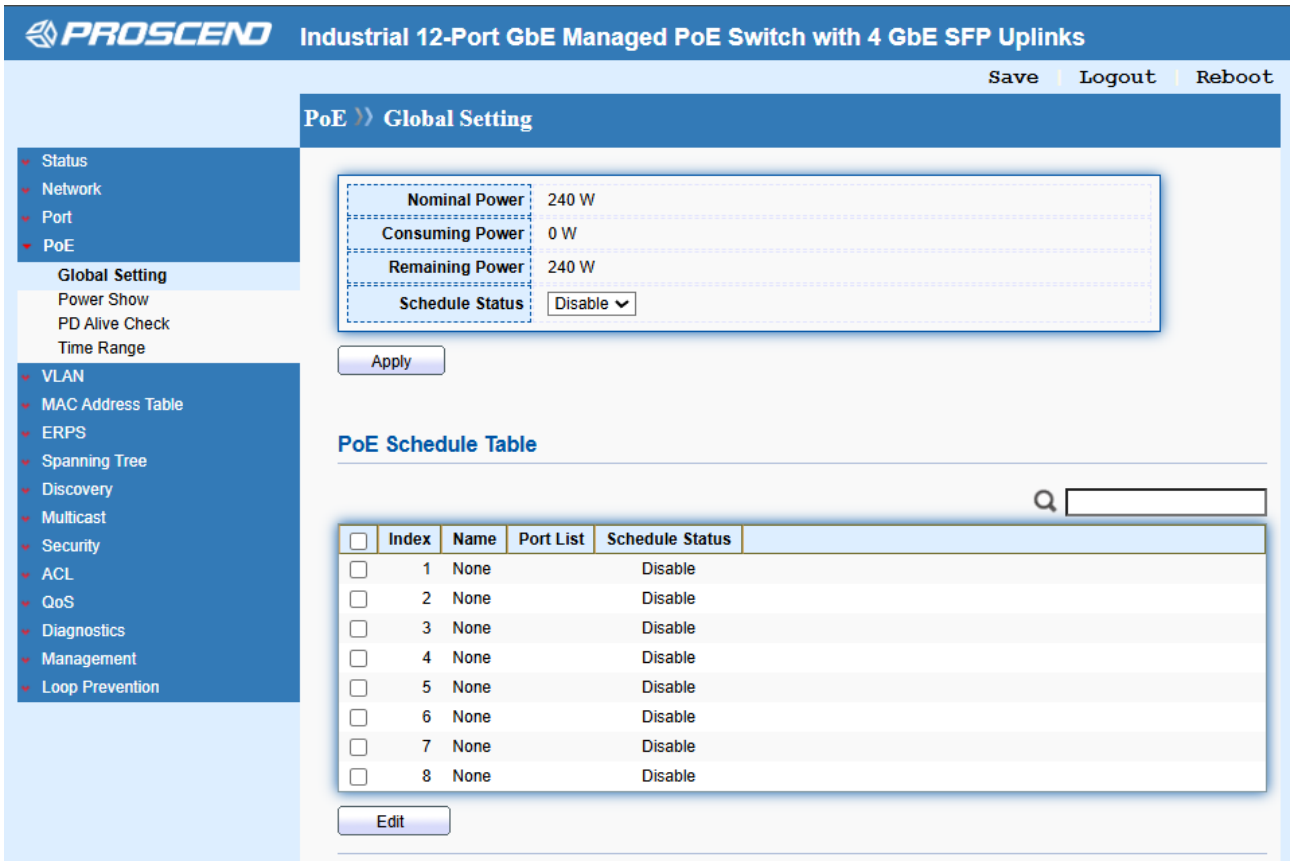


Item	Description
Jumbo Frame	Enable or disable the Jumbo Frame setting.
Apply	Apply the settings to the switch.

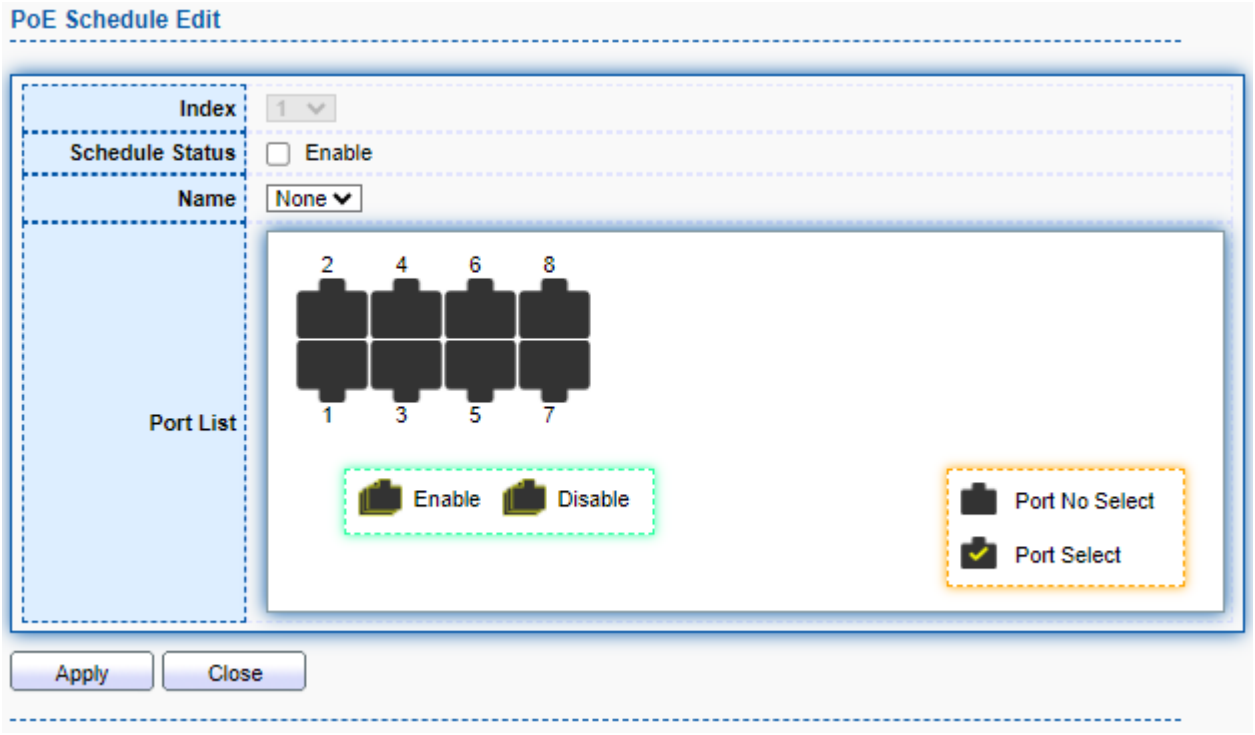
7 PoE

This section allows you to setup Global PoE Setting, Power Show, Power Passive PD Alive Check and Time Range.

7.1 Global Setting



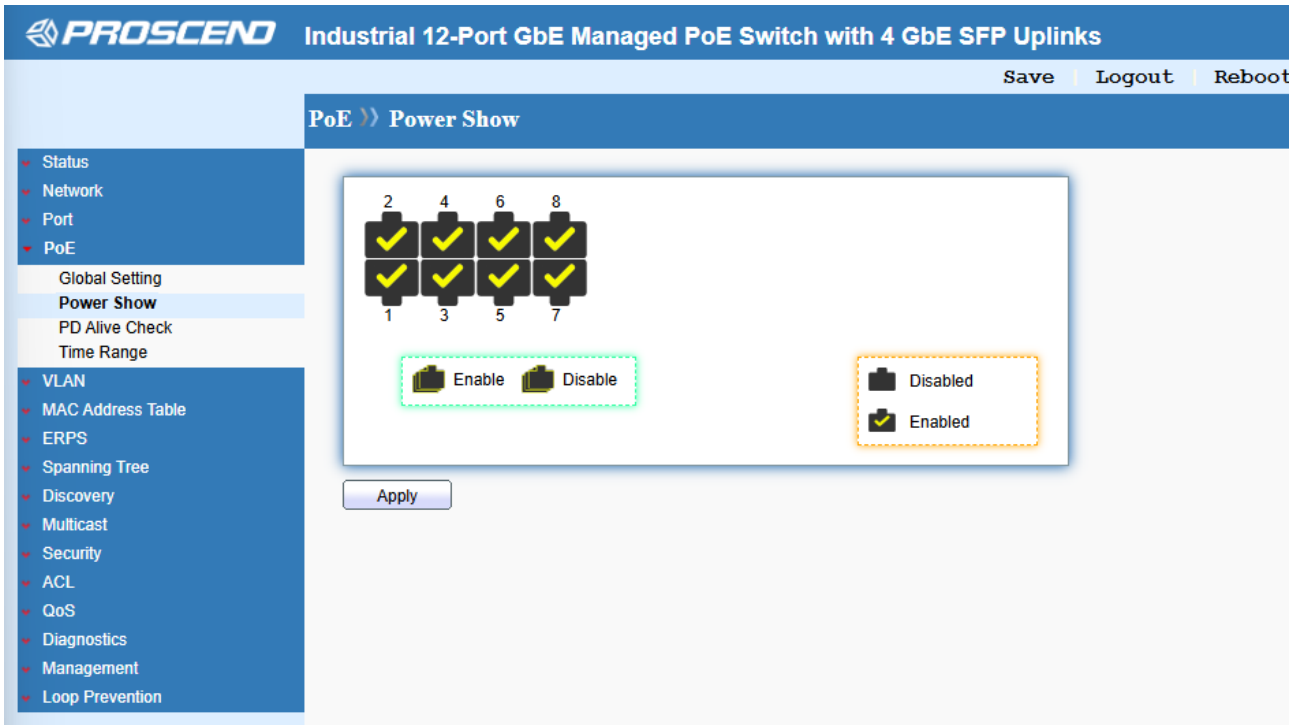
Item	Description
Nominal Power	Total PoE power budget of the device can be configured Max Power Limit Range is 240 (W).
Consuming Power	Displays the total consuming power for all the PDs.
Remaining Power	Displays the Remaining power for all the PDs.
Schedule Status	Enable/Disable schedule status



Item	Description
Index	Index of PoE schedule table.
Schedule Status	Enable/Disable schedule status.
Name	Name of schedule status name.
Port List	Port list for selecting port enable and disable schedule.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

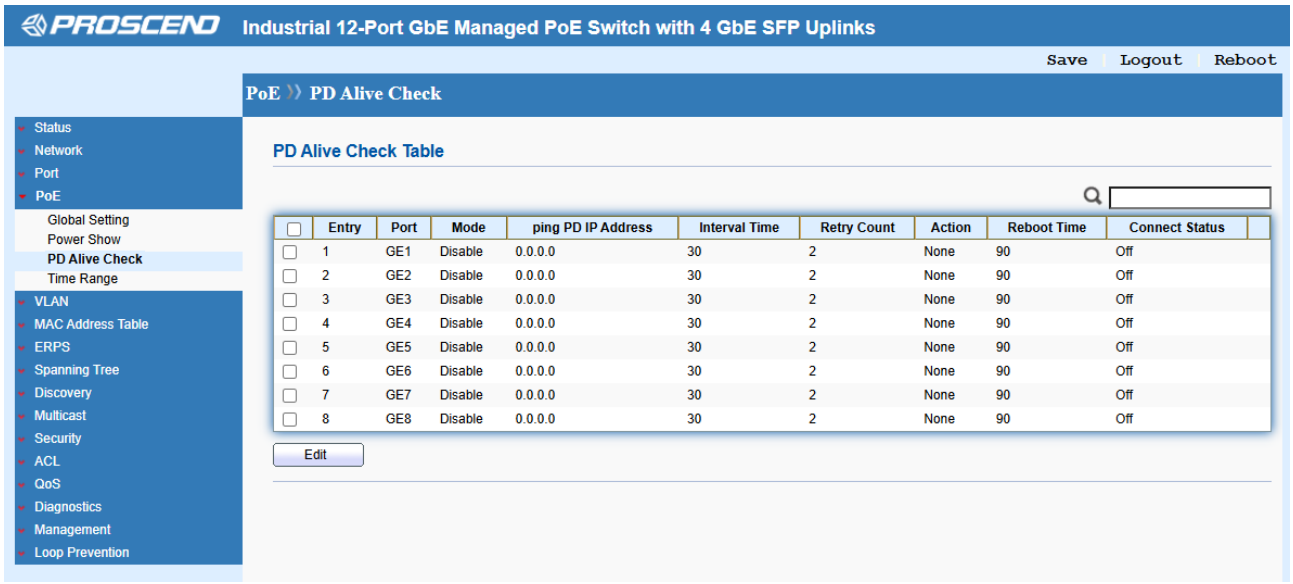
7.2 Power Show

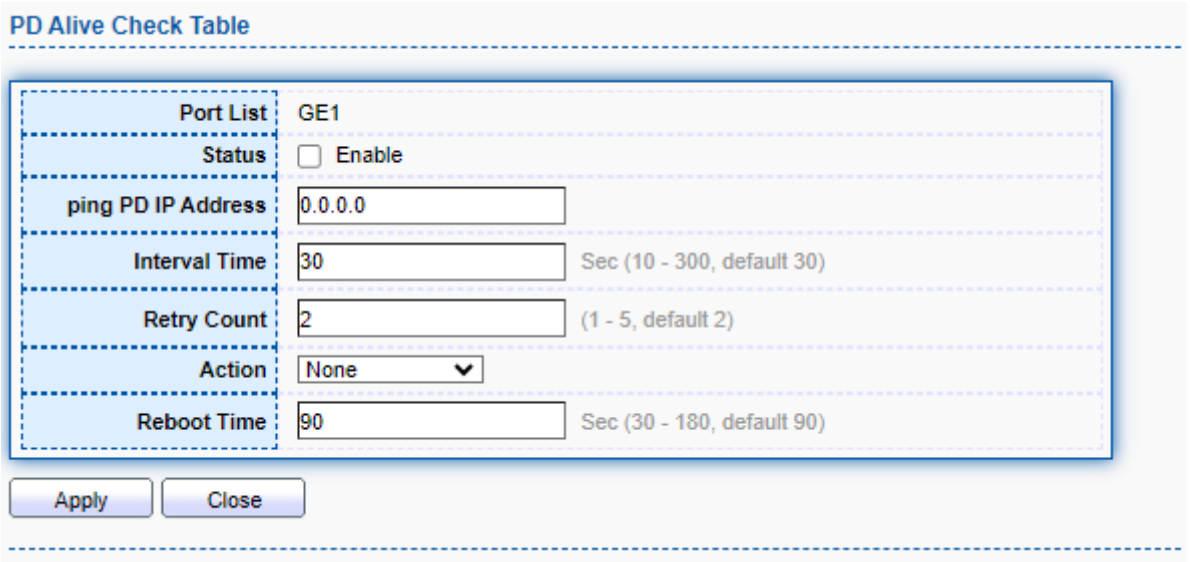
This page displays the current PoE mode of all ports.



7.3 PD Alive Check

This page allows a user to enable or disable port PD Alive Check function. If the port's state is enabled, the Switch will send keep-a-live probe packet every interval time. If the host cannot respond when the keep-a-live probe packet count is over the retry times, the Switch performs the action, PD Reboot/Reboot&Alarm/Alarm to the Power Device, depending on the port's configuration.



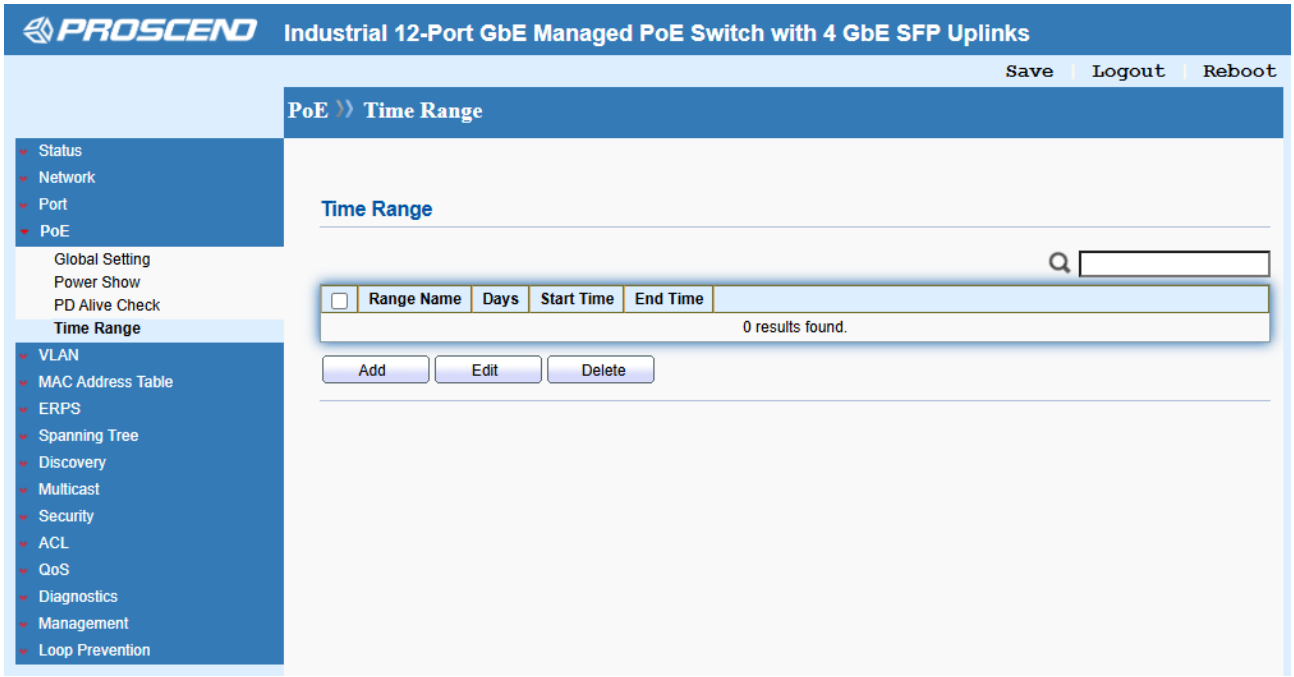


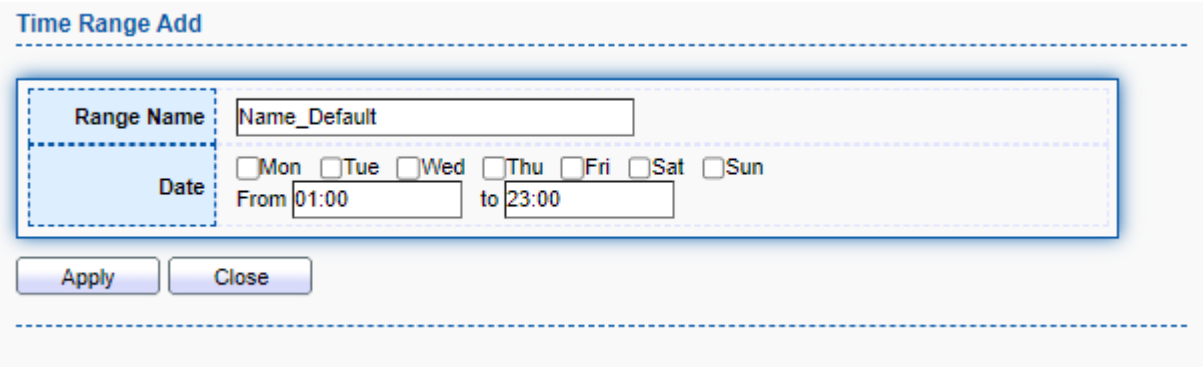
Item	Description
Edit	Edit the settings of the PD Alive Check.
Port List	The index number of the port

State	Enables/Disables the PD Alive Check.
ping PD IP Address	Specifies the Host IP address which connects to the port.
Interval Time	The interval to send the packet probes to check if the host is still alive.
Retry Count	The retry times when no response from the host for the keep-a-live probe packet.
Action	The action to the Power Device when the system detects that the Power Device cannot respond the keep-a-live probe packet. **PD Reboot**: Cut off the power of the PoE port, make PD rebooted. **Reboot&Alarm**: Send an alarm message to inform the administrator and then reboot the PD. **Alarm**: Just send an alarm message to inform the administrator. **None**: Keep Ping the remote PD but does nothing further.
Reboot Time	Reboot after retries timeout.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

7.4 Time Range

This page allow a user to add schedule status.





Item	Description
Range Name	Name of range.
Date	Week: Enables/Disables the PD Alive Check. Time: User can configure the PoE Schedule time from 0 to 24 Hrs
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

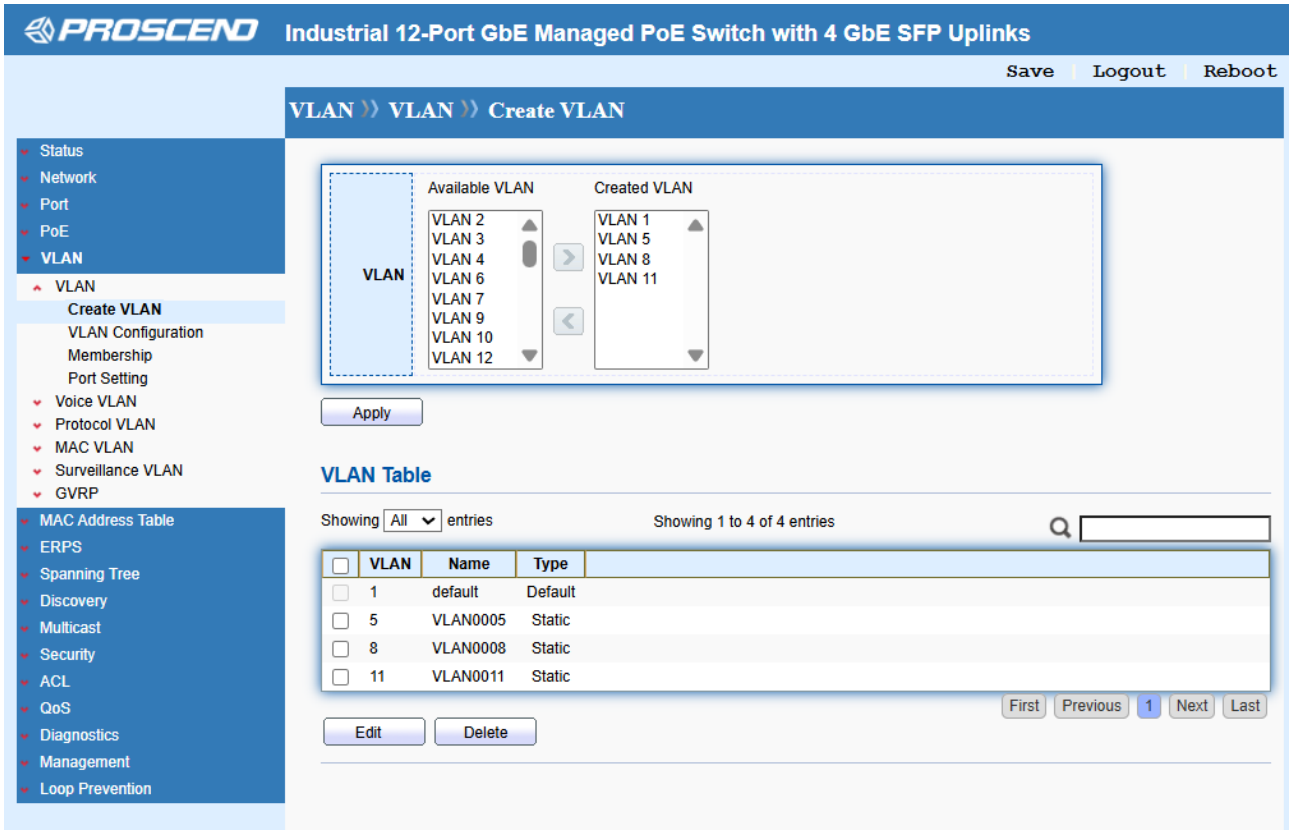
8 VLAN

This section allows for controlling VLAN configuration on the switch

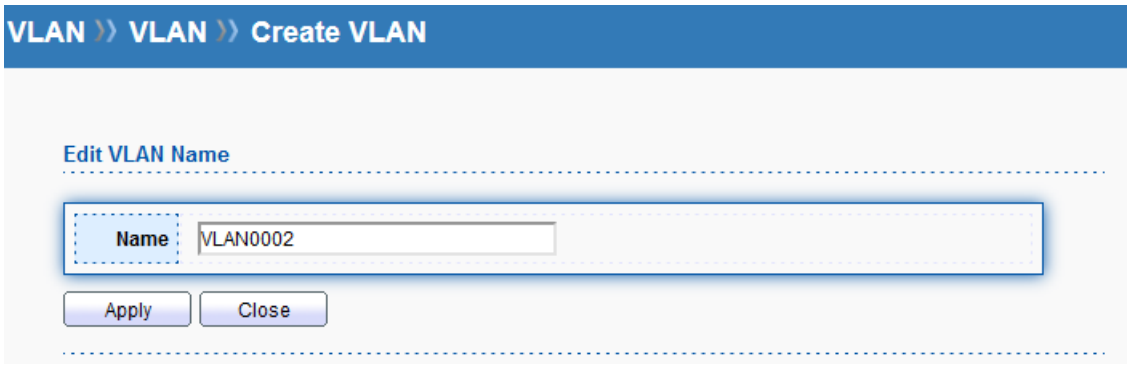
8.1 VLAN

8.1.1 Create VLAN

This page allows to add, edit or delete VLAN settings.



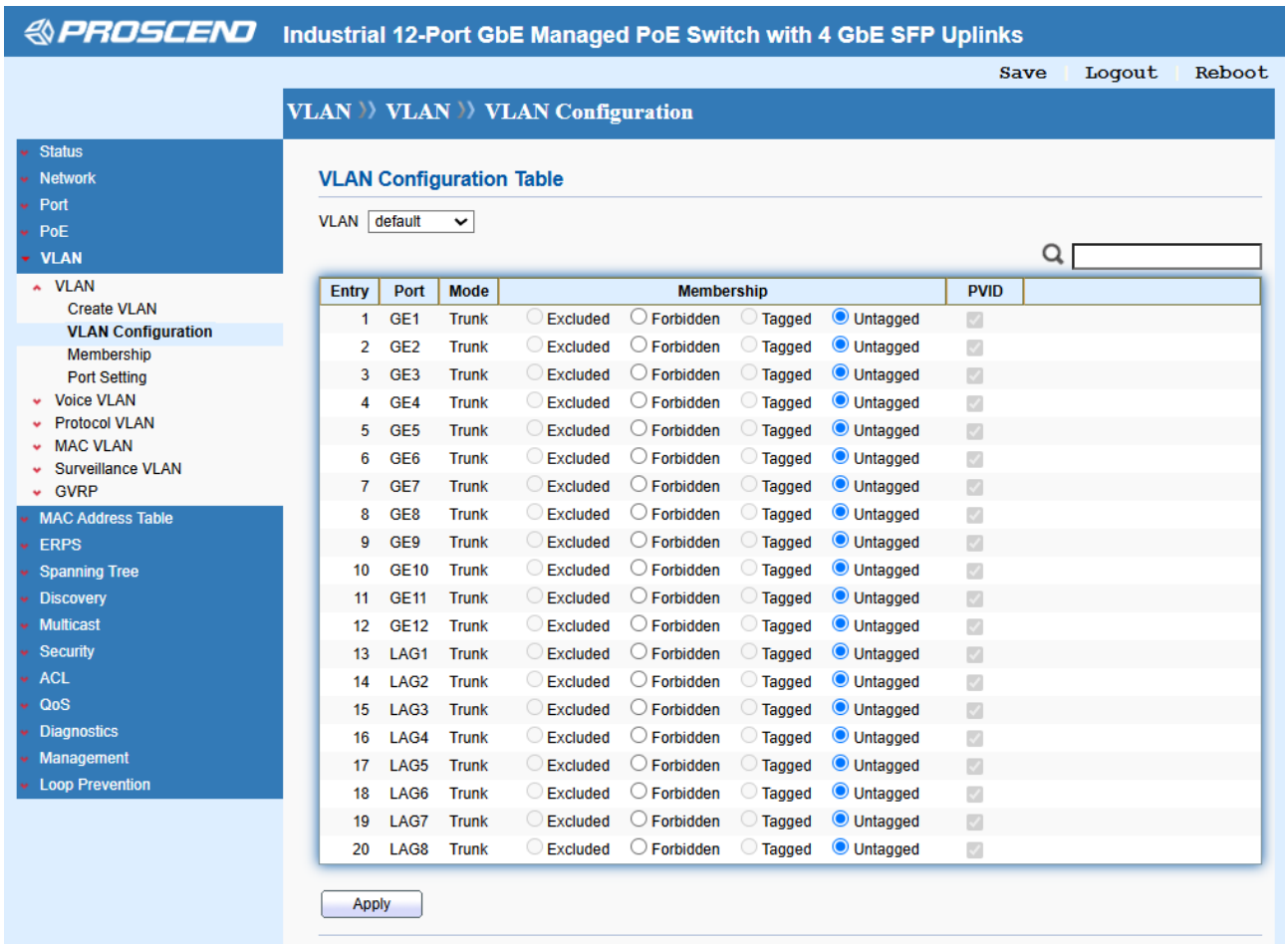
Item	Description
VLAN	Select available VLAN ID and move to created VLAN for creating VLAN settings.
Apply	Apply the settings to the switch.
Edit	Edit selected VLAN ID.
Delete	Delete selected VLAN ID.



Item	Description
Name	Modify the name of the specified VLAN ID.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

8.1.2 VLAN Configuration

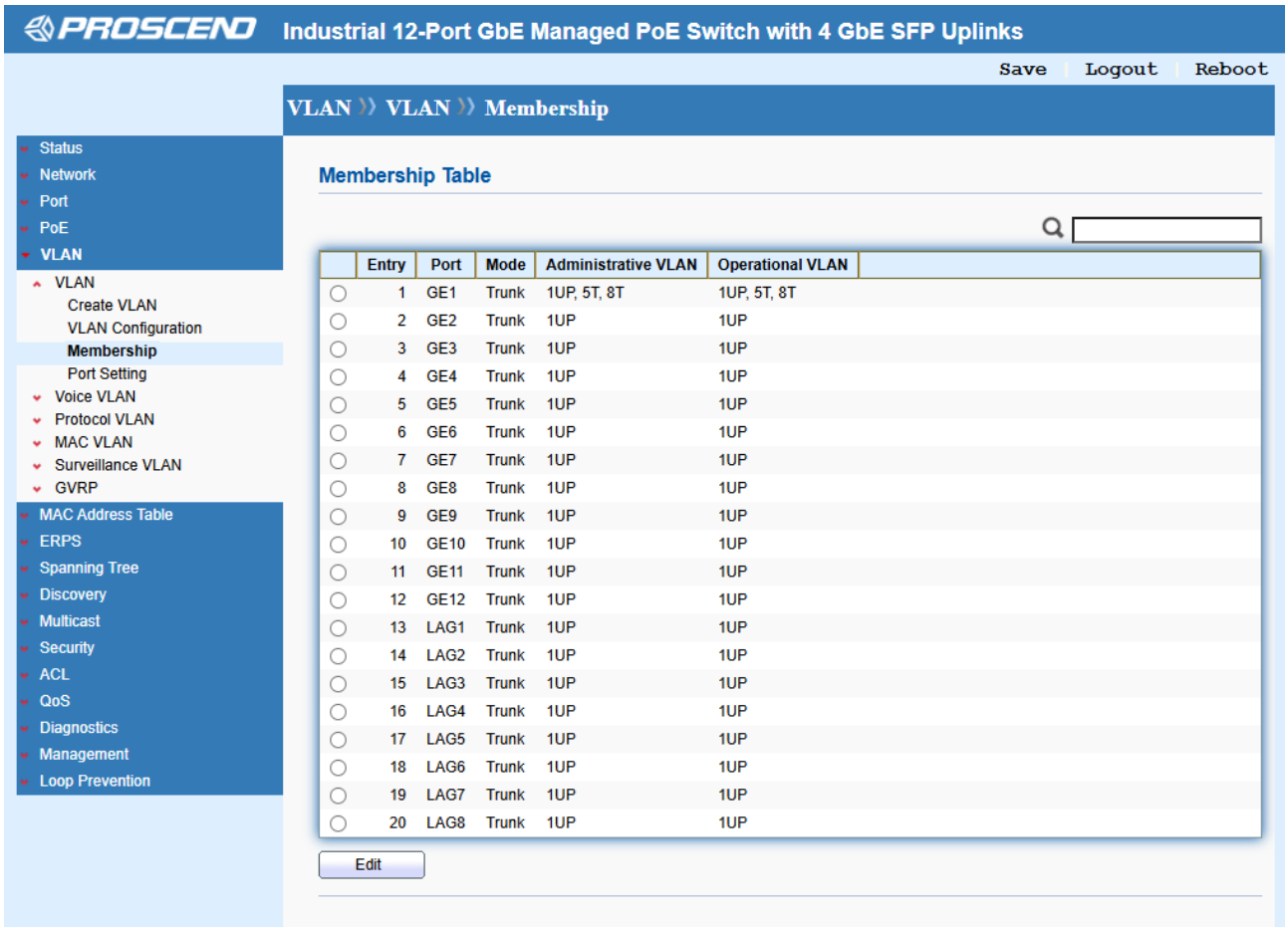
This page allows to configure interface setting related to VLAN.

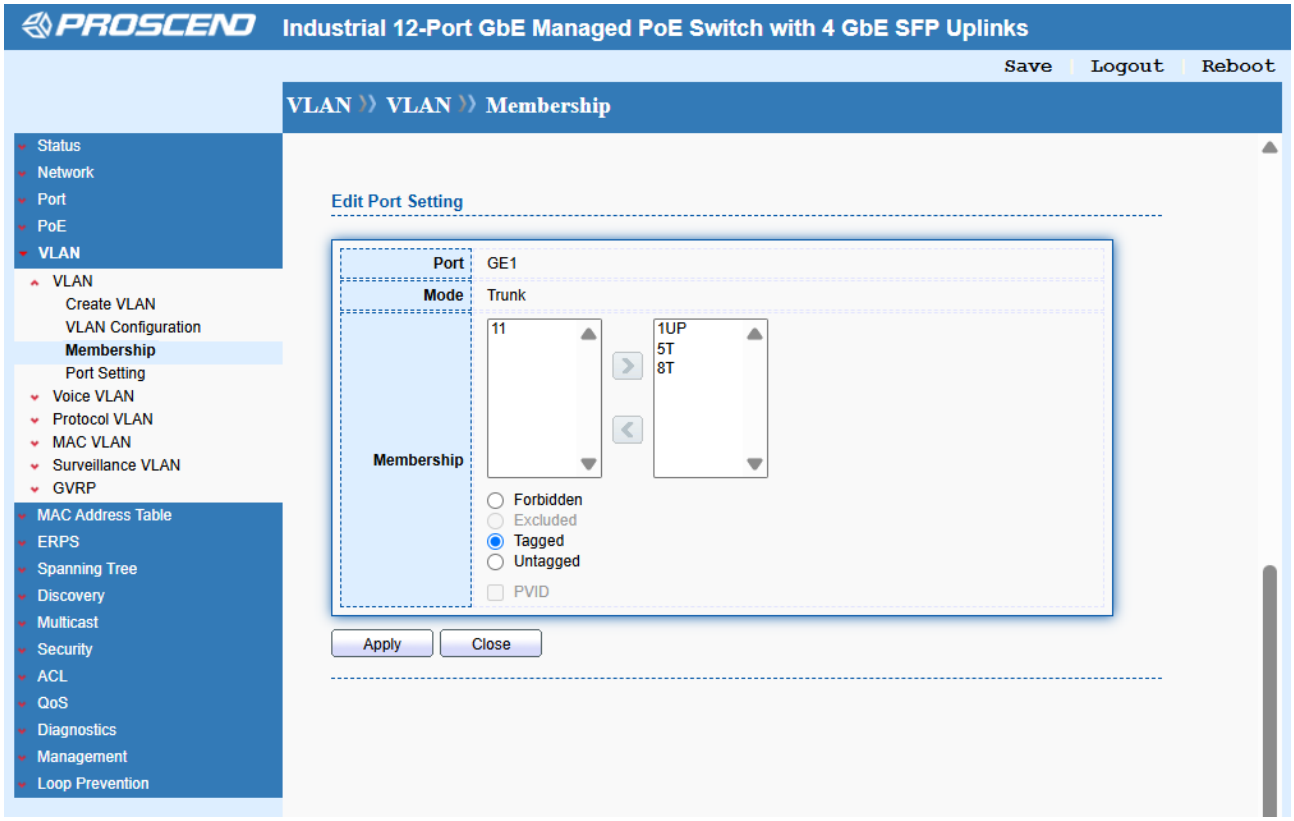


Item	Description
VLAN	Configure the VLAN settings of selected VLAN ID.
Membership	**Excluded**: Specify the VLAN profile excluded in the VLAN. **Forbidden**: Specify the VLAN profile forbidden in the VLAN. **Tagged**: Specify the VLAN profile tagged in the VLAN. **Untagged**: Specify the VLAN profile untagged in the VLAN.
PVID	A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines.
Apply	Apply the settings to the switch.

8.1.3 Membership

This page allows to configure the settings of membership on each port.

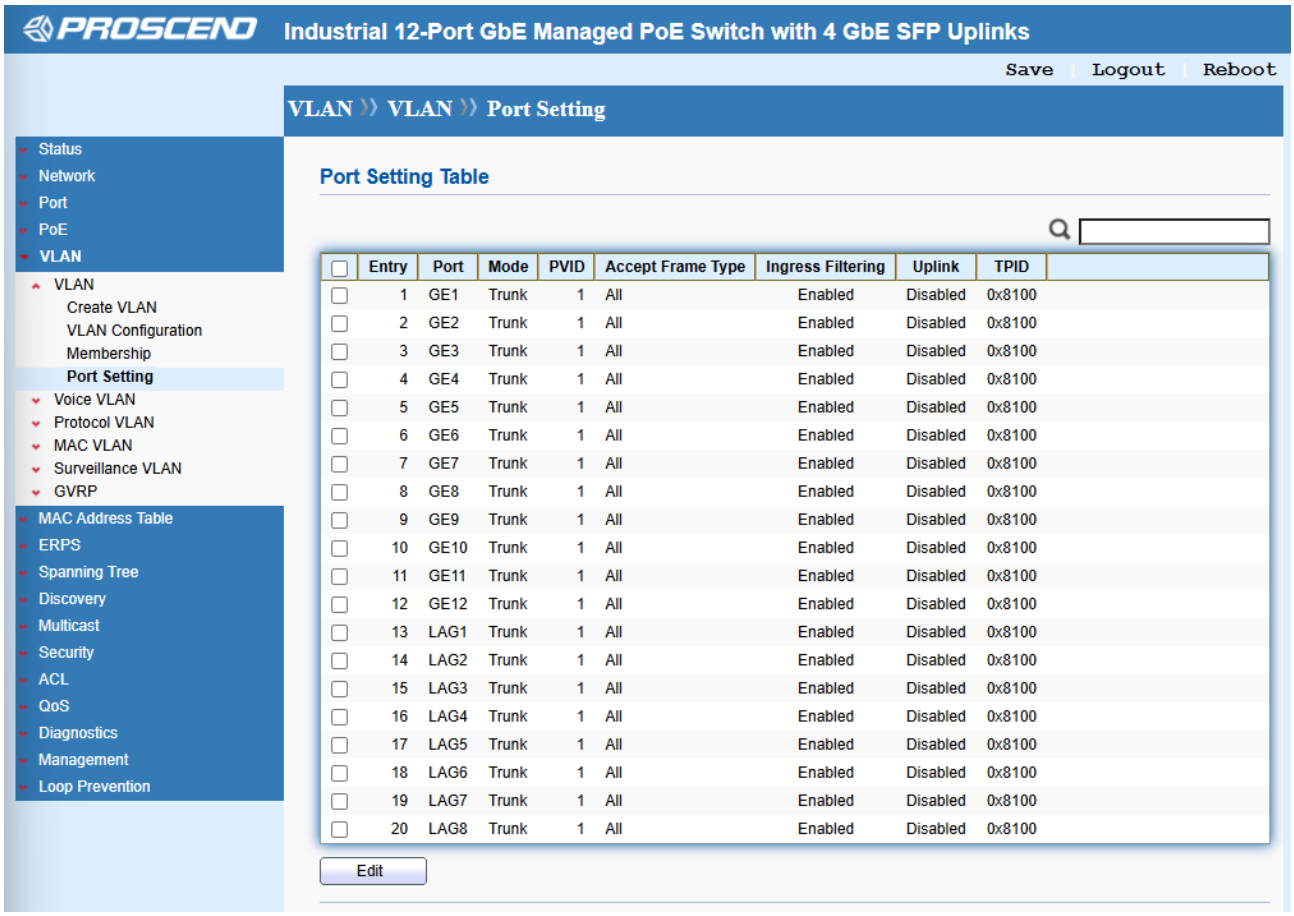


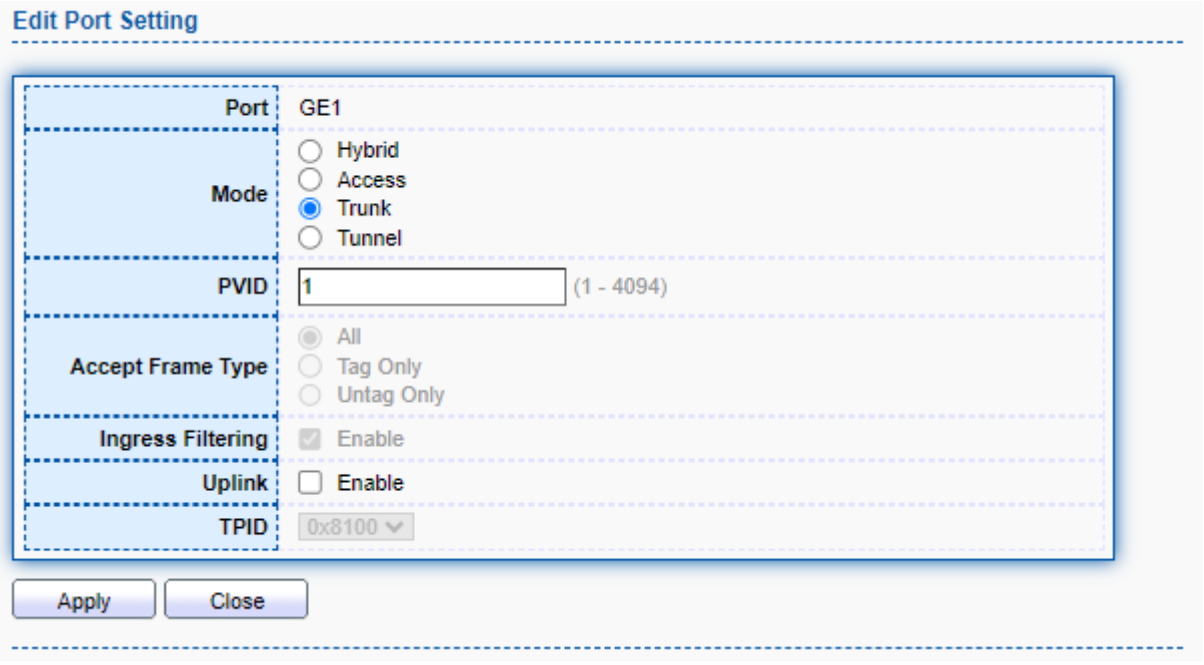


Item	Description
Edit	Edit the settings of the selected port.
Port	The index number of the selected port.
Mode	The mode of the selected port.
Membership	**Forbidden**: Specify the VLAN profile forbidden in the VLAN. **Excluded**: Specify the VLAN profile excluded in the VLAN. **Tagged**: Specify the VLAN profile tagged in the VLAN. **Untagged**: Specify the VLAN profile untagged in the VLAN.
PVID	A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

8.1.4 Port Setting

This page allows to configure more port settings of the VLAN.





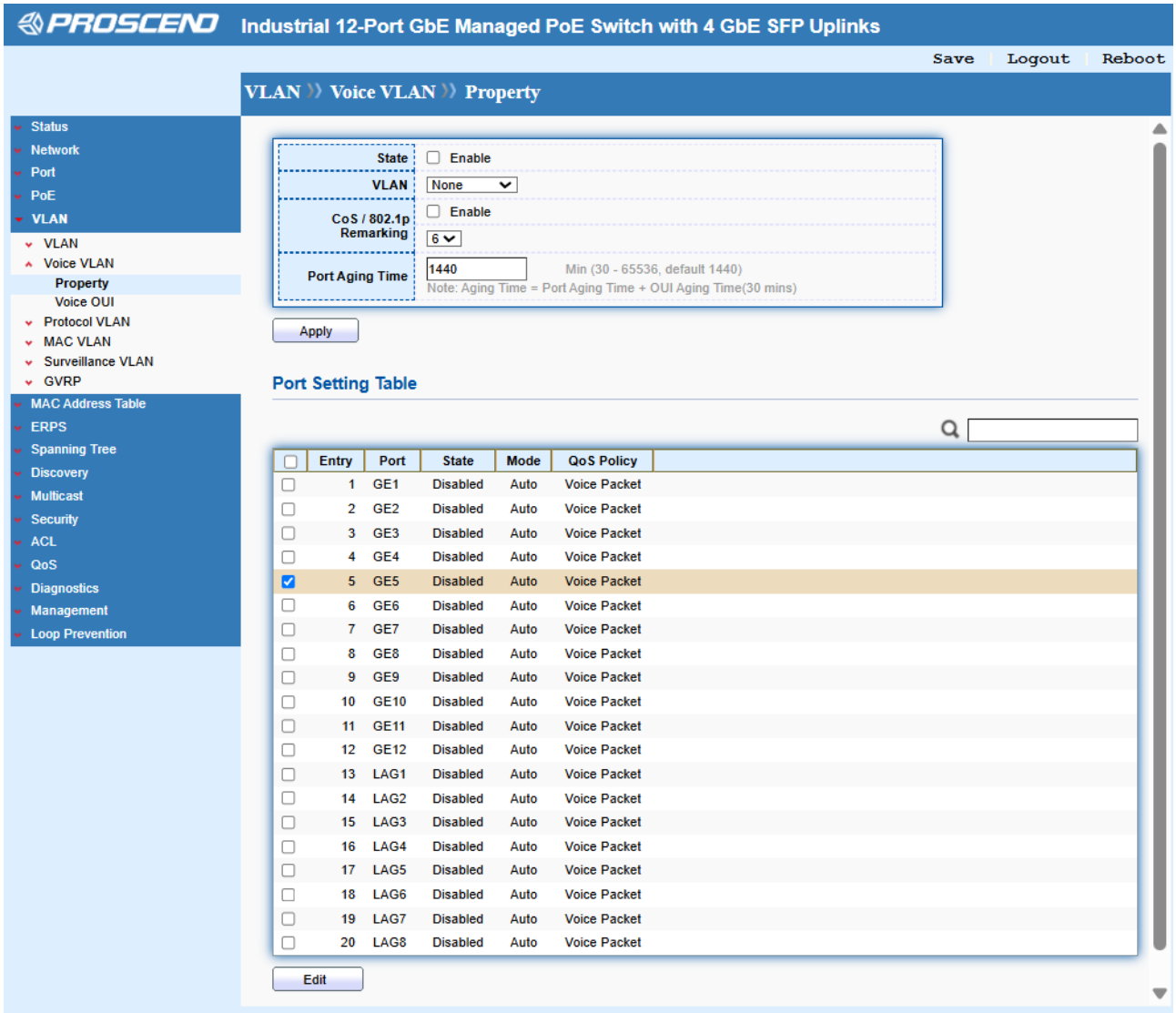
Item	Description
Edit	Edit the settings of the selected port.
Port	The index number of the selected port.
Mode	Select the VLAN mode of the port. Hybrid: Support all functions as defined in IEEE 802.1Q specification. **Access:** Accept only untagged frames and join an untagged VLAN. **Trunk:** An untagged member of one VLAN at most, and is a tagged member of zero or more VLANs. **Tunnel:** Accept packets with tag stacking (double tagging) by following the 802.1Q-in-Q tunneling.
PVID	A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines. For port under Access Mode, VLAN ID provided as PVID would automatically be selected as the untagged VLAN.
Accept Frame Type	Specify the acceptable-frame-type of the specified interfaces. It's only available with Hybrid mode. **All**: Accept frames regardless it's tagged with 802.1q or not. **Tag Only**: Accept frames only with 802.1q tagged. **Untag Only**: Accept frames untagged.
Ingress Filtering	Enable or disable the Ingress Filtering function. Enable the ingress filtering to filter out any packets not belong to any VLAN members of this port. It is enabled automatically while operating in Access and Trunk mode.
Uplink	Configure the selected port as the role of trunk. It can recognize double tagging on the interface.
TPID	Specify the TPID of the port.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

8.2 Voice VLAN

With such feature, a VLAN will be created temporarily and when the specified OUI device delivers protocol packets related to “VoIP”, the Switch will guide these packets into the specified Voice LAN with specified priority tag to speed up the packet transmission. Such voice VLAN is only active inside ~~Vigor~~Switch for packet transmission. After these packets leave ~~Vigor~~Switch, the Voice VLAN tag will be removed immediately.

8.2.1 Property

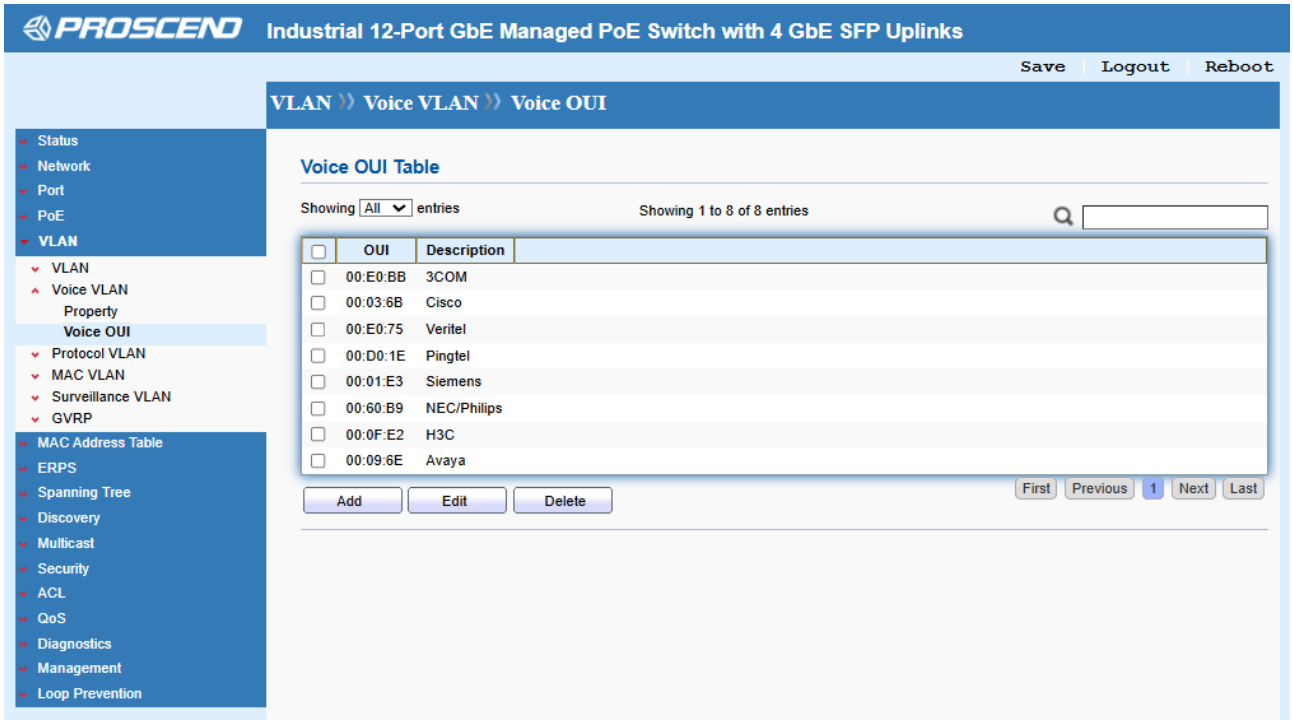
This page allows to configure global and per interface setting of voice VLAN.

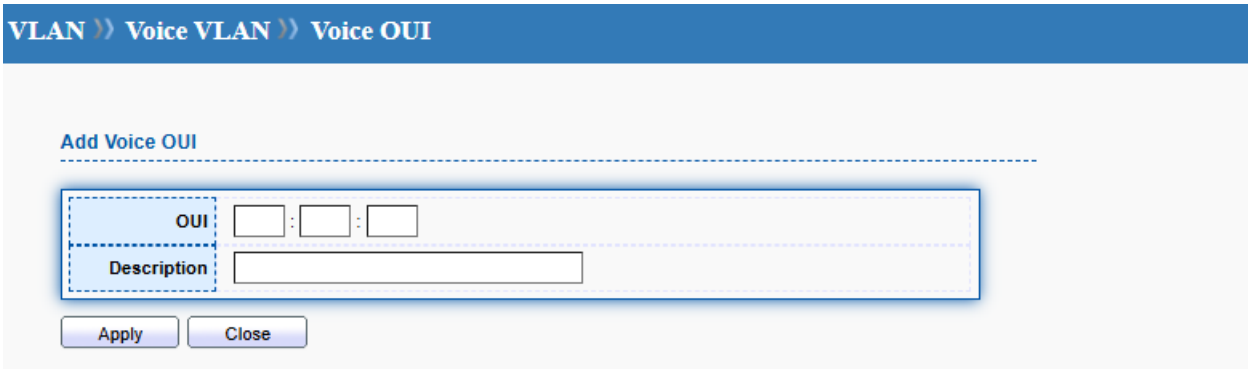


Item	Description
State	Enable or disable the Voice VLAN function.
VLAN	Select the VLAN ID which will be applied for Voice VLAN.
CoS / 802.1p Remarking	Enable or disable 802.1p remarking. If enabled, qualified packets will be remarked by specified value.
Port Aging Time	Enter the value of aging time (30~65536 min). Default is 1440 minutes. A voice VLAN entry will be age out after this time if without any packet pass through.
Apply	Apply the settings to the switch.
Edit	Edit the settings of the selected port.

8.2.2 Voice OUI

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





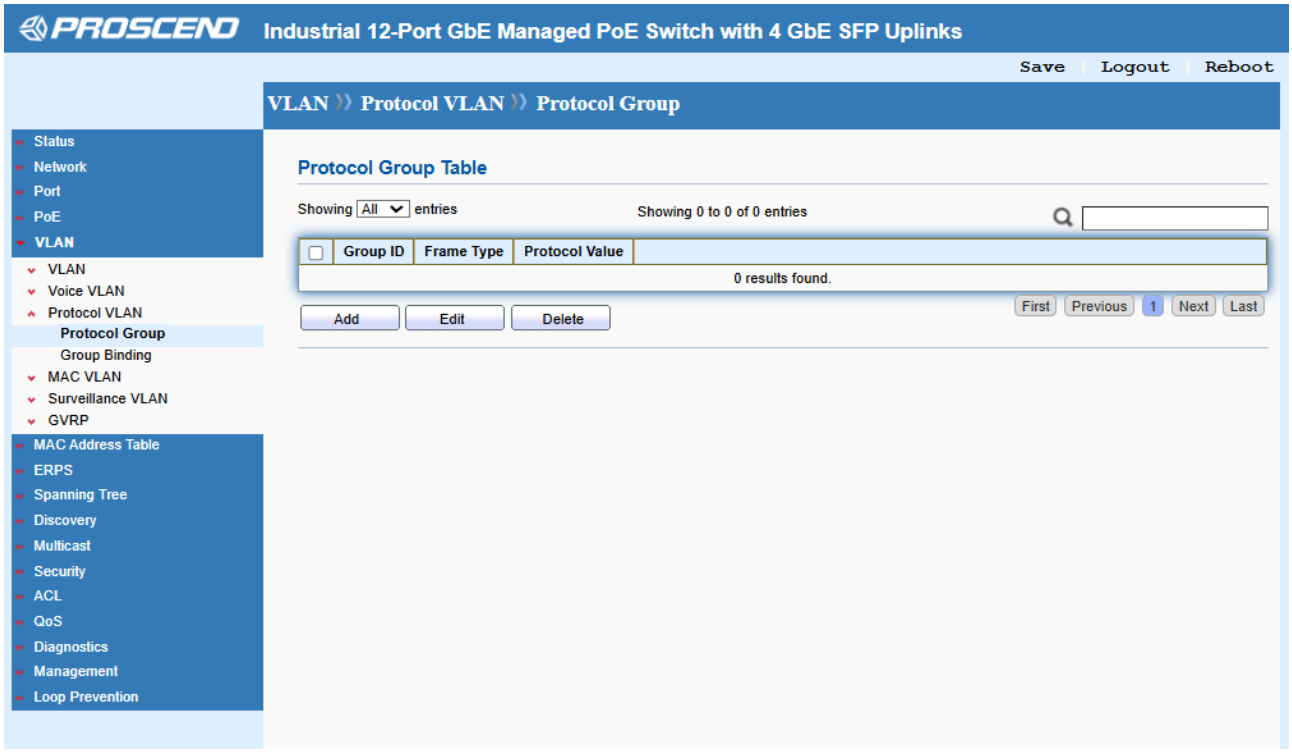
Item	Description
Add	Add a new OUI entry.
Edit	Edit the existing OUI entry.
Delete	Delete the existing OUI entry.
OUI	Type OUI address.
Description	Enter a description of the specified MAC address to the voice VLAN OUI table.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

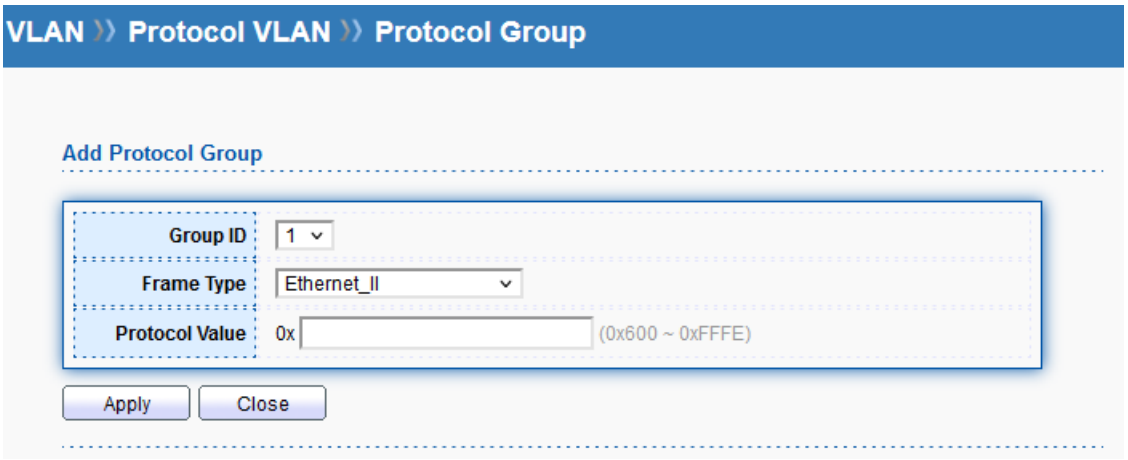
8.3 Protocol VLAN

The Switch offers protocol VLANs which allows Network Administrator to filter out untagged traffic of certain protocol and then assign them a specific VLAN ID.

8.3.1 Protocol Group

Up to eight protocol groups can be defined, each of them can have a unique filtering criteria such as frame type and protocol value.

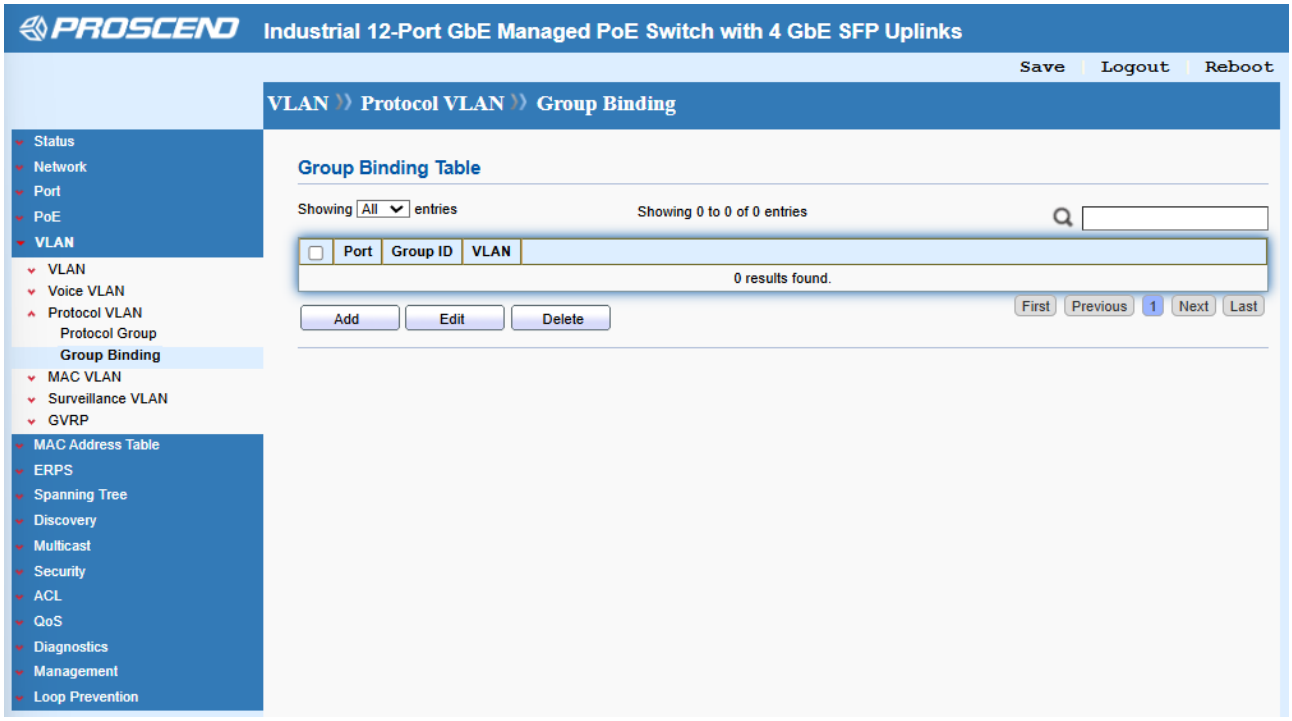


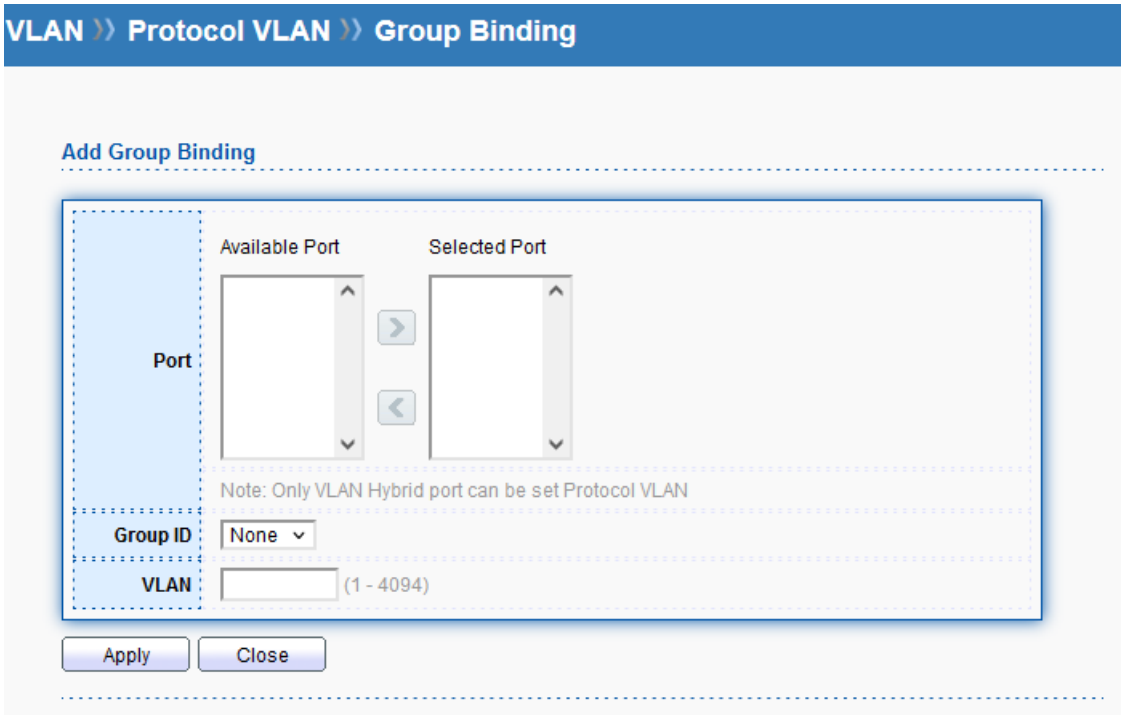


Item	Description
Add	Add a new Protocol VLAN entry.
Edit	Edit the existing Protocol VLAN entry.
Delete	Delete the existing Protocol VLAN entry.
Group ID	It is a number for identification while bounding with VLAN/Port.
Frame Type	Use the drop-down list to specify the frame type which you would like to filter. **Ethernet_II**: Packet will be mapped based on Ethernet version 2. **IEEE802.3_LLC_Other**: Packet will be mapped based on 802.3 packet with LLC other header. **RFC_1042**: Packet will be mapped based on RFC 1042.
Protocol Value	Input a value (ranging from 0x600 ~0xFFFE). Packets match with such value will be classified into this group.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

8.3.2 Group Binding

This page is for setting up the ports and protocol group that we would like to filter, and the VLAN ID we would like to assign.





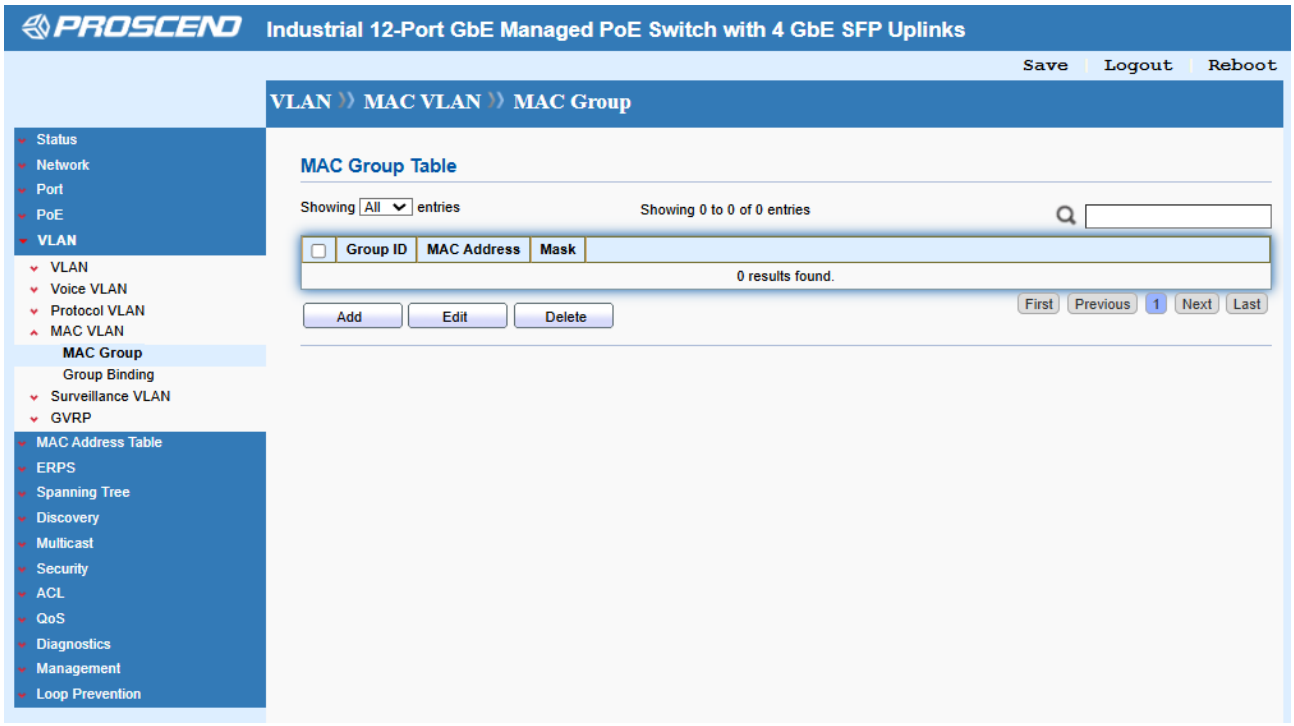
Item	Description
Add	Add a new entry.
Edit	Edit the VLAN number of existing entry.
Delete	Delete the existing entry.
Port	Select one or more ports for applying protocol-based VLAN. Note that protocol-based VLAN can only be applied to the ports of which Interface VLAN Mode is set to “Hybrid”.
Group ID	Select the protocol group defined in Protocol Group setup.
VLAN	Enter the VLAN number.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

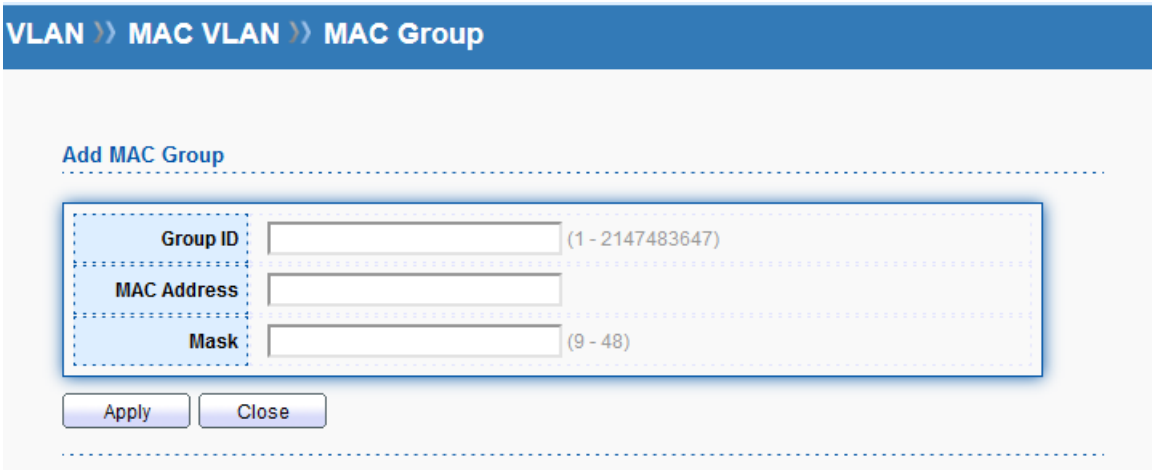
8.4 MAC VLAN

The MAC VLAN allows you to statically assign a VLAN ID to a host with specific MAC address(es). The Switch allows you configure multiple groups with configured MAC address and mask to be active on ports and to be bound with VLAN ID.

8.4.1 MAC Group

This page allows to define groups with specific MAC addresses for later binding with VLAN and Port.

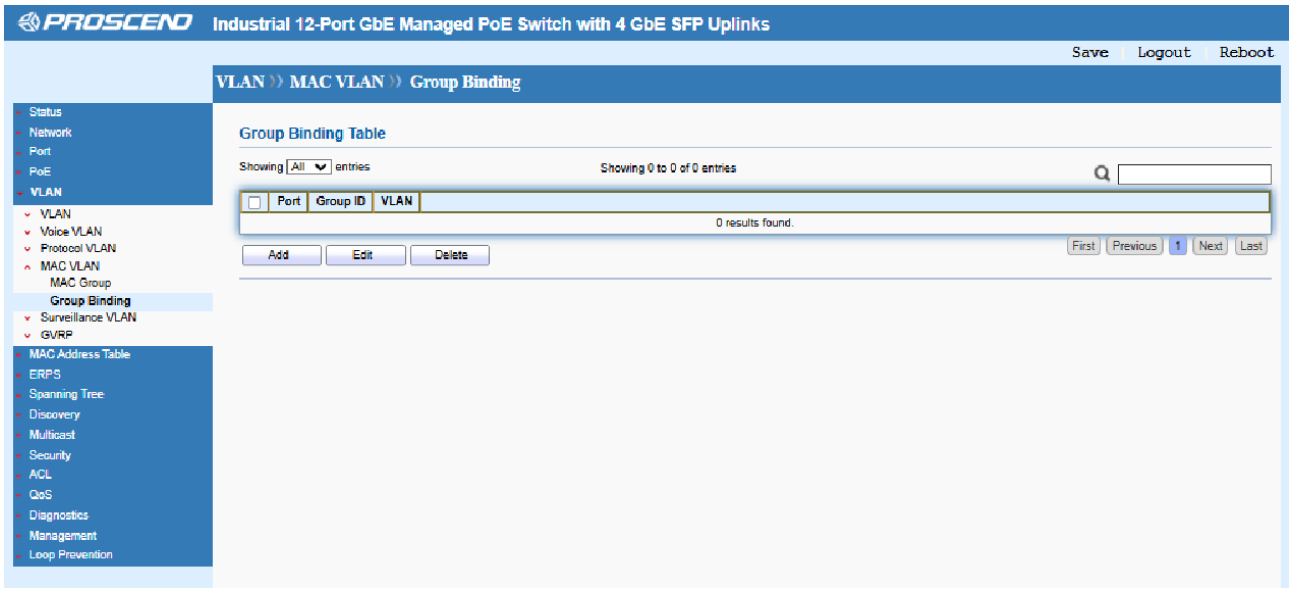


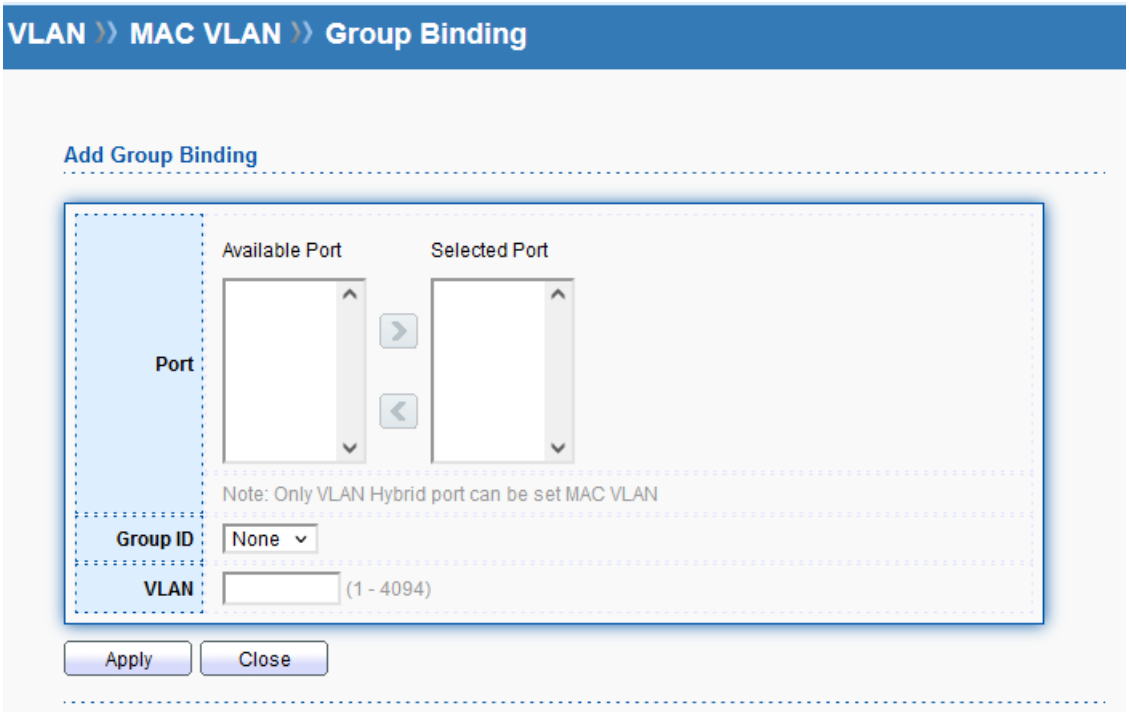


Item	Description
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the existing entry.
Group ID	It is a number for identification later, while chosen to be bound with VLAN/Port.
MAC Address	Enter the MAC address you wish to be classified in this group.
Mask	The mask is the length of matching prefix you wish to have on MAC address. For example, configure mask in 10. It means a host with beginning of the 10-digit of MAC address will be checked, and classified into this group if matched.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

8.4.2 Group Binding

This page allows to bind the group of specified MAC addresses with VLAN and Port.





Item	Description
Add	Add a new entry.
Edit	Edit the existing entry.

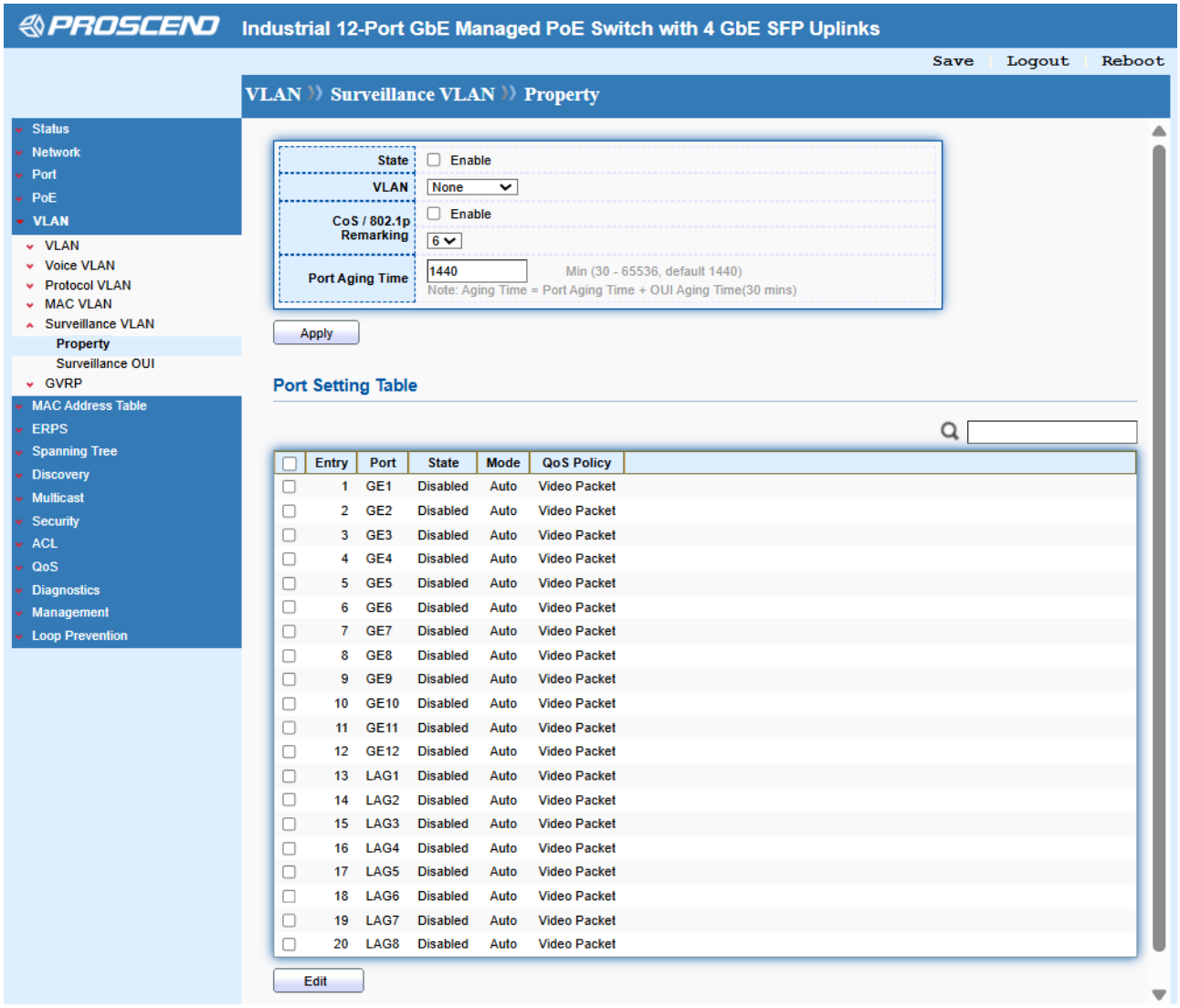
Delete	Delete the existing entry.
Port	Select the ports you wish to be bound with specified MAC address group.
Group ID	Choose the group ID you have created in section MAC VLAN ➔ MAC Group.
VLAN	Enter the VLAN ID that you wish to be bound with.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

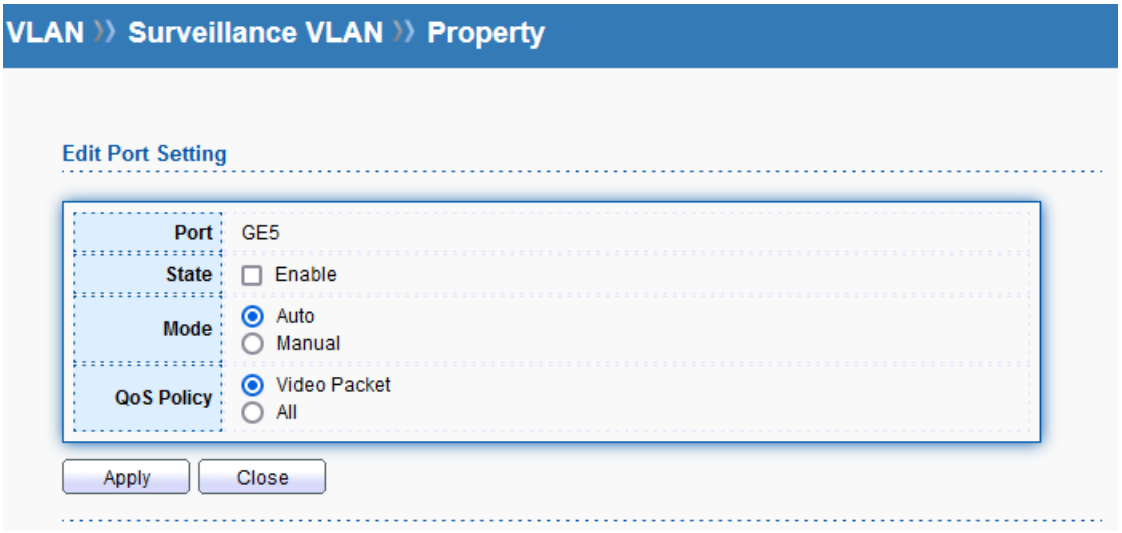
8.5 Surveillance VLAN

Surveillance VLAN can be configured for the Switch to identify the packets coming from an IP camera automatically and assign those traffics to a specific VLAN ID and CoS/802.1p value, this helps you to prioritize those traffics and improve video quality.

8.5.1 Property

This page is for setting up the VLAN to which the video traffic should be assigned and to enable/disable Surveillance VLAN on each port.



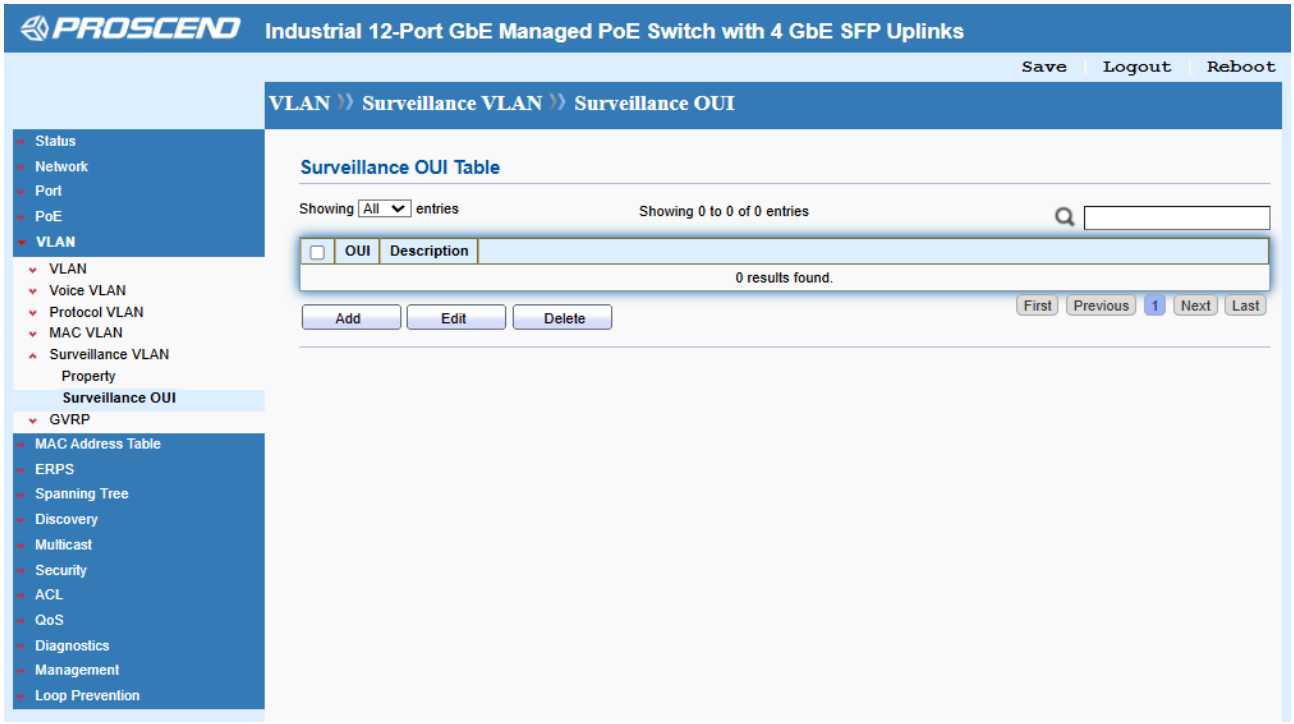


Item	Description
State	Enable or disable the port settings for this function.
VLAN	Choose a VLAN profile (created in VLAN ➔ Create VLAN) as Surveillance VLAN.
CoS / 802.1p Remarking	Specify the CoS/802.1p number you wish ingress packets be tagged with, so that QoS can prioritize it correctly. If enabled, the qualified packets will be remarked by this value.
Port Aging Time	Default is 1440. VLAN entry will be aged out after this time if no packet passes through.
Apply	Apply the settings to the switch.
Edit	Edit the existing entry.
Port	The index number of selected port.
State	Enable or disable surveillance VLAN function of the port.
Mode	Select surveillance VLAN mode of the port. **Auto**: Surveillance VLAN auto detect packets that match OUI table and add received port into surveillance VLAN ID tagged member. **Manual**: User need add interface to VLAN ID tagged member manually.
QoS Policy	Select QoS Policy mode of the port. **Video Packet**: QoS attributes are applied to packets with OUI in the source MAC address. **All**: QoS attributes are applied to packets that are classified to the Surveillance VLAN.

Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

8.5.2 Surveillance OUI

Filtering Surveillance traffic is based on the OUI of the IP cameras. Users can add, edit, and delete OUI on this page.

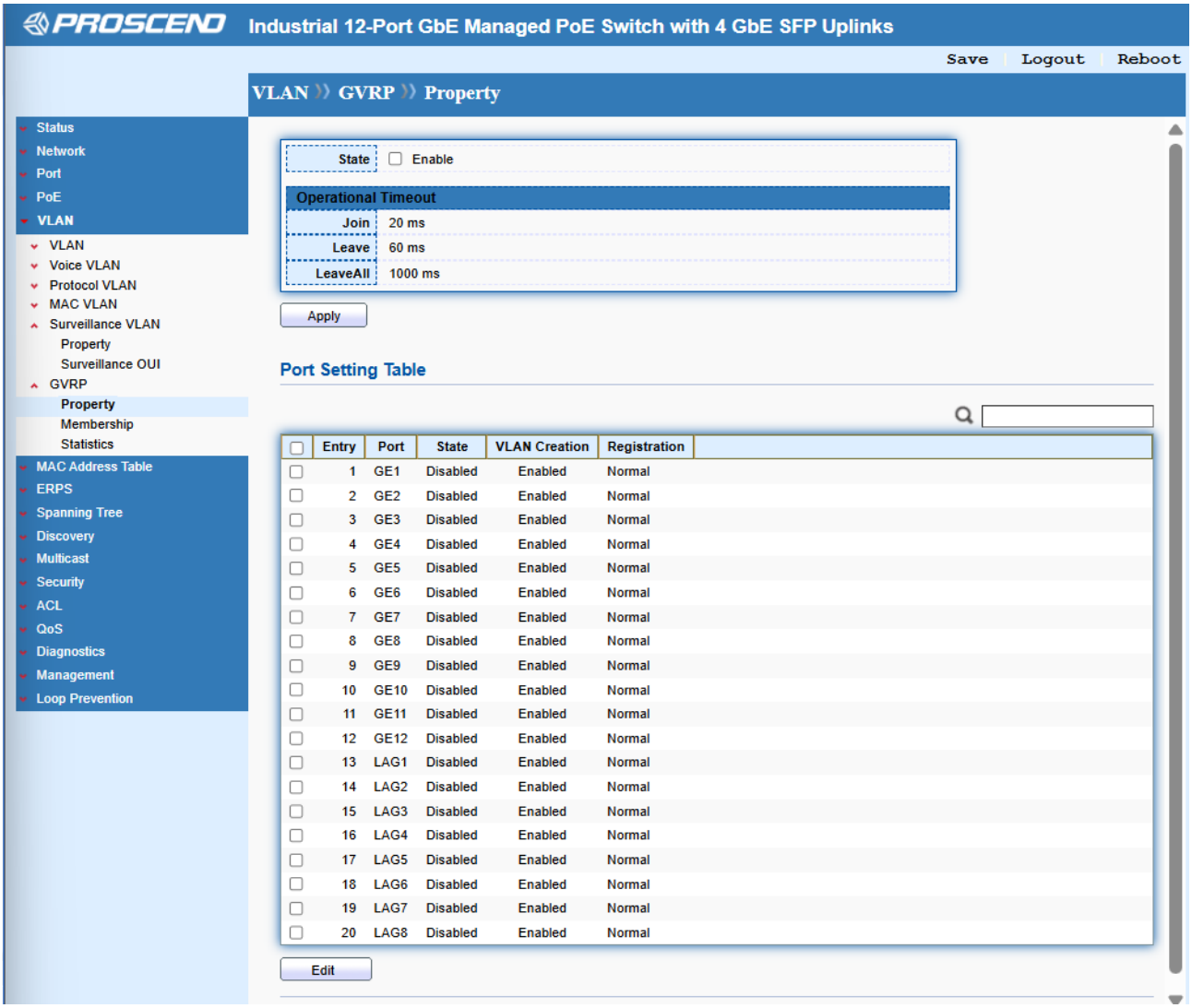


Item	Description
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the existing entry.
OUI	Enter OUI MAC address of monitored IP camera. It can't be edited in edit dialog.
Description	Enter a description of the specified MAC address to the surveillance VLAN OUI table.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

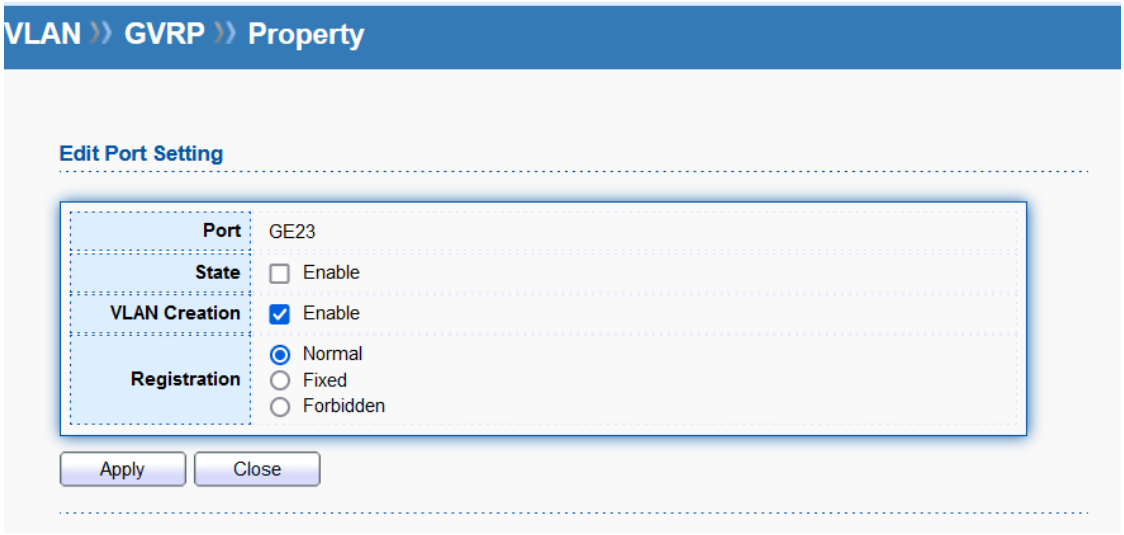
8.6 GVRP

8.6.1 Property

This page allows to enable or disable the GVRP function.



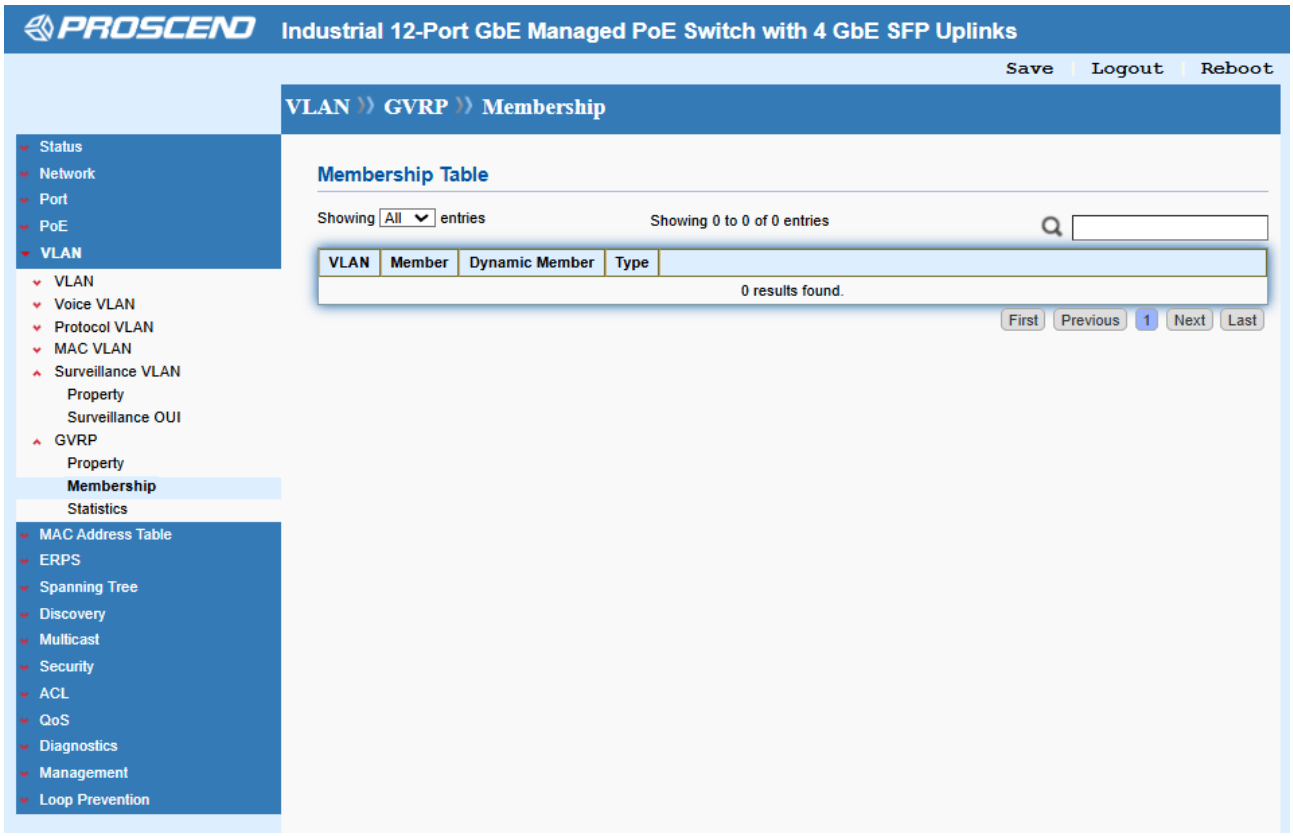
Item	Description
State	Enable or disable the GVRP setting for such VLAN.
Operational Timeout	Display the current time status for GVRP.
Apply	Apply the settings to the switch.
Edit	Edit the existing entry.



Item	Description
Port	The index number of selected port.
State	Enable or disable the port settings for such VLAN.
VLAN Creation	Select Enable or disable.
Registration	**Normal**: Default setting. All packets can pass through the selected port. **Fixed**: The selected port only sends static VLAN information to neighboring device and allows static VLAN packet to pass through. **Forbidden**: The selected port only allows default VLAN packet to pass through.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

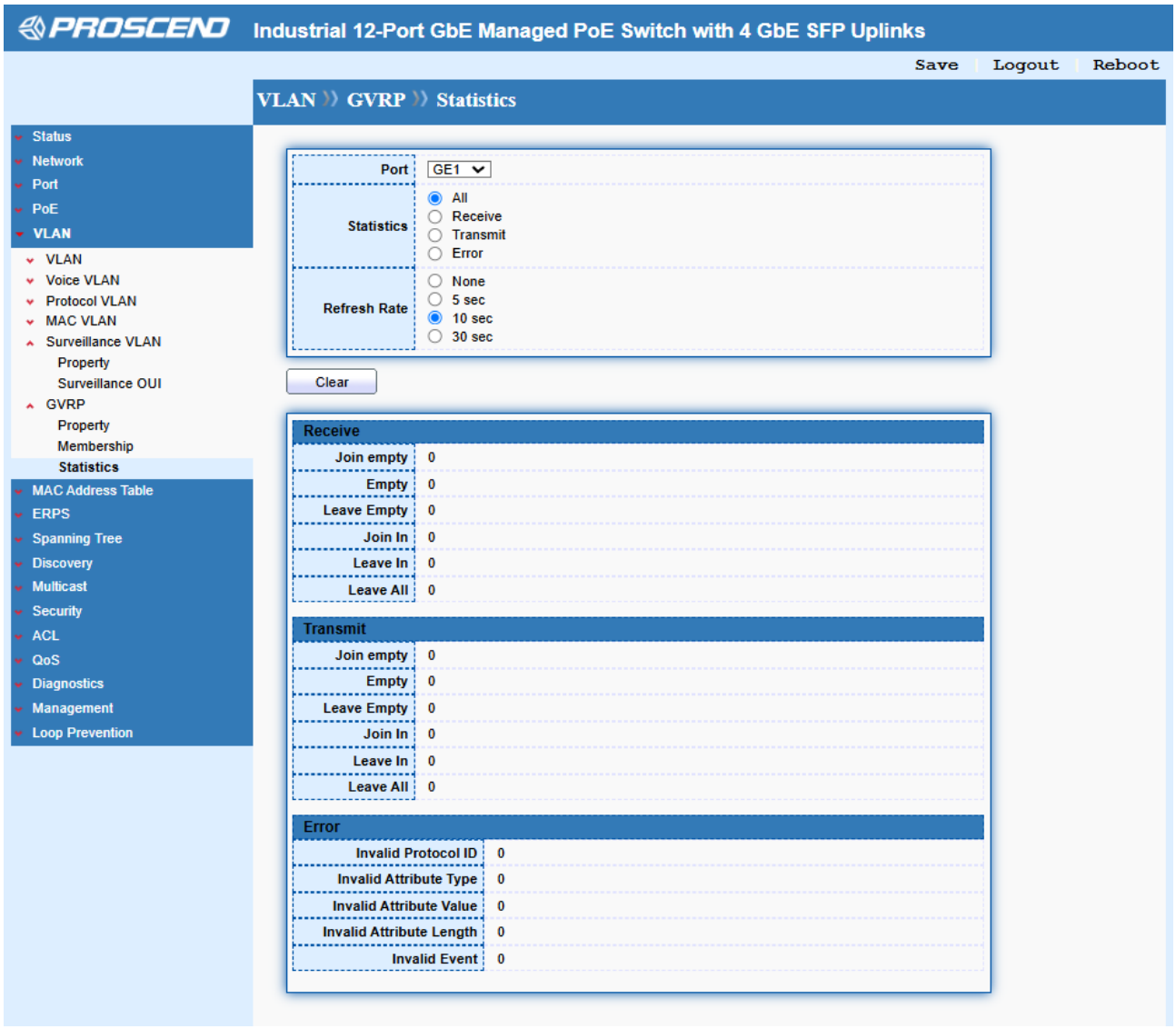
8.6.2 Membership

This page displays information about membership of GVRP.



8.6.3 Statistics

This page displays detailed statistics of each port.

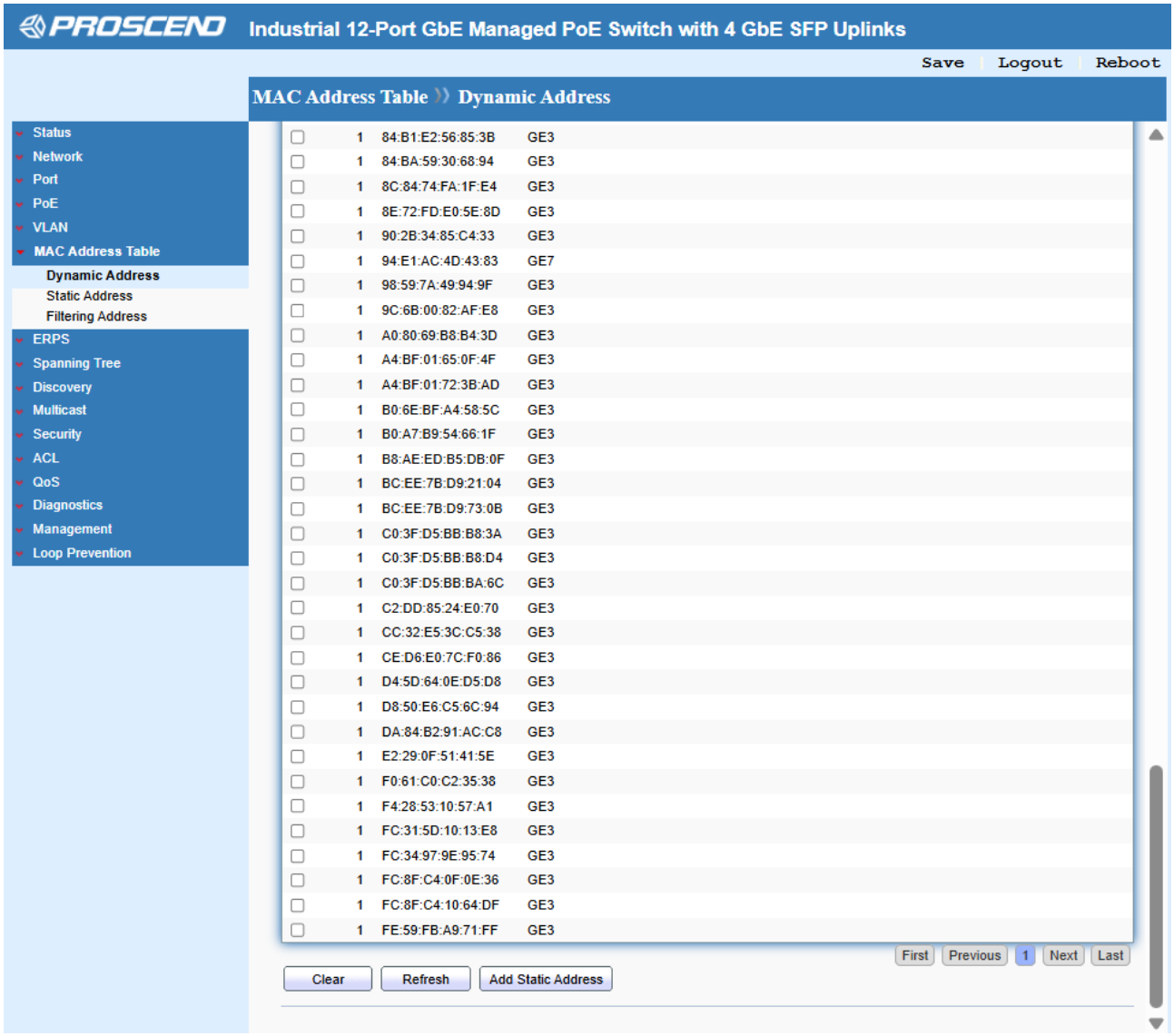


9 MAC Address Table

This section allows user to view the dynamic MAC address entries in the MAC table, change related setting and assign MAC address into MAC table.

9.1 Dynamic Address

This page allows to configure aging time for dynamic MAC address.

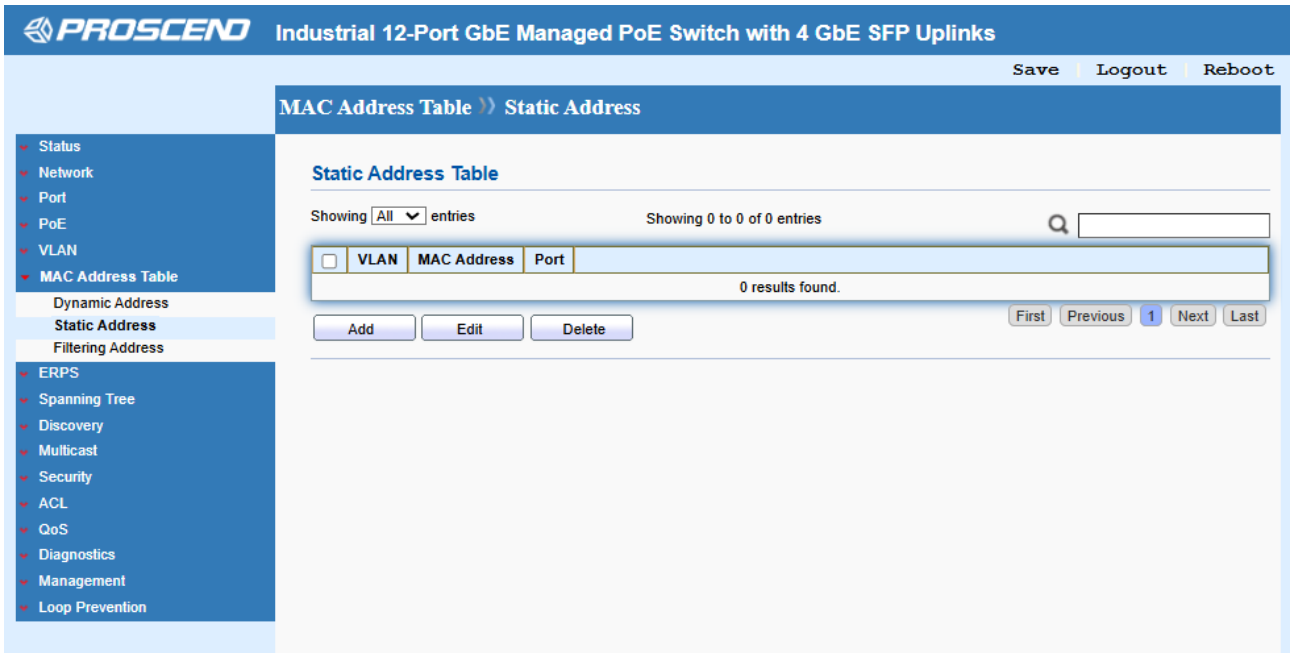


Item	Description
Apply	Apply the settings to the switch.
Aging Time	Enter the aging out value for the dynamic MAC address.

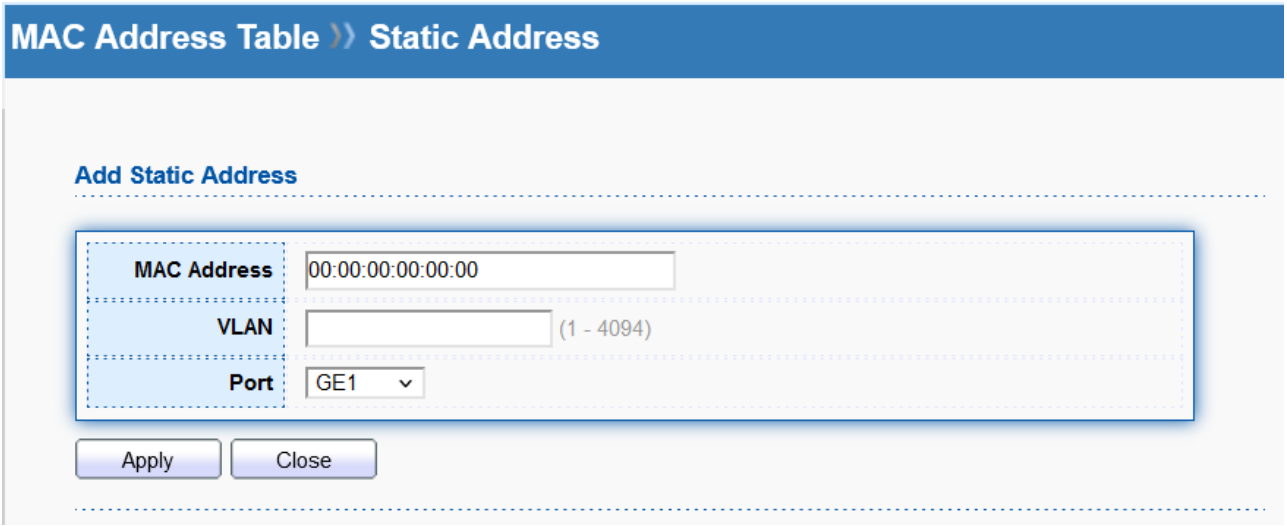
Clear	Clear the entry that is still not out of aging time.
Refresh	Refresh the Dynamic address table.
Add Static Address	Add selected dynamic MAC address into the static MAC address table.

9.2 Static Address

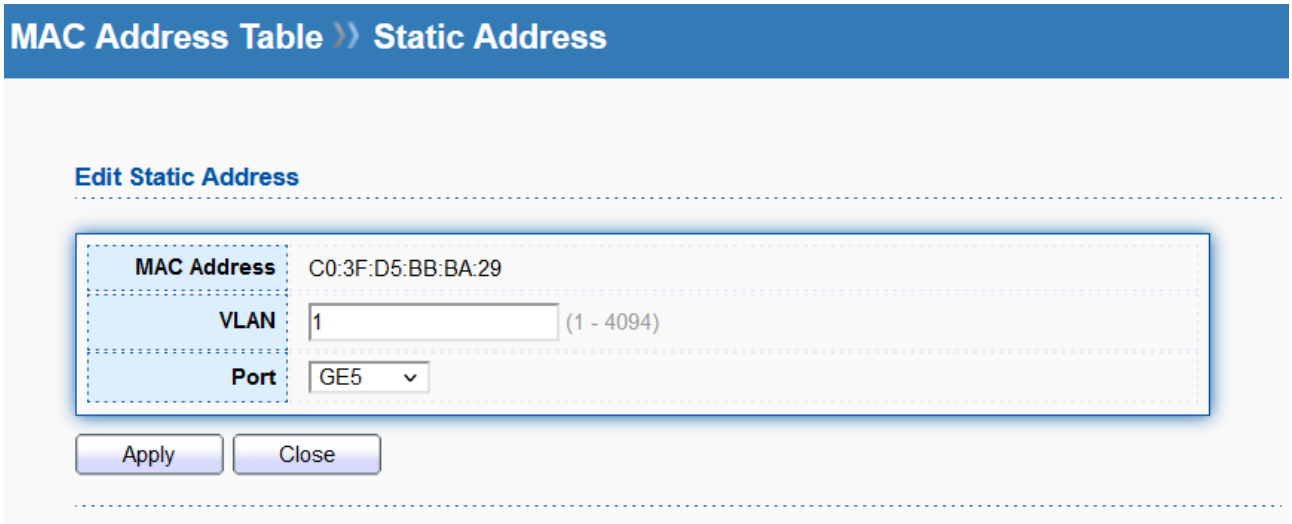
This page allows user to manually assign MAC address into MAC table.



Item	Description
Add	Add a new MAC address into MAC address table.
Edit	Edit existing entry of MAC address.
Delete	Delete selected entry of MAC address.



Item	Description
MAC Address	Enter the MAC address that will be forwarded.
VLAN	This is the VLAN group to which the MAC address belongs.
Port	Select the port where received frame of matched destination MAC address will be forwarded to.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

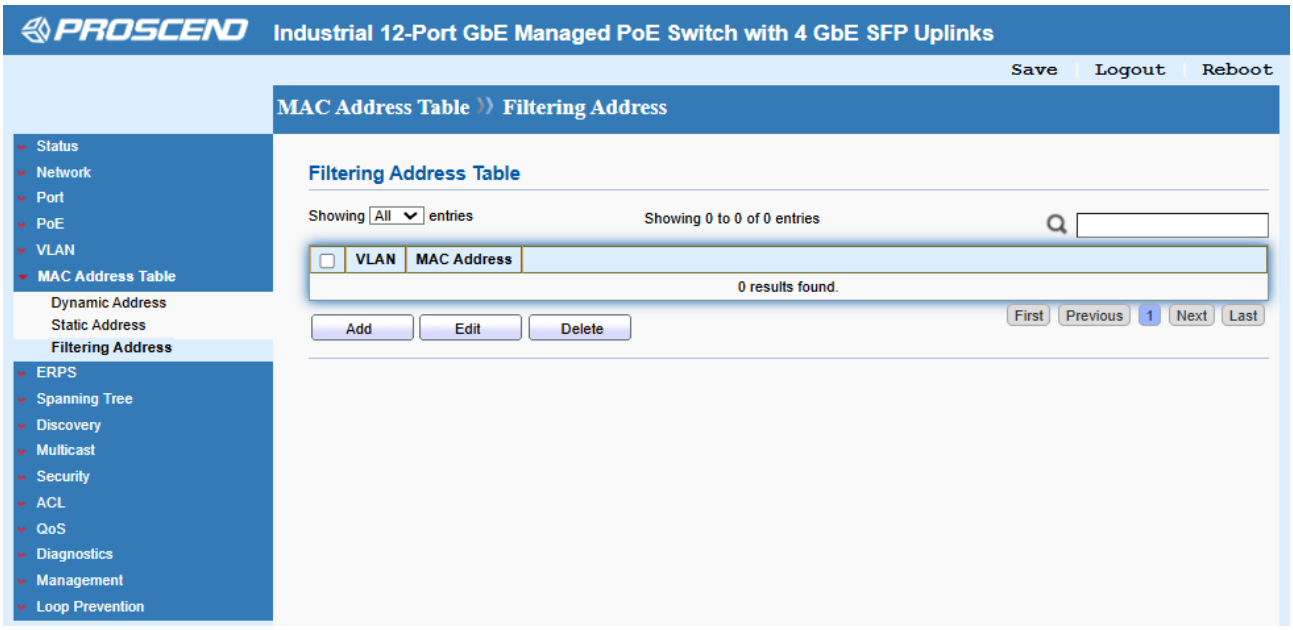


Item	Description
MAC Address	The MAC address that will be forwarded.
VLAN	This is the VLAN group to which the MAC address belongs.
Port	Select the port where received frame of matched destination MAC address will be forwarded to.

Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

9.3 Filtering Address

Filtering addresses are manually added and determine the packets with specific source or destination MAC addresses that will should dropped by the switch.

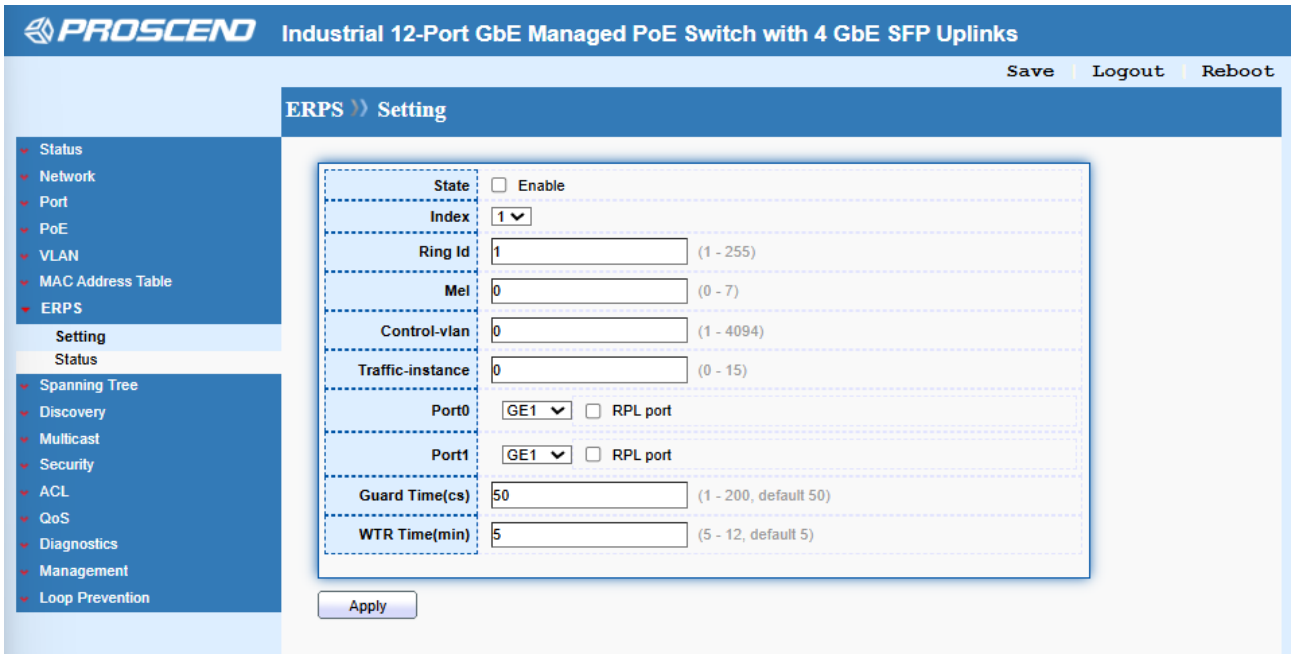


Item	Description
Add	Add a new MAC address into MAC address table.
Edit	Edit existing entry of MAC address.
Delete	Delete selected entry of MAC address.

10 ERPS

Ethernet Ring Protection Switching (ERPS) is a Layer 2 ring protection protocol defined by ITU-T G.8032. It is designed to provide high network availability and fast recovery in Ethernet ring topologies commonly used in industrial automation, power utilities, transportation, and surveillance networks.

10.1 Setting

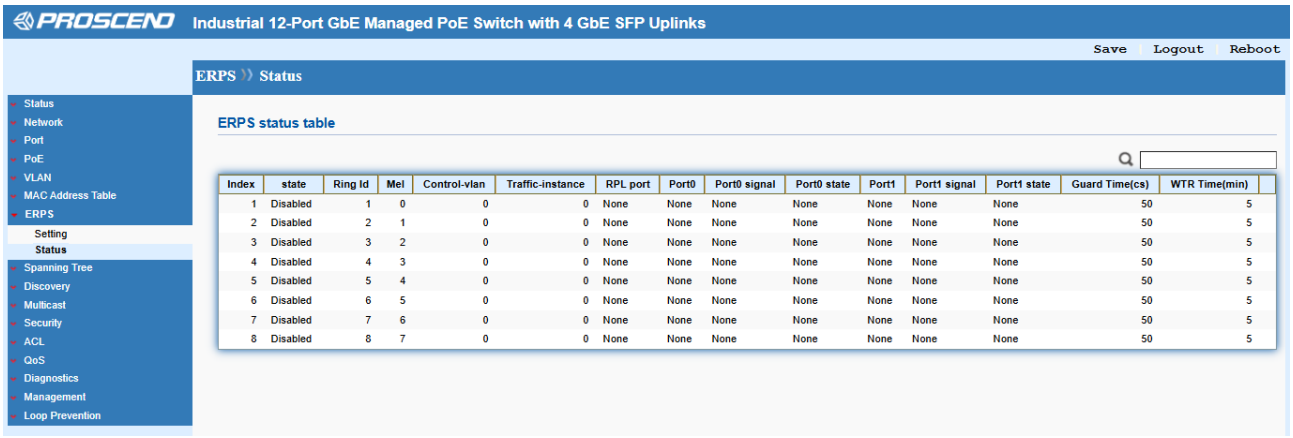


Item	Description
State	Enable / Disable
Index	ERP table index value
Ring Id	Unique identifier for an ERPS ring. All switches in the same ring must use the same Ring ID.
Mel	It specifies the **maintenance level of OAM** (Operations, Administration, and Maintenance) messages within an Ethernet network.
Control-vlan	VLAN used to transmit R-APS (Ring Automatic Protection Switching) control messages. It should be dedicated and consistent across all ring members.
Traffic-instance	A logical forwarding instance that associates one or more VLANs with a specific ERPS ring.

Port0	The two Ethernet ports that form the ERPS ring connection.
Port1	**RPL port** designated to block or unblock the RPL in an ERPS ring network.
Guard Times(cs)	Prevents unnecessary topology changes caused by delayed or duplicated control messages.
WTR Time(min)	Delay before reverting traffic back to the original RPL after a failure is repaired, preventing frequent switching.

10.2 Status

Check the ERPS configuration.



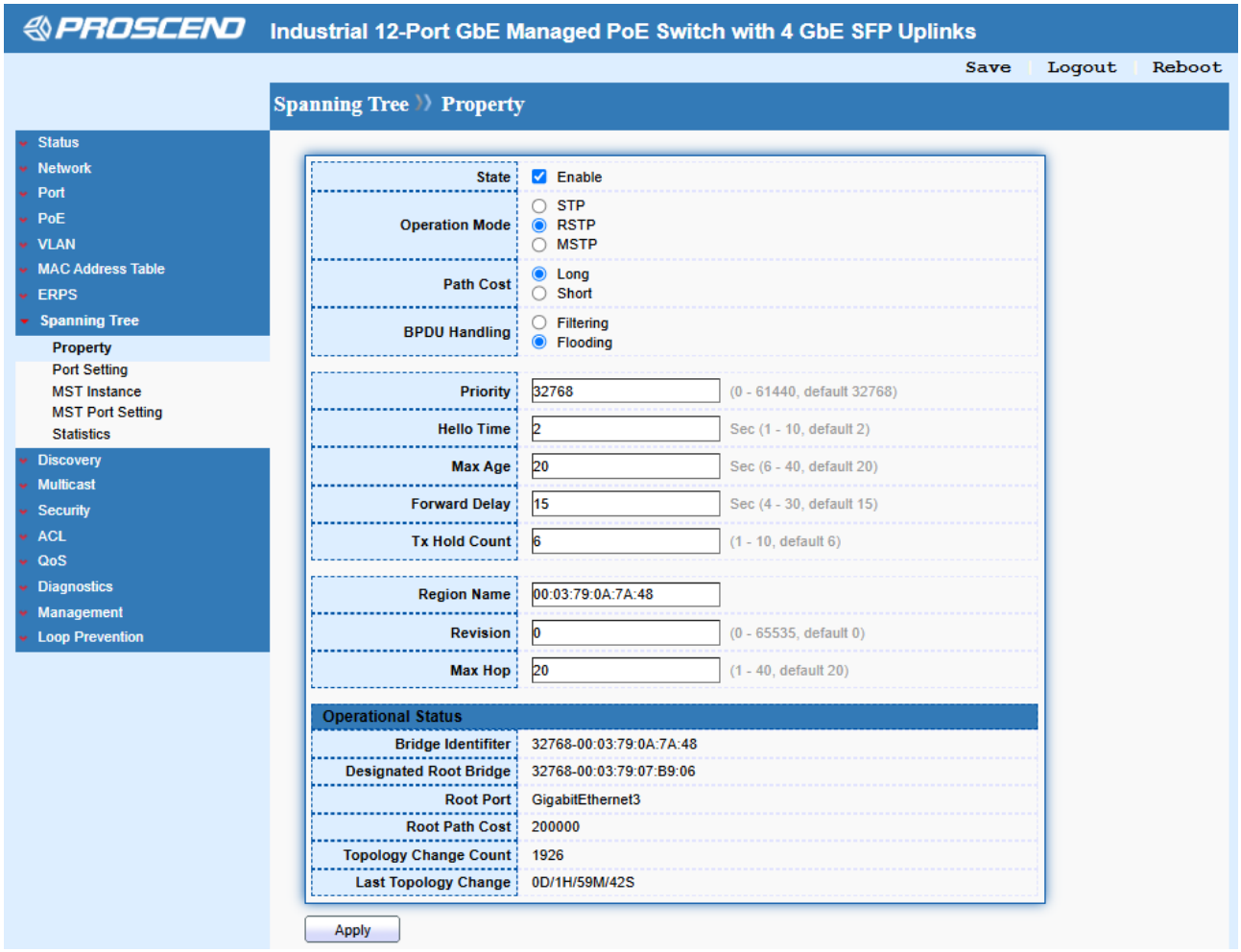
Index	state	Ring Id	Mel	Control-vlan	Traffic-instance	RPL port	Port0	Port0 signal	Port0 state	Port1	Port1 signal	Port1 state	Guard Time(cs)	WTR Time(min)
1	Disabled	1	0	0	0	None	None	None	None	None	None	None	50	5
2	Disabled	2	1	0	0	None	None	None	None	None	None	None	50	5
3	Disabled	3	2	0	0	None	None	None	None	None	None	None	50	5
4	Disabled	4	3	0	0	None	None	None	None	None	None	None	50	5
5	Disabled	5	4	0	0	None	None	None	None	None	None	None	50	5
6	Disabled	6	5	0	0	None	None	None	None	None	None	None	50	5
7	Disabled	7	6	0	0	None	None	None	None	None	None	None	50	5
8	Disabled	8	7	0	0	None	None	None	None	None	None	None	50	5

11 Spanning Tree

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

11.1 Property

This page allows to configure and display Spanning Tree Protocol (STP) property configuration.

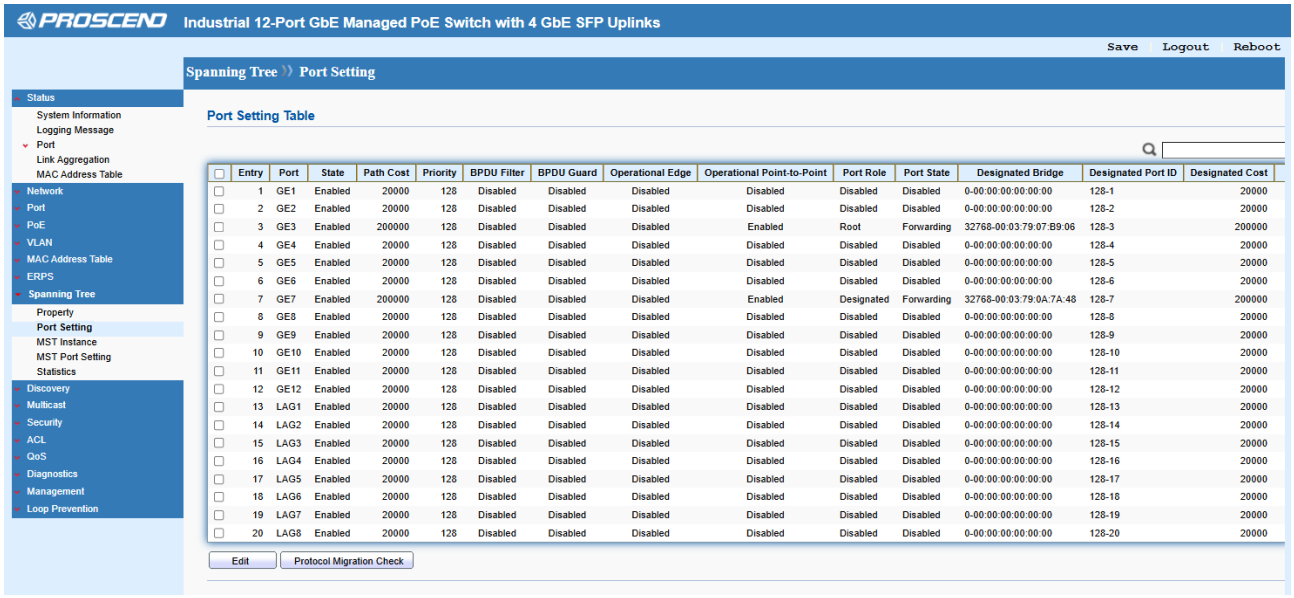


Item	Description
State	Enable or disable the STP operation.
Operation Mode	**STP**: Enable the Spanning Tree (STP) operation. **RSTP**: Enable the Rapid Spanning Tree (RSTP) operation. Default is RSTP. **MSTP**: Enable the Multiple Spanning Tree Protocol (MSTP)

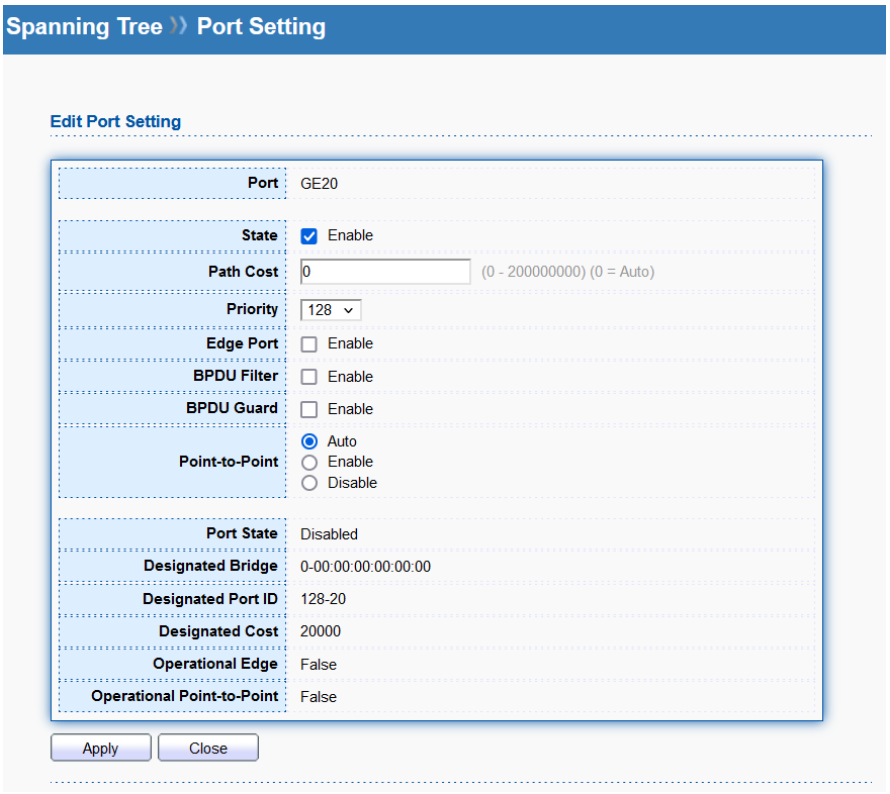
Path Cost	Specify the path cost method. **Long**: Specifies that the default port path costs are within the range: 1~200,000,000. **Short**: Specifies that the default port path costs are within the range: 1~65,535.
BPDU Handling	Specify the BPDU forward method when the STP is disabled. **Filtering**: Filter the BPDU when STP is disabled. **Flooding**: Flood the BPDU when STP is disabled.
Priority	Specify a priority value for the switch. The smaller the priority value, the higher the priority and greater chance of becoming the root.
Hello Time	Specify the STP hello time in second to broadcast its hello message to other bridge 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 30 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 default region name of the device is its MAC address.
Revision	Enter the revision number.
Max Hop	Set the number of hops for BPDI packets to be forwarded in the MSTP region.
Operational Status	Display the current STP operational status.
Apply	Apply the settings to the switch.

11.2 Port Setting

This page allows to configure and display Spanning Tree Protocol (STP) port settings.



Item	Description
Edit	Edit the selected port settings.
Protocol Migration Check	Run protocol migration check on selected port.

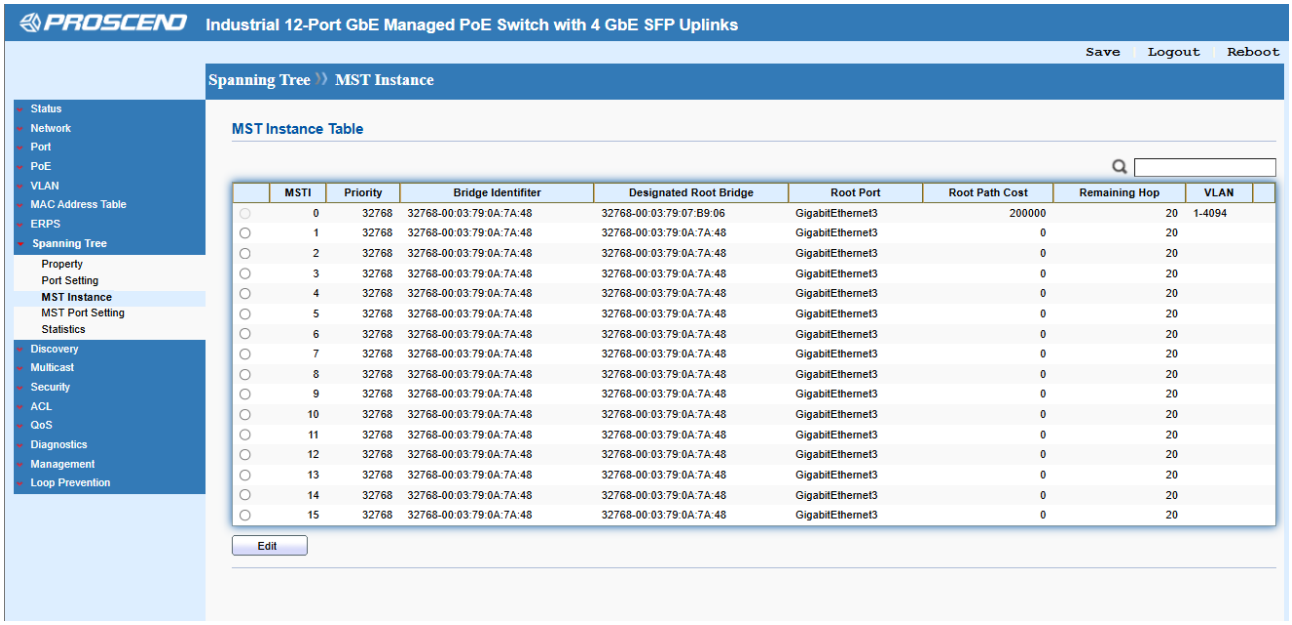


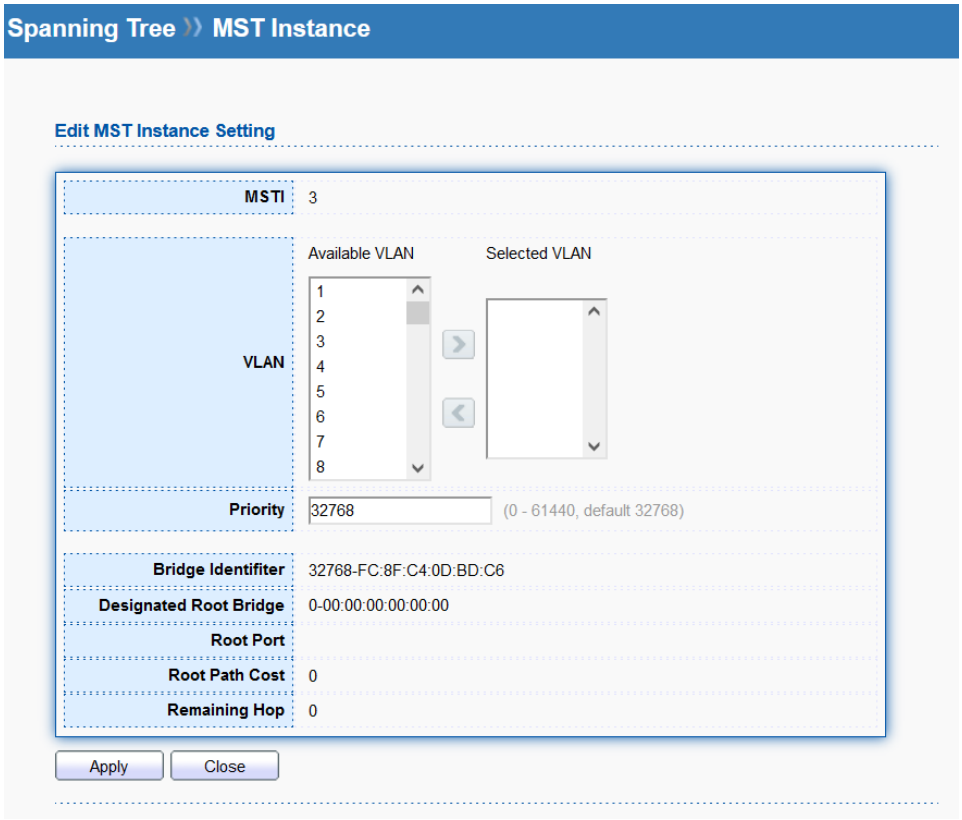
Item	Description
Port	The index number of selected port.
State	Enable or disable the port settings.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost. Entering 0 means the switch will automatically assign a value.
Priority	Specify a priority value for the switch. The smaller the priority value, the higher the priority and greater chance of becoming the root.
Edge Port	Enable or disable 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 before the STP state change.
BPDU Filter	Checked means drop all BPDU packets and no BPDU will be sent.
BPDU Guard	When it is checked that BPDU Guard further protects your switch by turning this port into error state and shutdown if any BPDU received from this port.

Point-to-Point	**Auto**: Switch determines the STP of link type for this port automatically. **Enable**: It means the STP of link type on this port is full-duplex and directly connect to another switch or host. **Disable**: It means the STP of link type on this port is “not” full-duplex and “does not” directly connect to another switch or host.
Port State	Display current port status.
Designated Bridge	Display designated bridge information.
Designated Port ID	Display designated port ID information.
Designated Cost	Display designated cost information.
Operational Edge	Display current state of edge port.
Operational Point-to-Point	Display current state of Point-to-Point.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

11.3 MST Instance

MSTP allows traffic of different VLAN to be mapped into different MST Instances, the switch supports up to 16 independent MST instances (0~15) with which the VLAN can be associated.

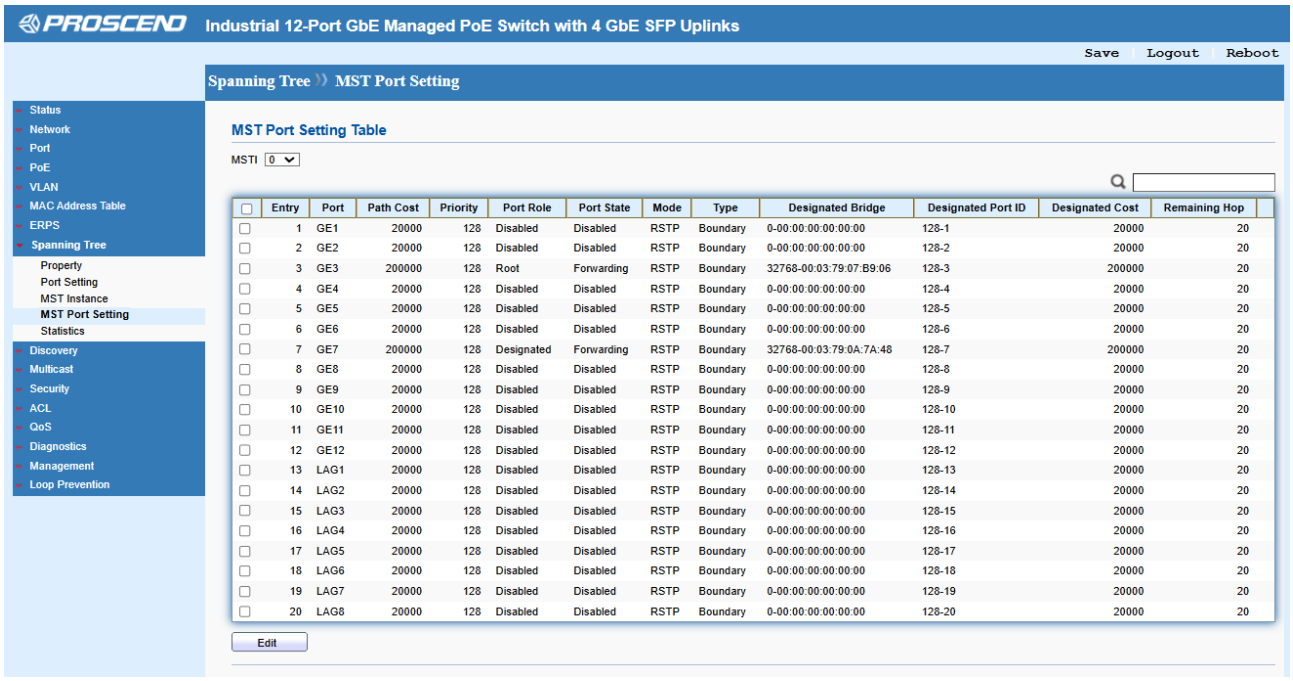


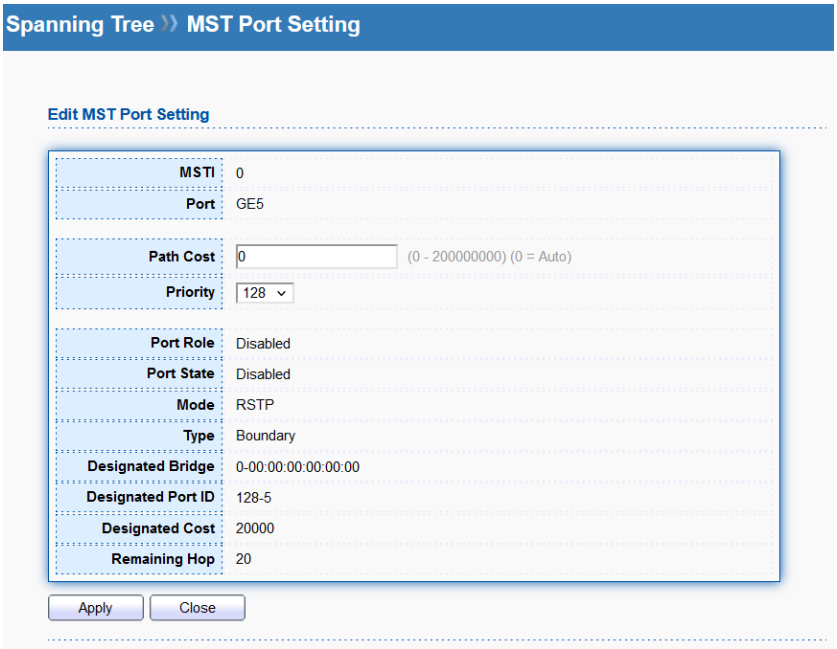


Item	Description
Edit	Edit the settings of selected instance.
MSTI	The index number of selected MST instance.
VLAN	Enter the ID of the VLAN which should be associated with this MSTI.
Priority	The switch priority for this MST instance. A lower number gives the switch higher chance to be chosen as the root bridge.
Bridge Identifier	Display the priority of MSTI instance number + MAC address of the switch.
Designated Root Bridge	Display the Bridge Identifier of the root bridge.
Root Port	Display the port toward the root.
Root Path Cost	Display the path cost toward the root.
Remaining Hop	Display the remaining hop count in BPDU.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

11.4 MST Port Setting

MST Port Settings is used to configure the GE port / LAG group settings for each MST instance. The table displays the MST parameters for each port.



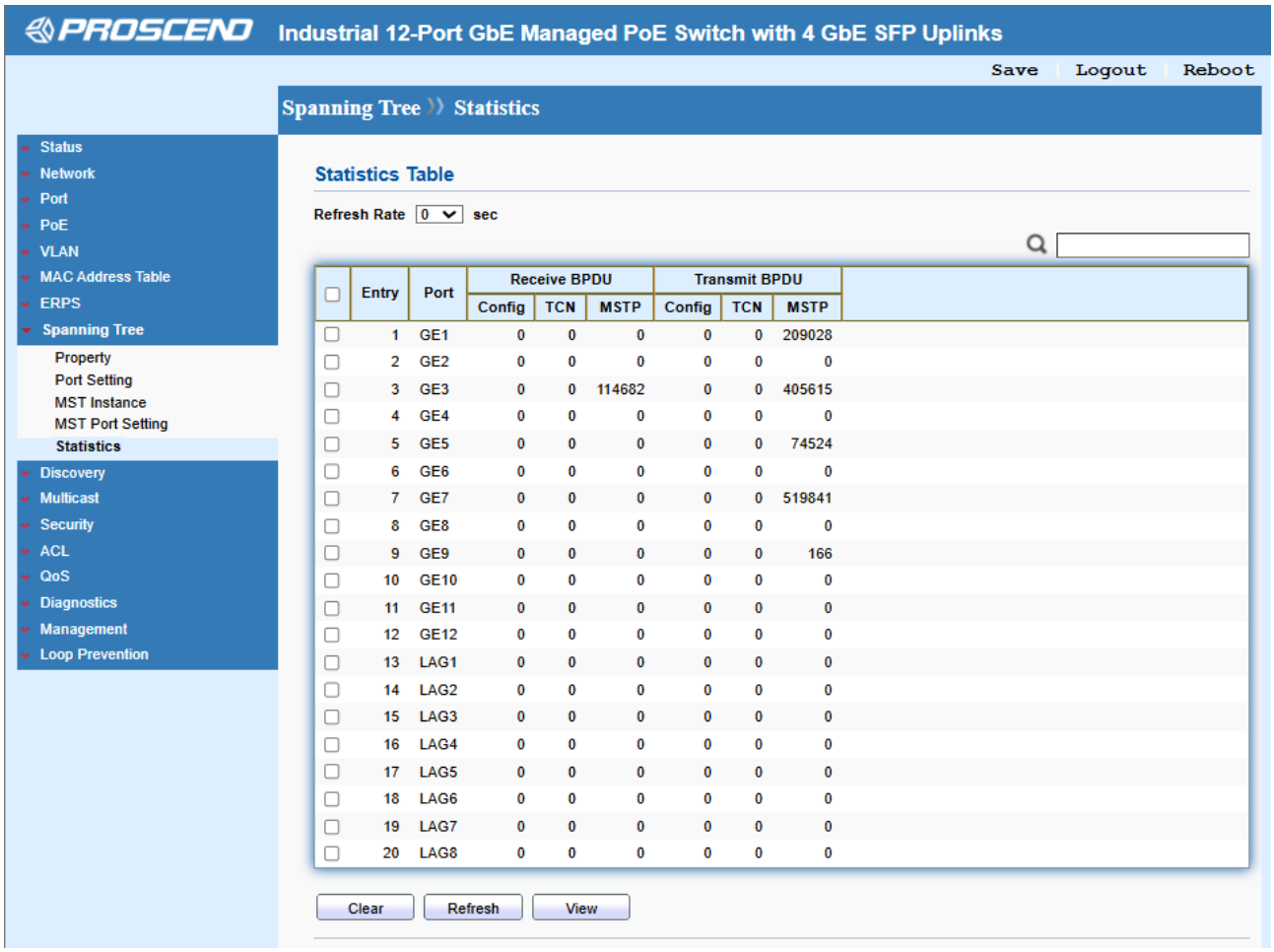


Item	Description
MSTI	Select one of the MST instances.
Edit	Edit the settings of selected port.

MSTI	Display the selected MST instance.
Port	Display the selected port number.
Path Cost	Set path cost value for the port. A port with lowest value will be used as the forwarding port by spanning tree. Default value was set according to the bandwidth of the port.
Priority	Among the ports with same path cost, port with lower priority will have higher chance to be used as the forwarding port by spanning tree. Use the drop down list to choose desired priority value.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

11.5 Statistics

This page displays the statistics of BPDU on each port.



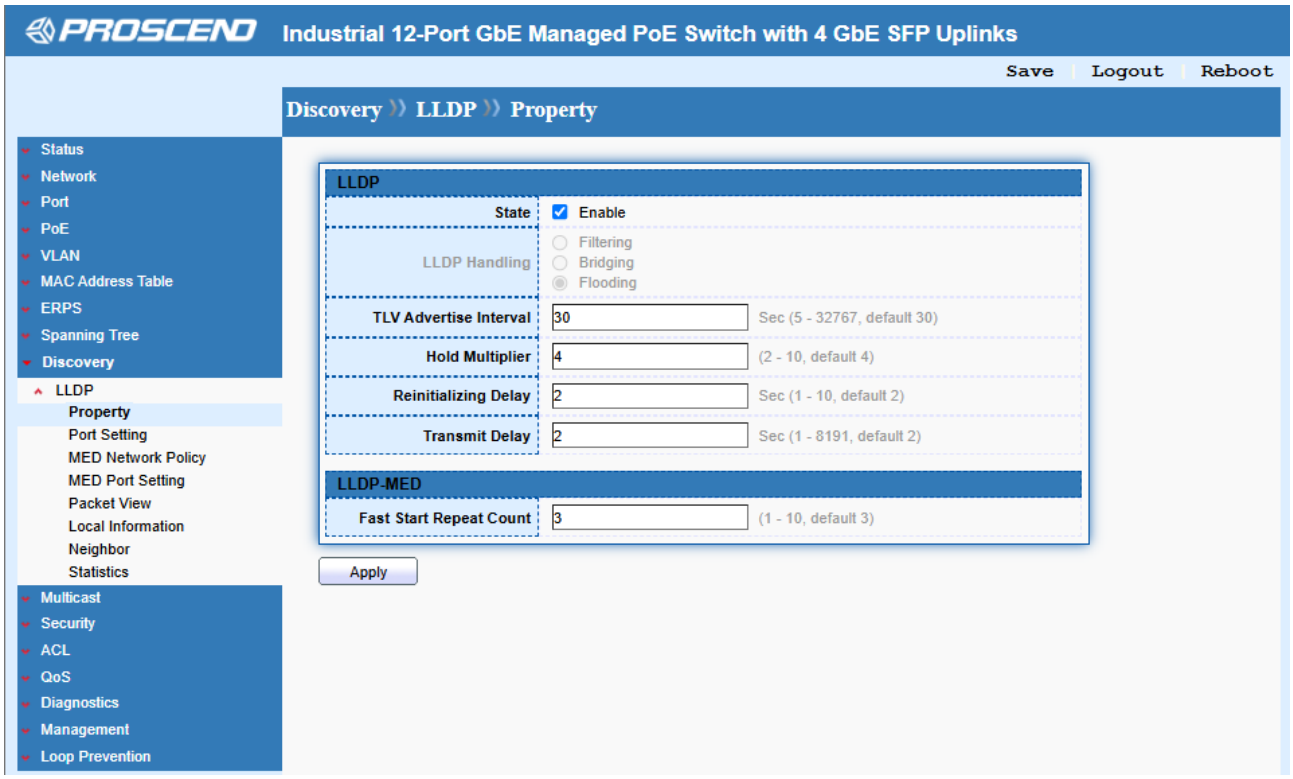
12 Discovery

12.1 LLDP

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

12.1.1 Property

This page allows to configure general settings of LLDP.

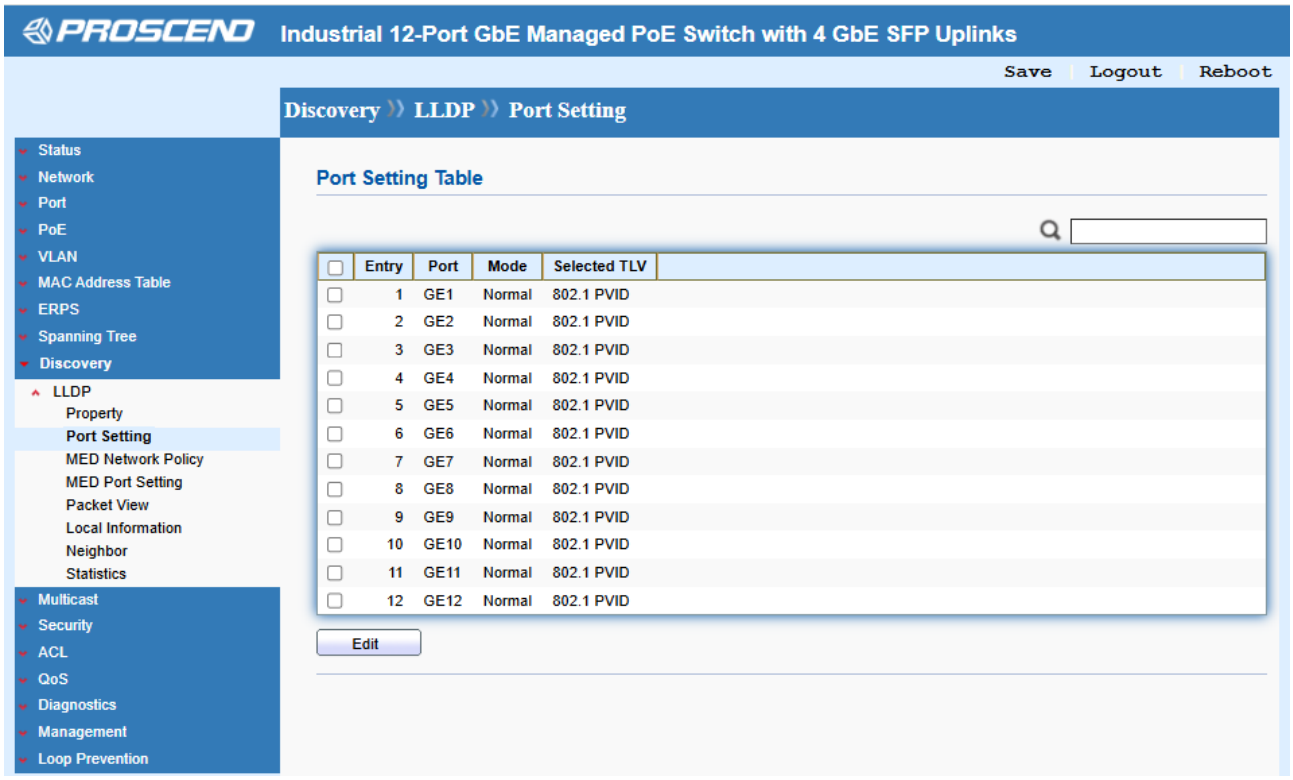


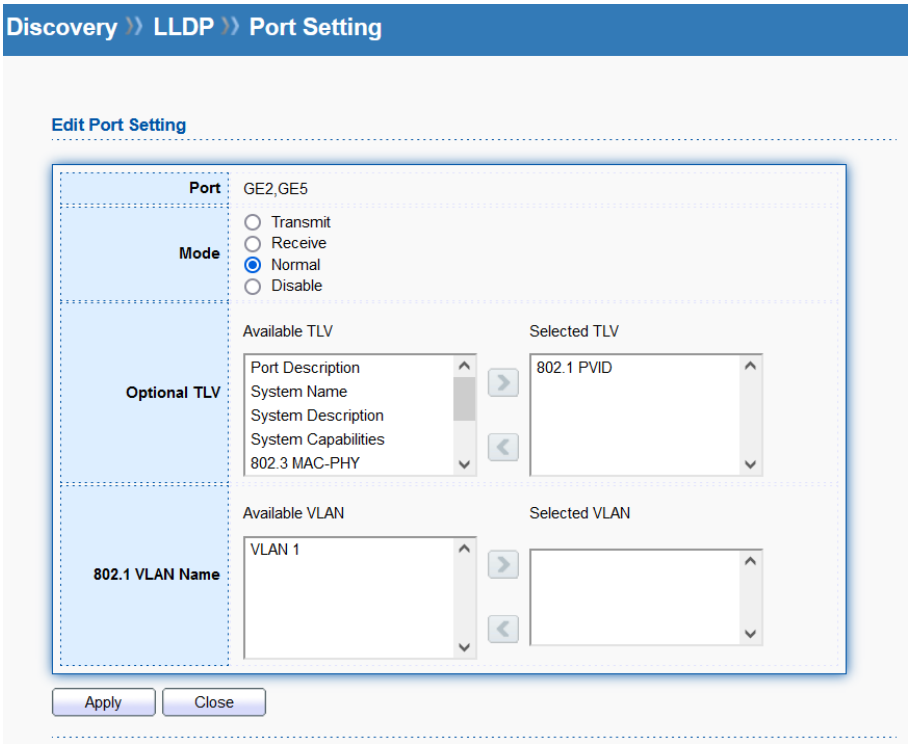
Item	Description
State	Enable or disable the LLDP protocol on this switch. Default is Enable.
LLDP Handling	Select the handling mode for LLDP protocol. **Filtering:** Filters LLDP packets to prevent them from being forwarded to unauthorized ports. **Bridging:** Prevents LLDP packets from being bridged between switch ports. **Flooding:** Controls the flooding of LLDP packets to ensure they are forwarded only to the appropriate ports.

TLV Advertise Interval	Select the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 5–32767seconds.
Hold Multiplier	Select the multiplier on the transmit interval to assign to TTL (range 2–10, default = 4).
Reinitializing Delay	Select the delay before a re-initialization (range 1–10 seconds, default = 2).
Transmit Delay	Select the delay after an LLDP frame is sent (range 1–8191 seconds, default = 2).
Fast Start Repeat Count	Select the number of LLDP packets that will be sent during LLDP-MED Fast Start period. The default is 3. Available range is from 1 to 10.
Apply	Apply the settings to the switch.

12.1.2 Port Setting

This page allows to select specified port or all ports to configure LLDP state.

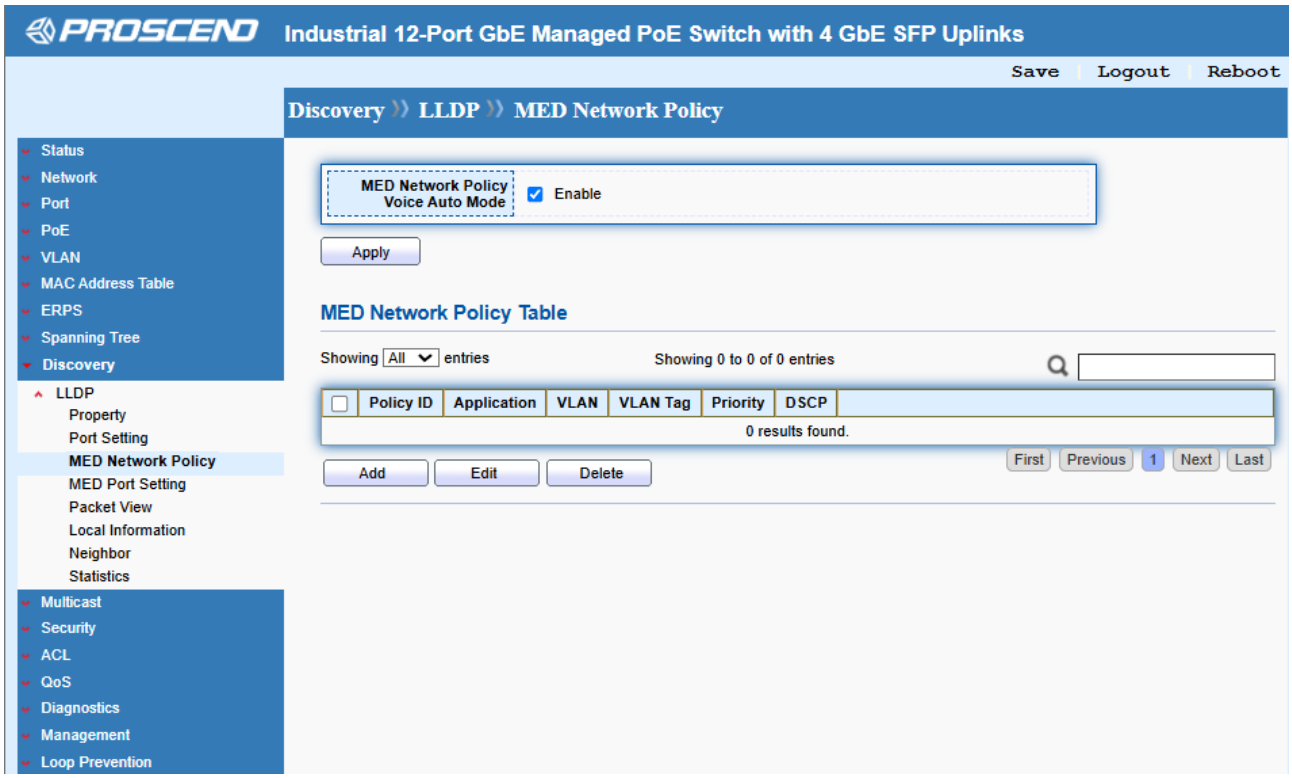




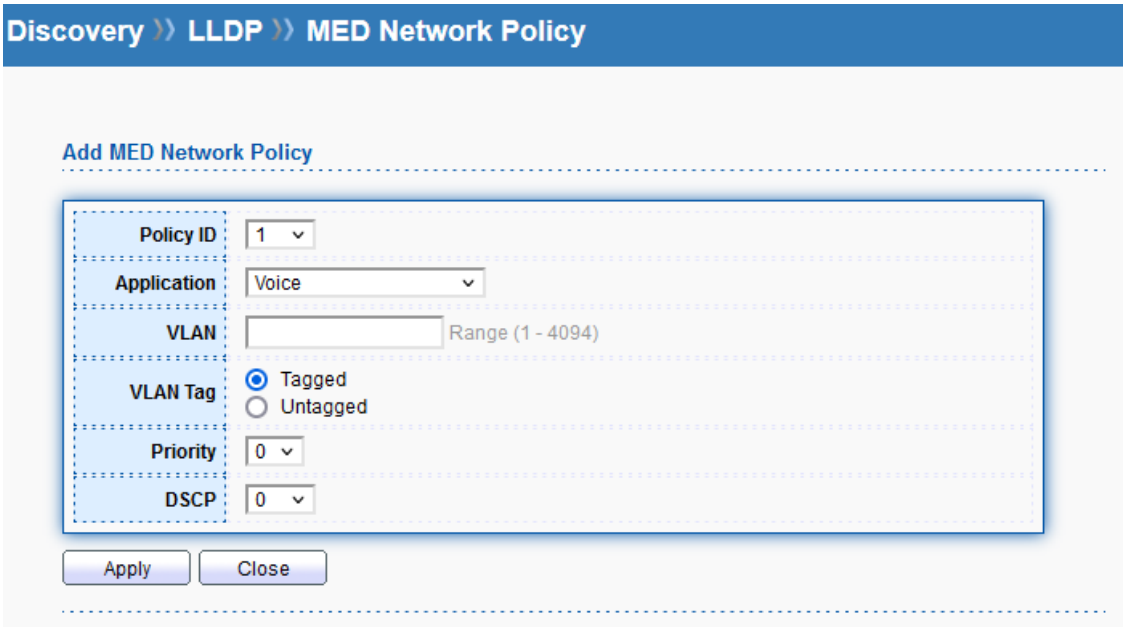
Item	Description
Edit	Edit the settings of selected port.
Port	Display the selected port.
Mode	**Transmit**: Transmit LLDP PDUs only. **Receive**: Receive LLDP PDUs only. **Normal**: Transmit and receive LLDP PDUs. **Disable**: Disable the transmission of LLDP PDUs.
Optional TLV	Within data communication protocols, optional information may be encoded as a type-length-value or TLV element inside a protocol. TLV is also known as tag-length value. The type and length are fixed in size (typically 1-4 bytes), and the value field is of variable size. Select the LLDP optional TLVs to be carried (multiple selection is allowed). Available items include System Name, Port Description, System Description, System Capability, 802.3 MAC-PHY, 802.3 Link Aggregation, 802.3 Maximum Frame Size, Management Address and 802.1 PVID.
802.1 VLAN Name	Select the VLAN ID number to be performed (multiple selections are allowed).
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

12.1.3 MED Network Policy

This page allows to set MED (Media Endpoint Discovery) network policy.



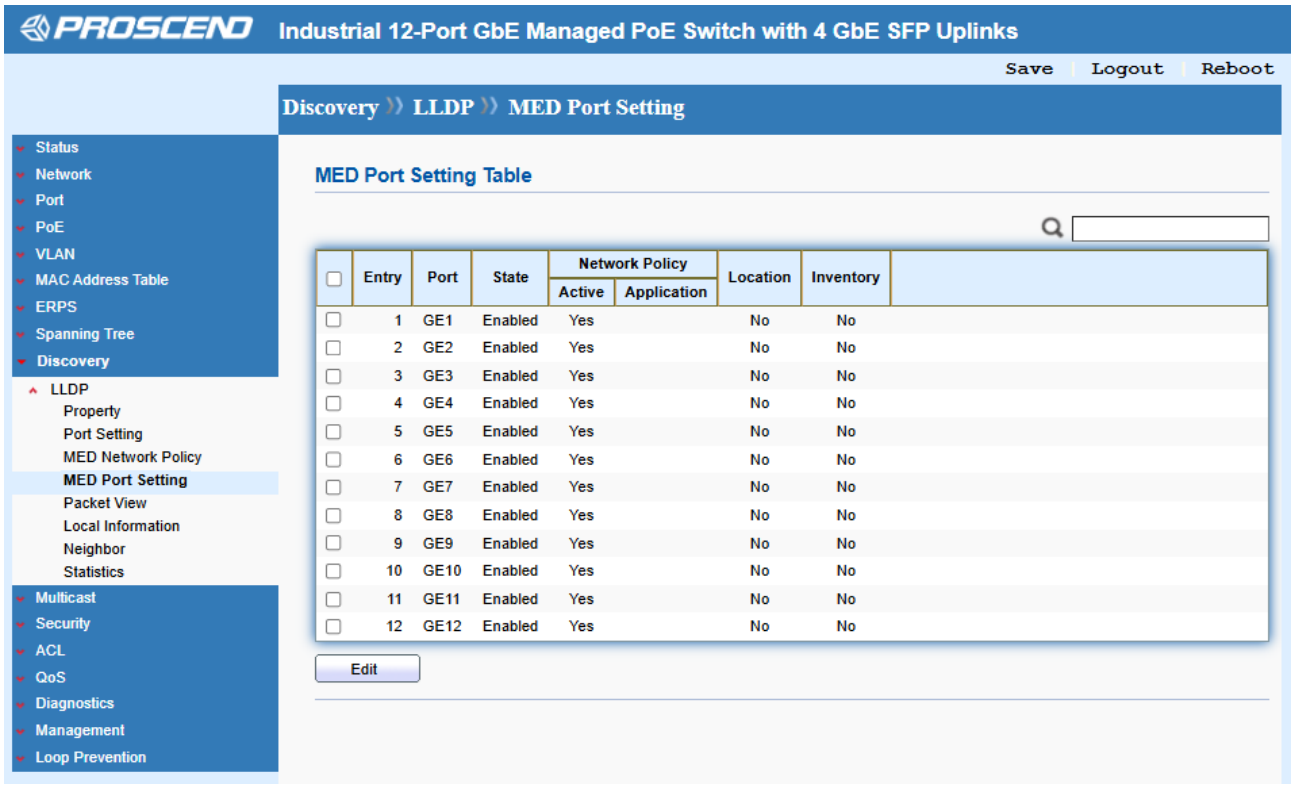
Item	Description
Add	Add a new MED network policy.
Edit	Edit existing entry of MED network policy.
Delete	Delete selected entry of MED network policy.



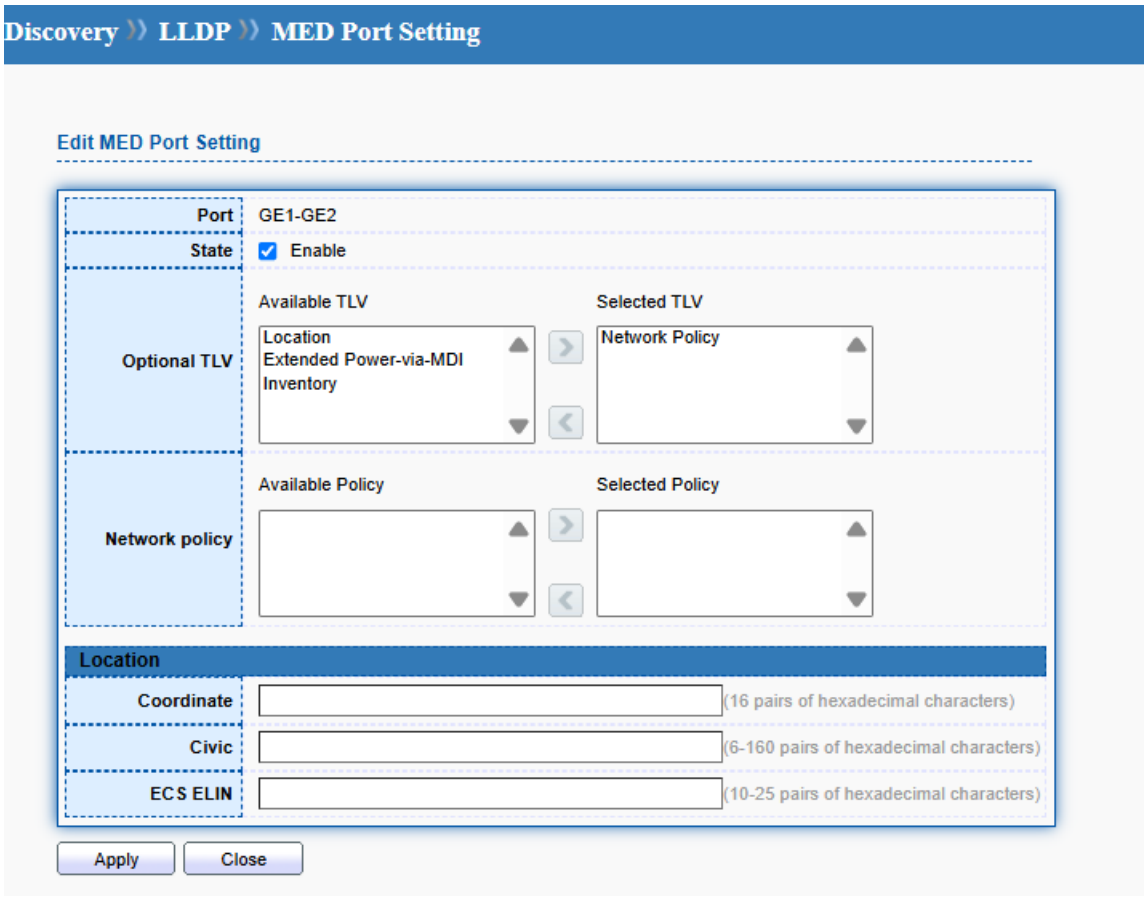
Item	Description
Policy ID	Choose a number for configuring the policy profile. Available selections include 1 to 32.
Application	There are several applications which can be used for MED network. Selections include Voice, Voice Signaling, Guest Voice, Guest Voice Signaling, Softphone Voice, Video Conferencing, Stream Video and Video Signaling.
VLAN	Set a VLAN ID (ranging from 1 to 4095) for such profile.
VLAN Tag	Specify if the outgoing packets will be tagged or not. **Tagged**: Packets will be sent out with a number tagged. **Untagged**: Packets will be sent out without any tag.
Priority	Set Layer2 priority (range from 0 to 7).
DSCP	Set DSCP value (range from 0 to 63).
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

12.1.4 MED Port Setting

This page allows to configure TLV (Type / Length / Value) settings for each port.



Entry	Port	State	Network Policy		Location	Inventory
			Active	Application		
1	GE1	Enabled	Yes		No	No
2	GE2	Enabled	Yes		No	No
3	GE3	Enabled	Yes		No	No
4	GE4	Enabled	Yes		No	No
5	GE5	Enabled	Yes		No	No
6	GE6	Enabled	Yes		No	No
7	GE7	Enabled	Yes		No	No
8	GE8	Enabled	Yes		No	No
9	GE9	Enabled	Yes		No	No
10	GE10	Enabled	Yes		No	No
11	GE11	Enabled	Yes		No	No
12	GE12	Enabled	Yes		No	No

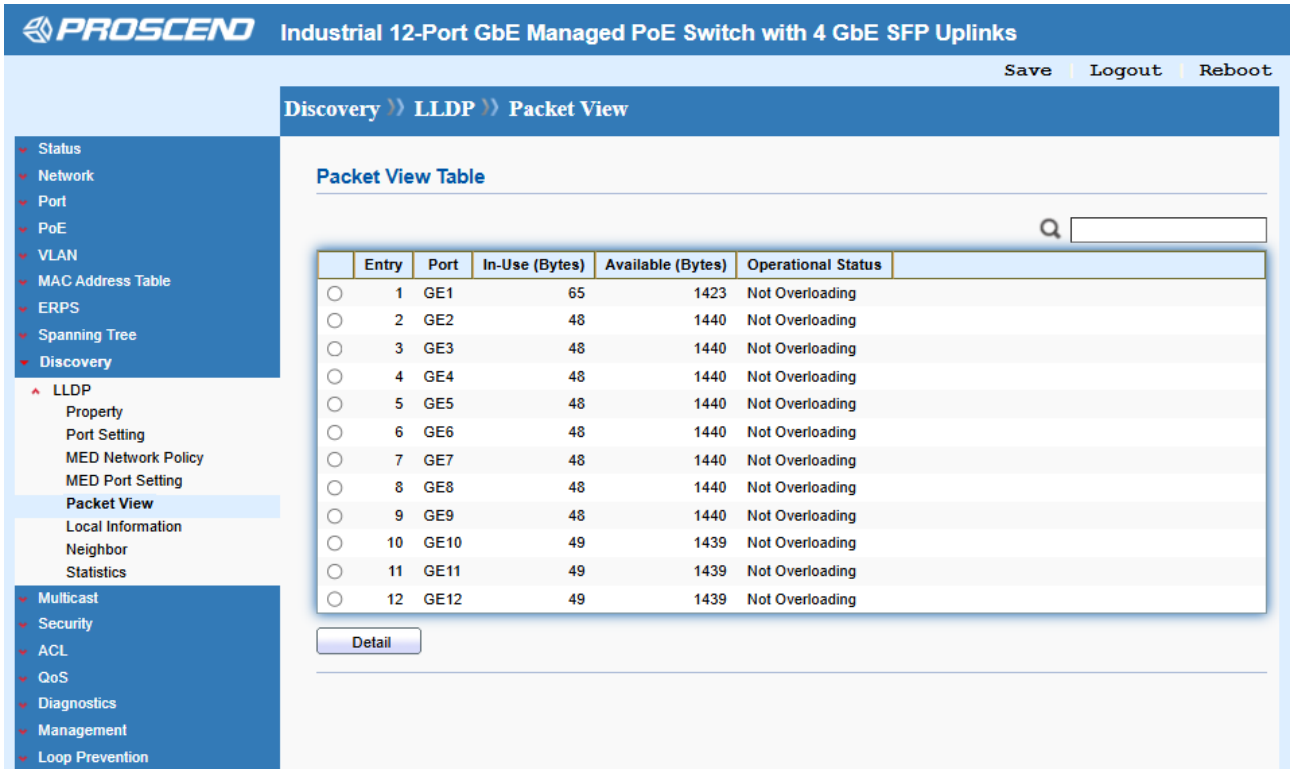


Item	Description
Edit	Edit the settings of selected port.
Port	The index number of selected port.
State	Enable or disable the LLDP MED on the selected port.
Optional TLV	Available TLV items will be shown in this field of “Available TLV”. Choose the one(s) you want and click the >> arrow to transfer the selection(s) to the field of “Selected TLV”.
Network policy	Available policy will be shown in this field of “Available Policy”. Choose the one(s) you want and click the >> arrow to transfer the selection(s) to the field of “Selected Policy”.
Coordinate	Enter the coordinate location in 16 pairs of hexadecimal characters.
Civic	Enter the civic address in 6 ~ 160 pairs of hexadecimal characters.
ECS ELIN	Enter the ECS (Emergency Call Service) ELIN (Emergency Location

	Identification Number) in 10 ~ 25 pairs of hexadecimal characters.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

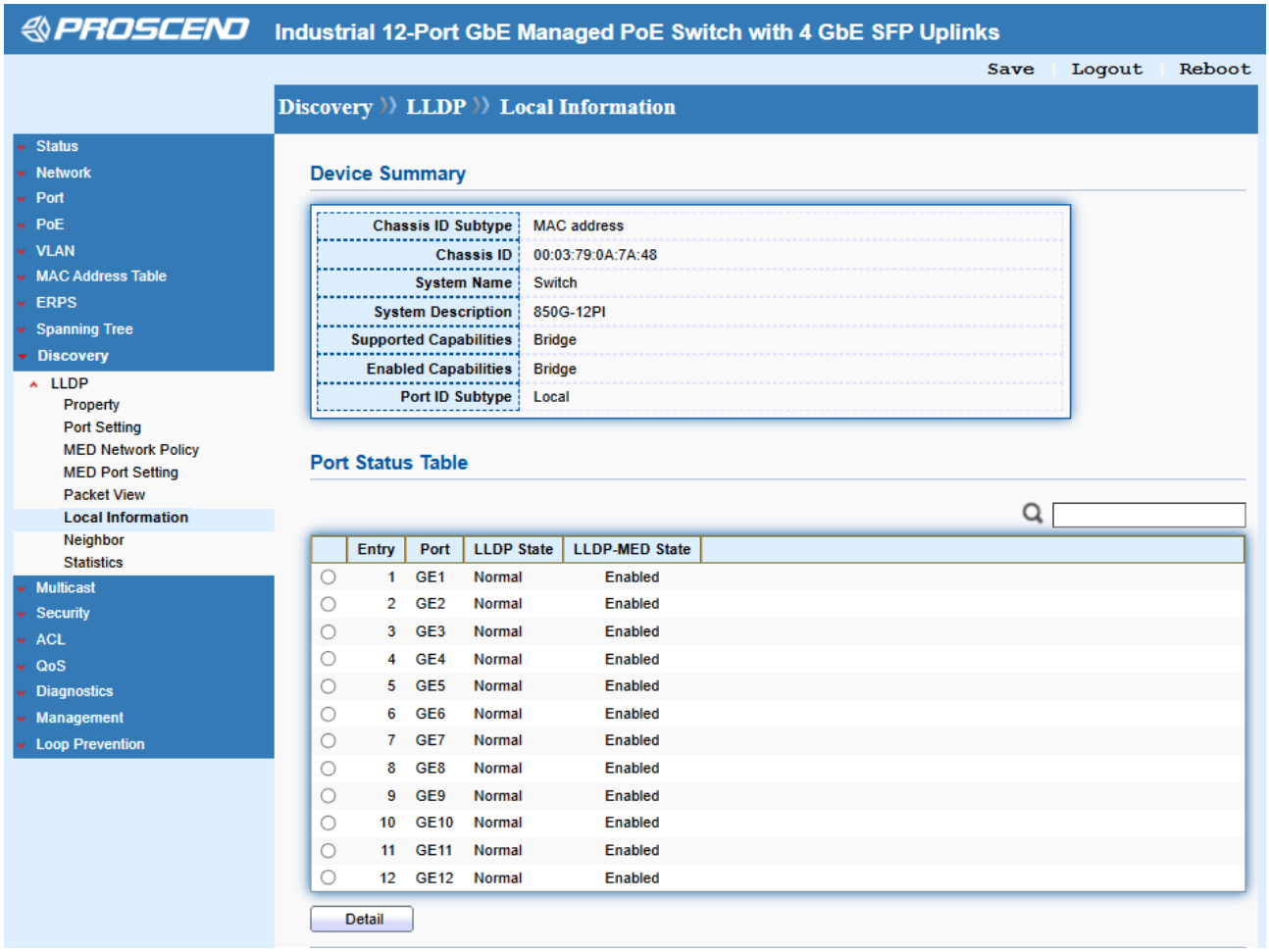
12.1.5 Packet View

This page provides packet view detail of each port.



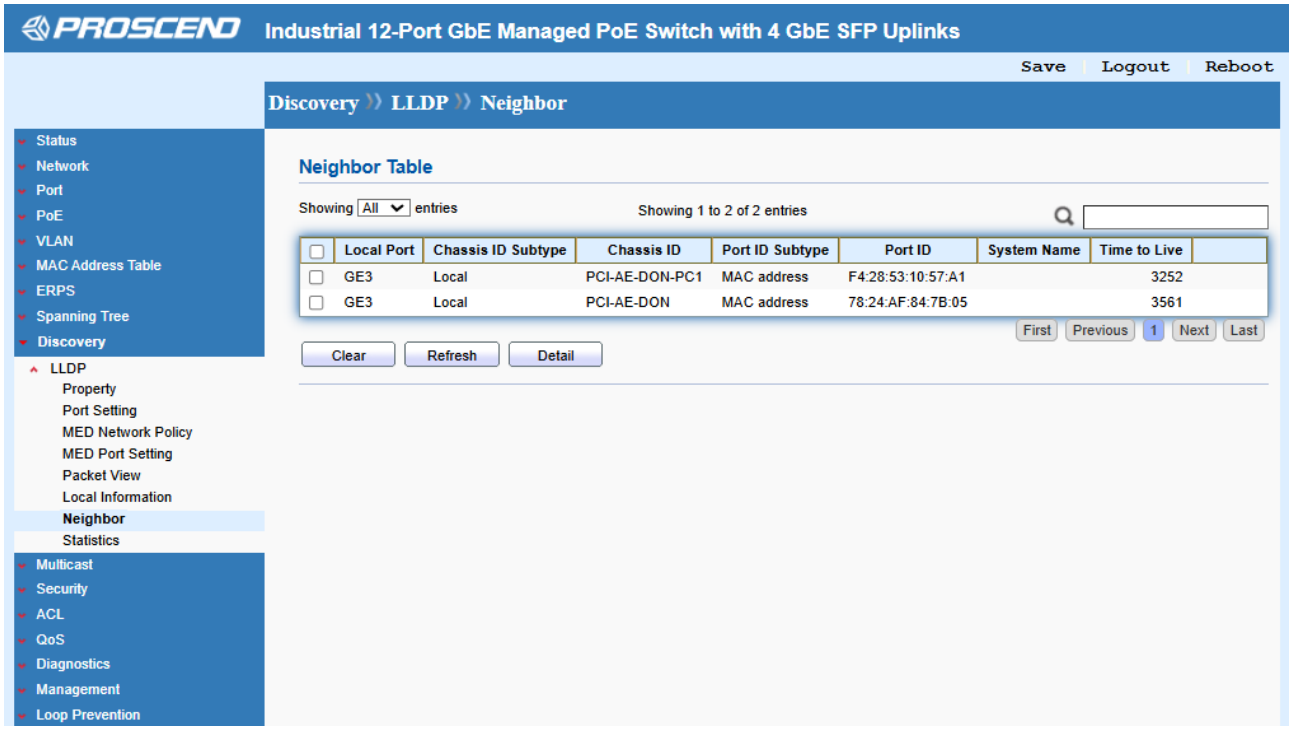
12.1.6 Local Information

This page shows detailed local information of LLDP.



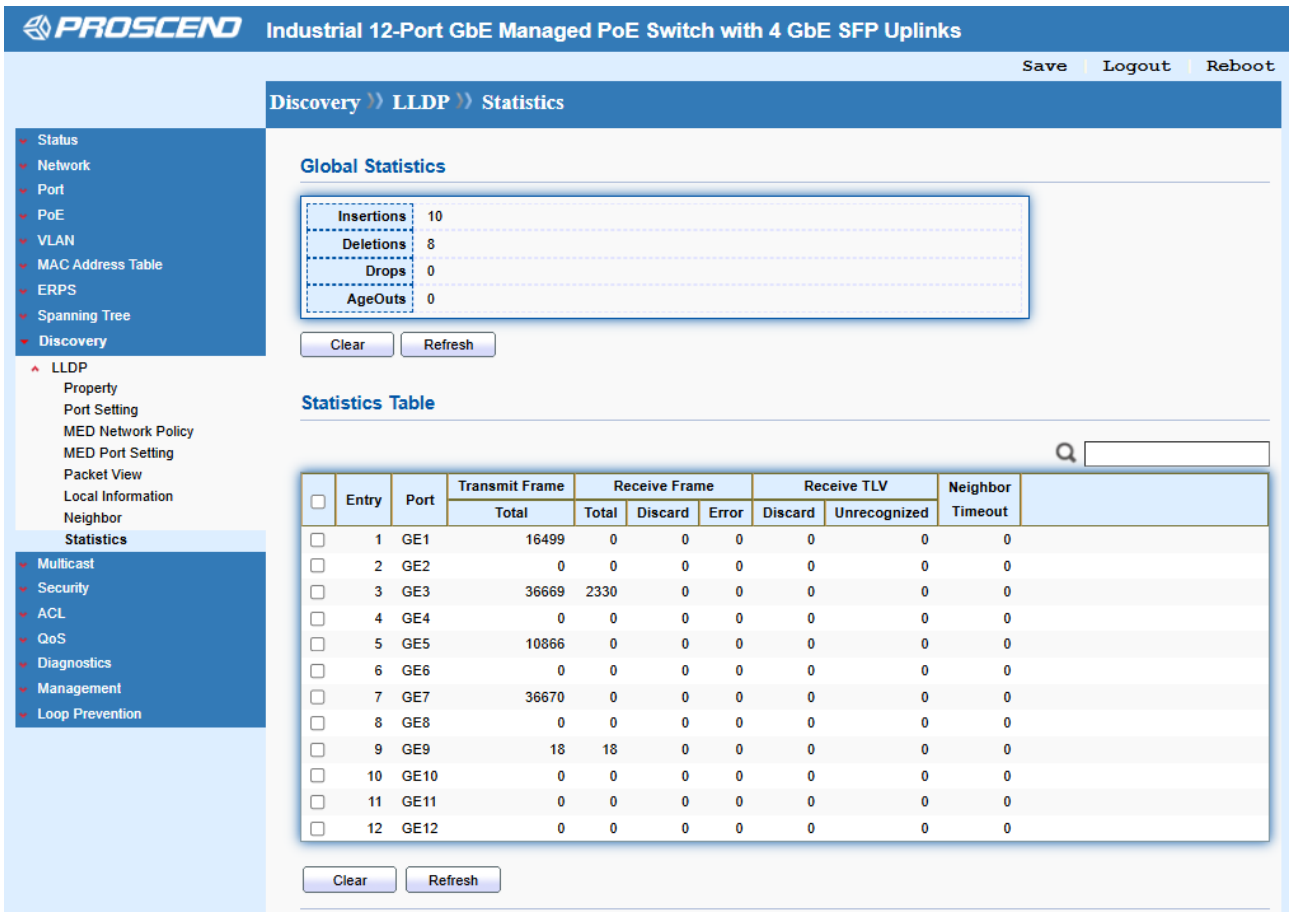
12.1.7 Neighbor

This page allows to view the information sent from neighboring devices by LLDP protocol.



12.1.8 Statistics

This page shows global statistics and statistics of each port.



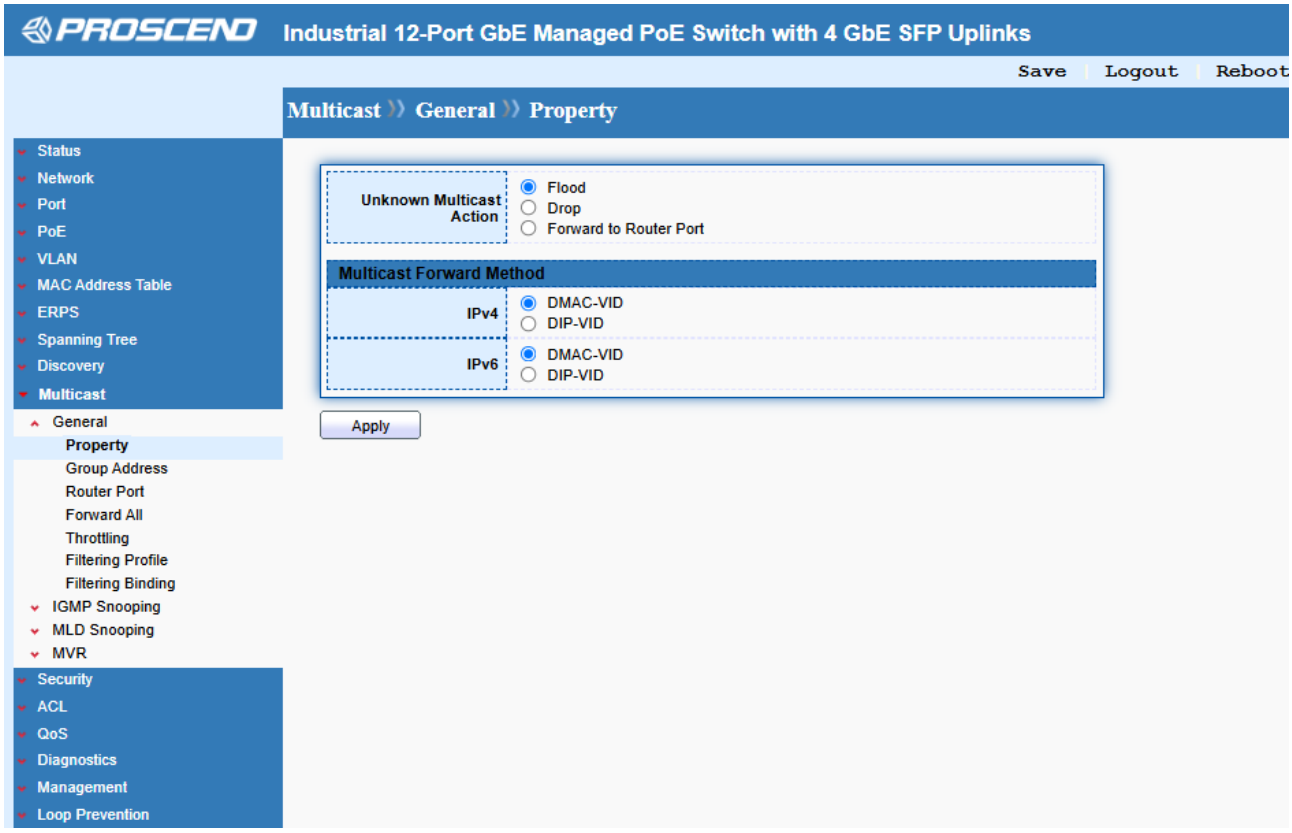
13 Multicast

IP multicast is a technique for one-to-many communication over an IP infrastructure in a network. To avoid the incoming data broadcasting to all GE ports, multicast is useful to transfer the data/message to specified GE ports for IGMP snooping. When Switch receives a message "subscribed" by the client, it must decide to transfer the data to specified GE ports according to the location of the client (subscribed member).

13.1 General

13.1.1 Property

For the multicast packets, this page allows the network administrator to choose actions for processing the unknown multicast packets and for handling known packets with MAC address, IP address and VLAN ID.

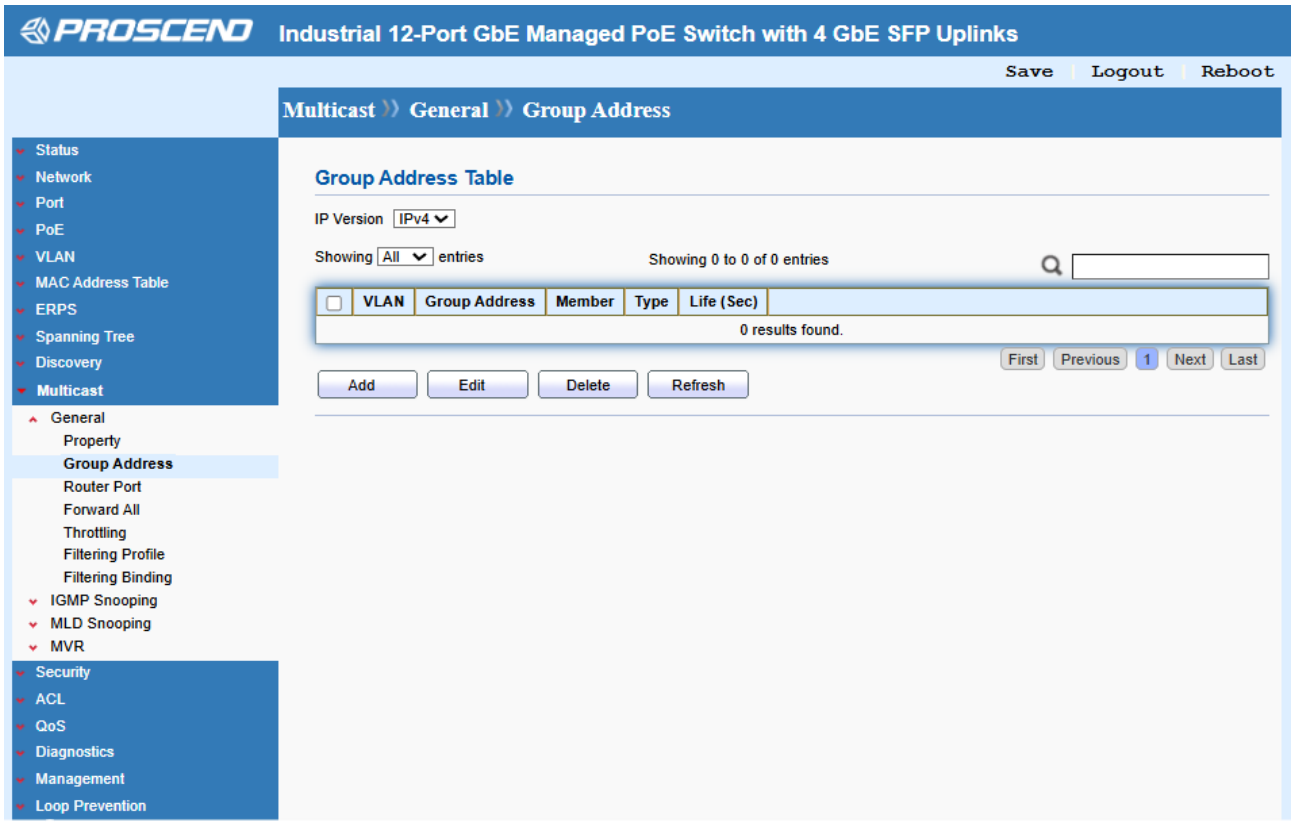


Item	Description
Unknown Multicast Action	Select an action for switch to handle with unknown multicast packet. **Flood**: Flood the unknown multicast data. **Drop**: Drop the unknown multicast data.

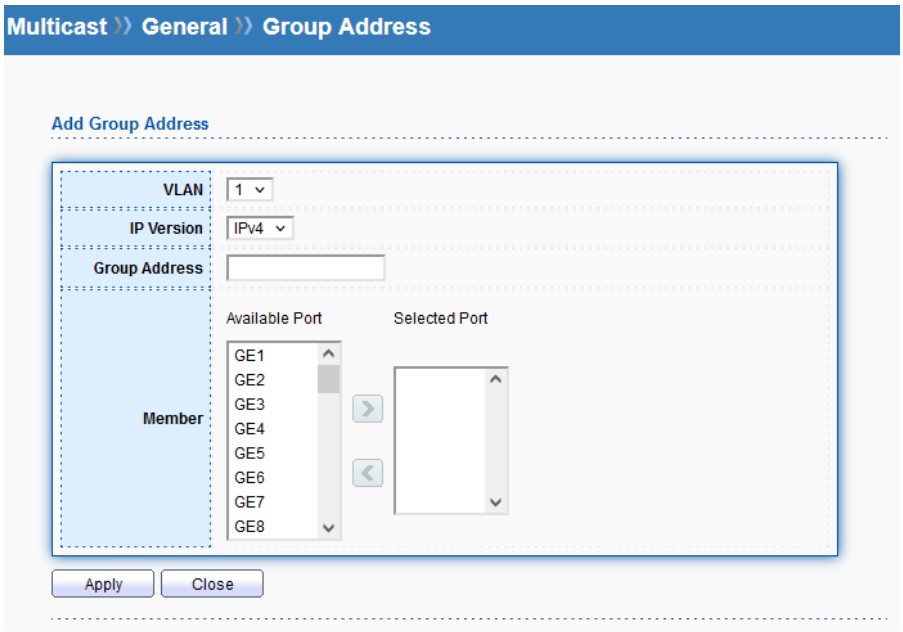
	Forward to Router port: Forward the unknown multicast data to router port.
IPv4	Set the IPv4 multicast forward method. **DMAC-VID:** Forward using destination multicast MAC address and VLAN IDs. **DIP-VID:** Forward using destination multicast IP address and VLAN ID.
IPv6	Set the IPv6 multicast forward method. **DMAC-VID:** Forward using destination multicast MAC address and VLAN IDs. **DIP-VID:** Forward using destination multicast IPv6 address and VLAN ID.
Apply	Apply the settings to the switch.

13.1.2 Group Address

The page allows to assign a VLAN/port as a specific IPv4/IPv6 multicast member. Every IPv4/IPv6 multicast stream that belongs to the specified group IP address will be forwarded to the specified port/VLAN member.



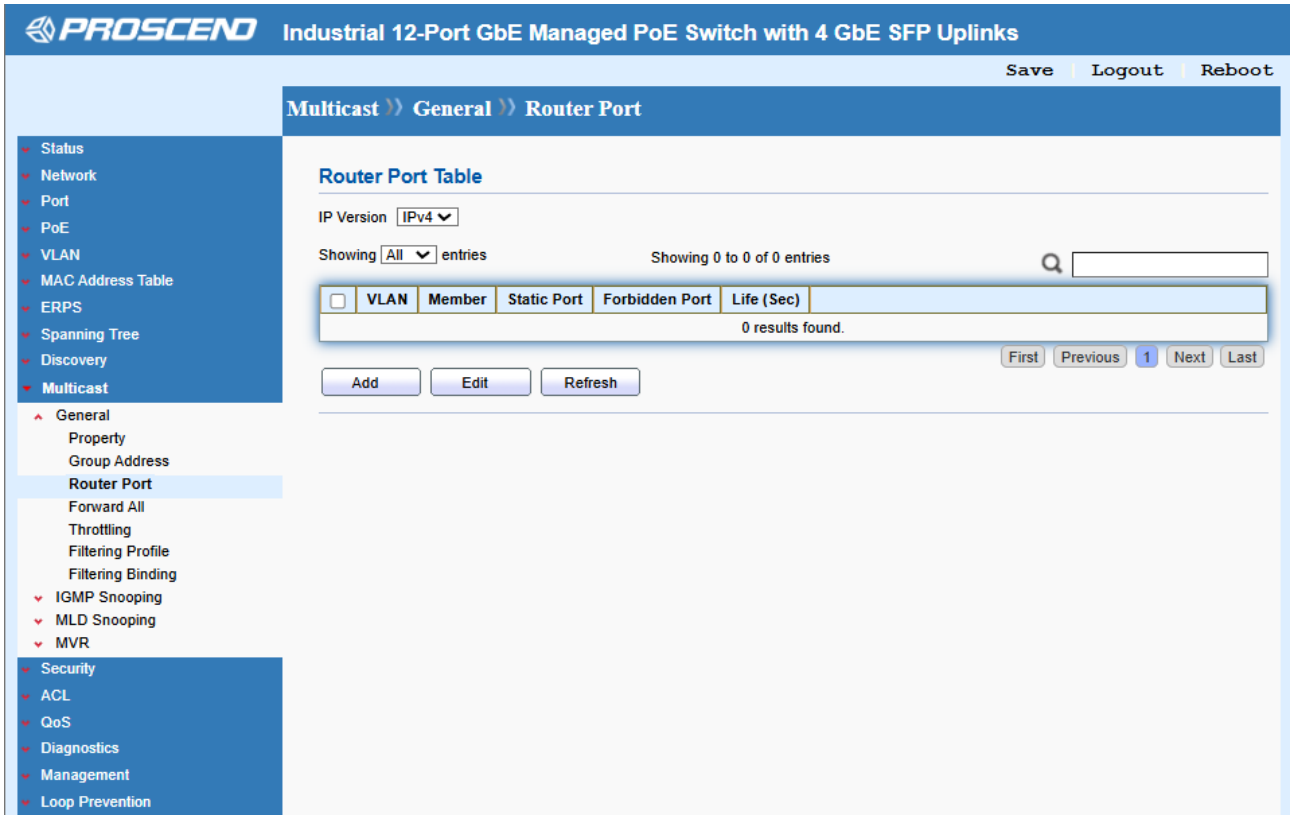
Item	Description
IP Version	Select the IP version which will be displayed on this page.
Add	Add a new group address.
Edit	Edit the existing group address.
Delete	Delete the selected group address.
Refresh	Refresh the current page.



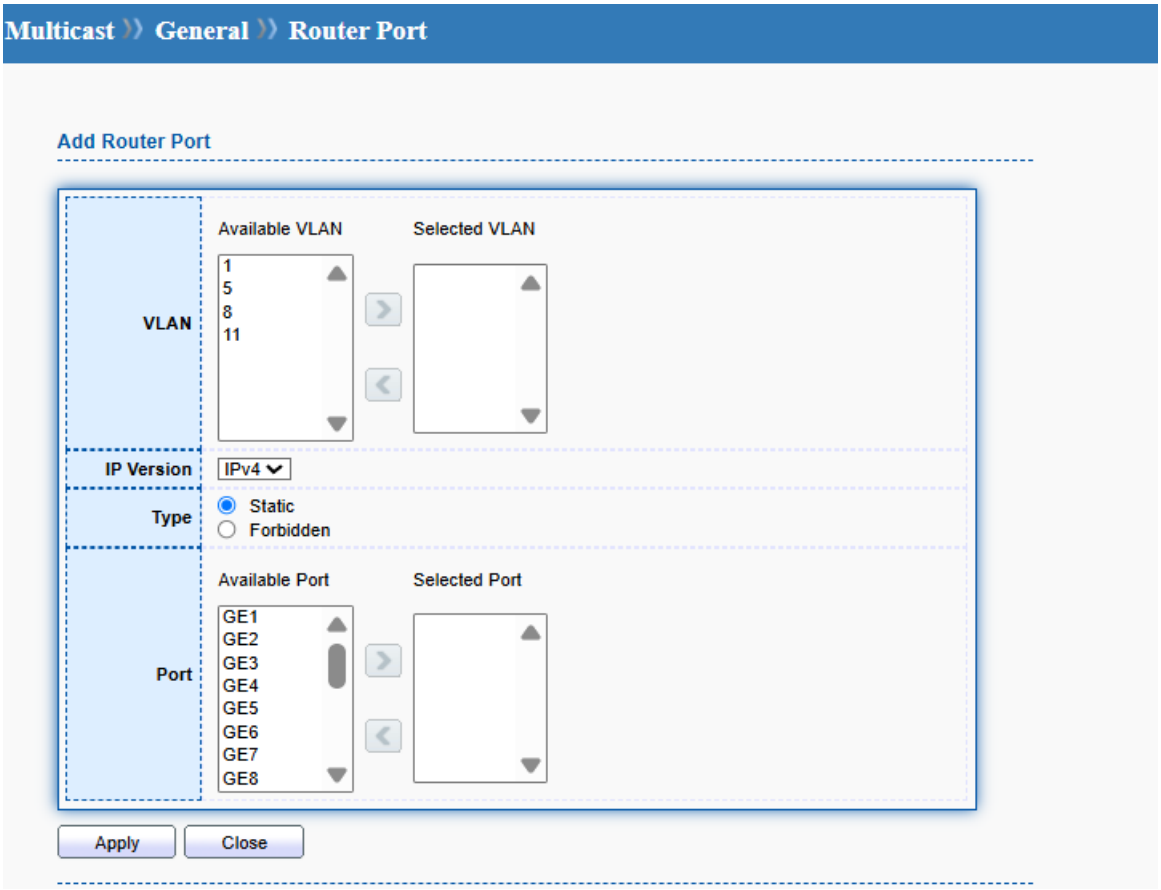
Item	Description
VLAN	Use the drop down list to specify a VLAN profile as IGMP Static Group.
IP Version	Select the IP Version.
Group Address	It is an identifier for the group member. Packets sent to such address will be transferred to all interfaces defined in Member Ports. Specify the IPv4/IPv6 multicast address you wish to assign for the static group (defined in VLAN).
Member	Specify the port(s) that static group with given IPv4/IPv6 multicast address shall include.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

13.1.3 Router Port

This page shows the IGMP queried router known to this switch.



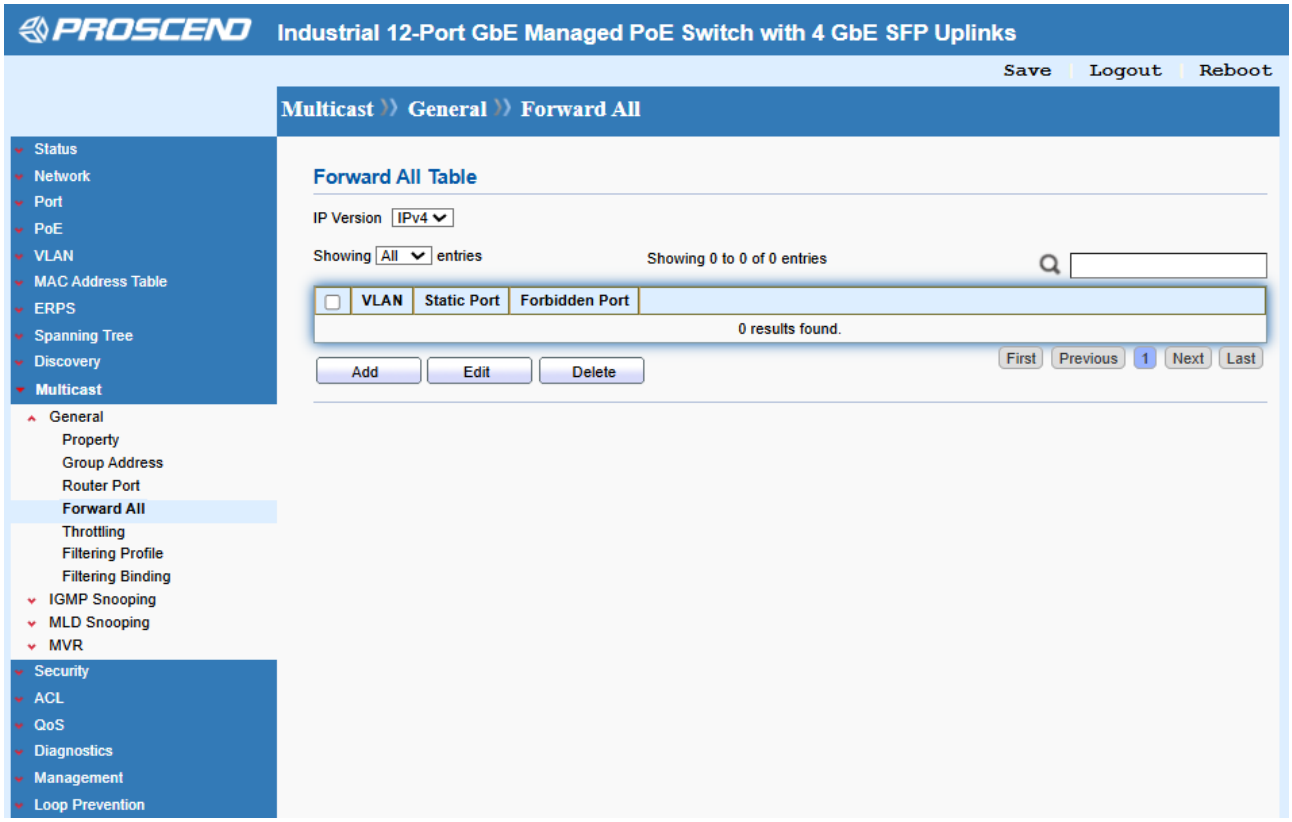
Item	Description
IP Version	Select the IP version which will be displayed on this page.
Add	Add a new entry.
Edit	Edit the existing entry.
Refresh	Refresh the current page.



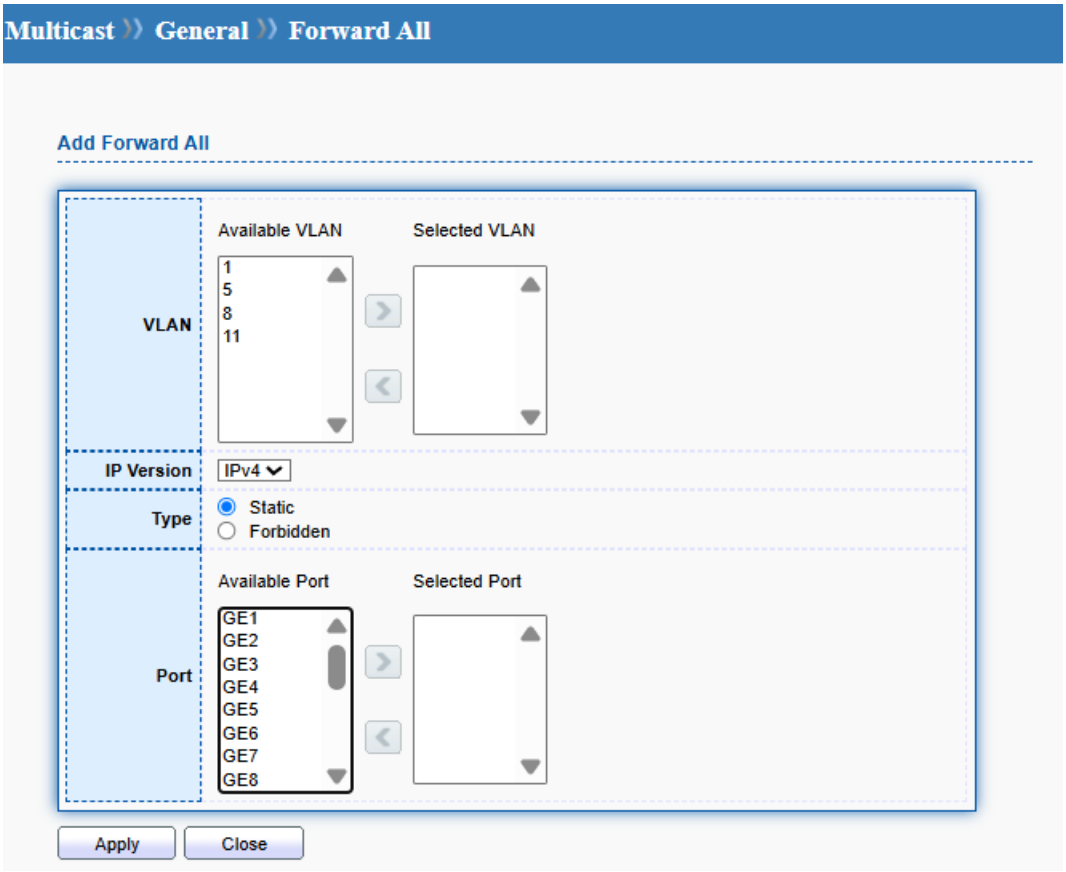
Item	Description
VLAN	Available VLAN will be shown in this field of “Available VLAN”. Choose the one(s) you want and click the >> arrow to transfer the selection(s) to the field of “Selected VLAN”.
IP Version	Select the IP Version.
Type	**Static**: Specify LAN Port (GE/LAG) to send out query to remote host. **Forbidden**: Use the drop down list to specify forbidden LAN Port (GE/LAG).
Port	Available port will be shown in this field of “Available Port”. Choose the one(s) you want and click the >> arrow to transfer the selection(s) to the field of “Selected Port”.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

13.1.4 Forward All

This page is allowed to determine which port(s) would like to receive the data (multicast packets) that forwarded by Switch.



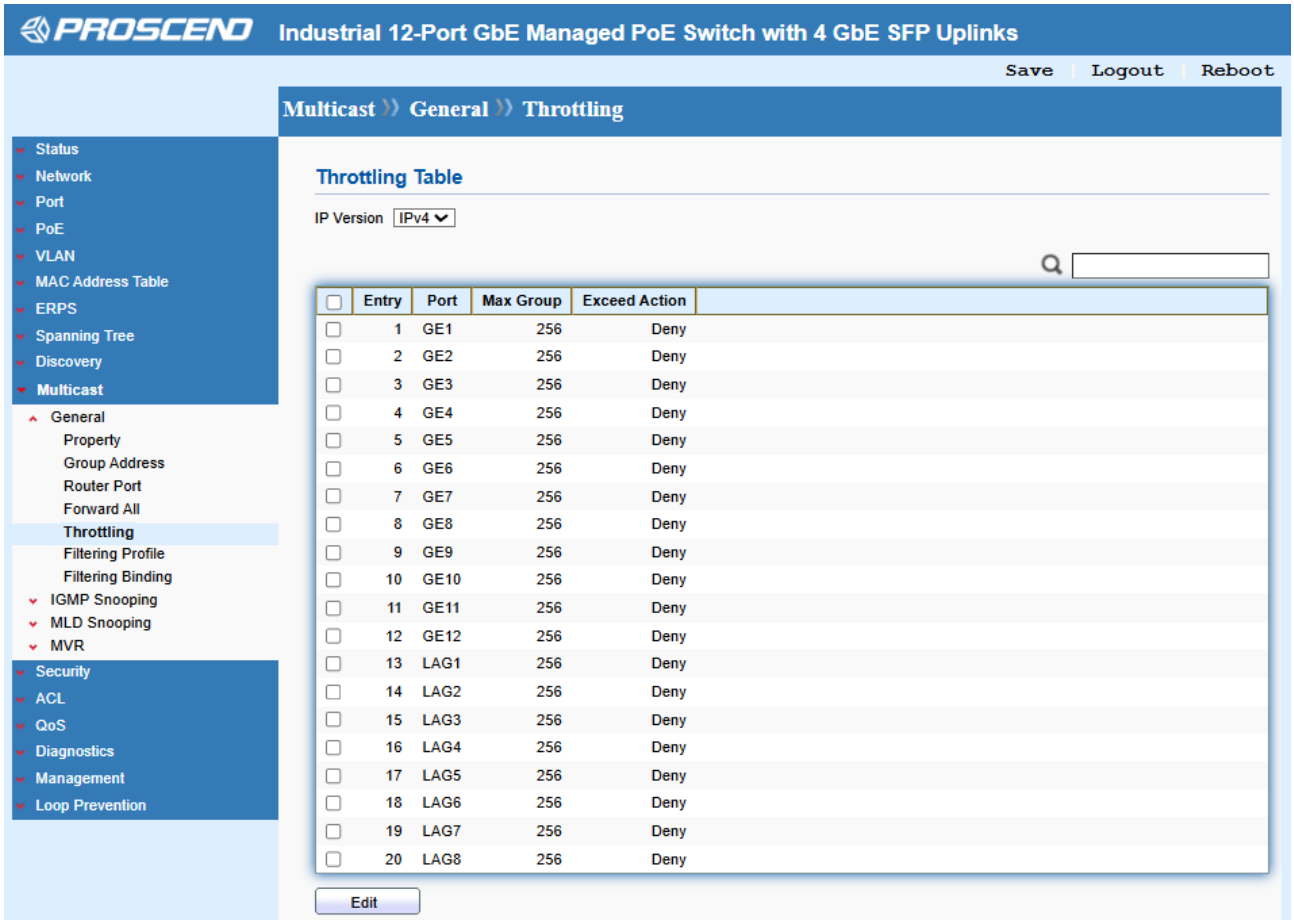
Item	Description
IP Version	Select the IP version which will be displayed on this page.
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the selected entry.



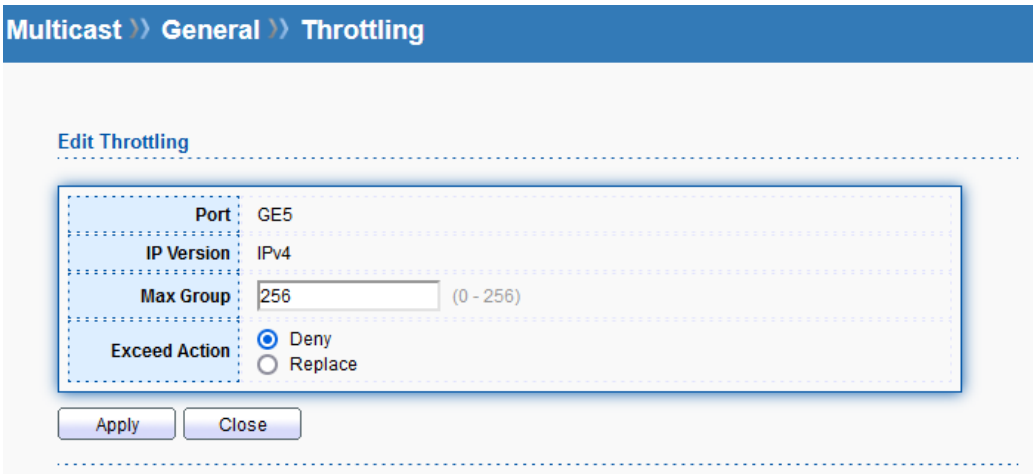
Item	Description
VLAN	Available VLAN will be shown in this field of “Available VLAN”. Choose the one(s) you want and click the >> arrow to transfer the selection(s) to the field of “Selected VLAN”.
IP Version	Select the IP Version.
Type	**Static**: The multicast packets will be delivered to the network device connected by these ports. **Forbidden**: the multicast packets will not be delivered to the network device connected by these ports.
Port	Available port will be shown in this field of “Available Port”. Choose the one(s) you want and click the >> arrow to transfer the selection(s) to the field of “Selected Port”.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

13.1.5 Throttling

The Throttling page is used for configuring the maximum number (0~256) of IGMP group that a user on a switch port can join. After defined the maximum number, each switch port interface can be set to deny the IGMP join report or set to replace randomly selected multicast interface with received IGMP join report.



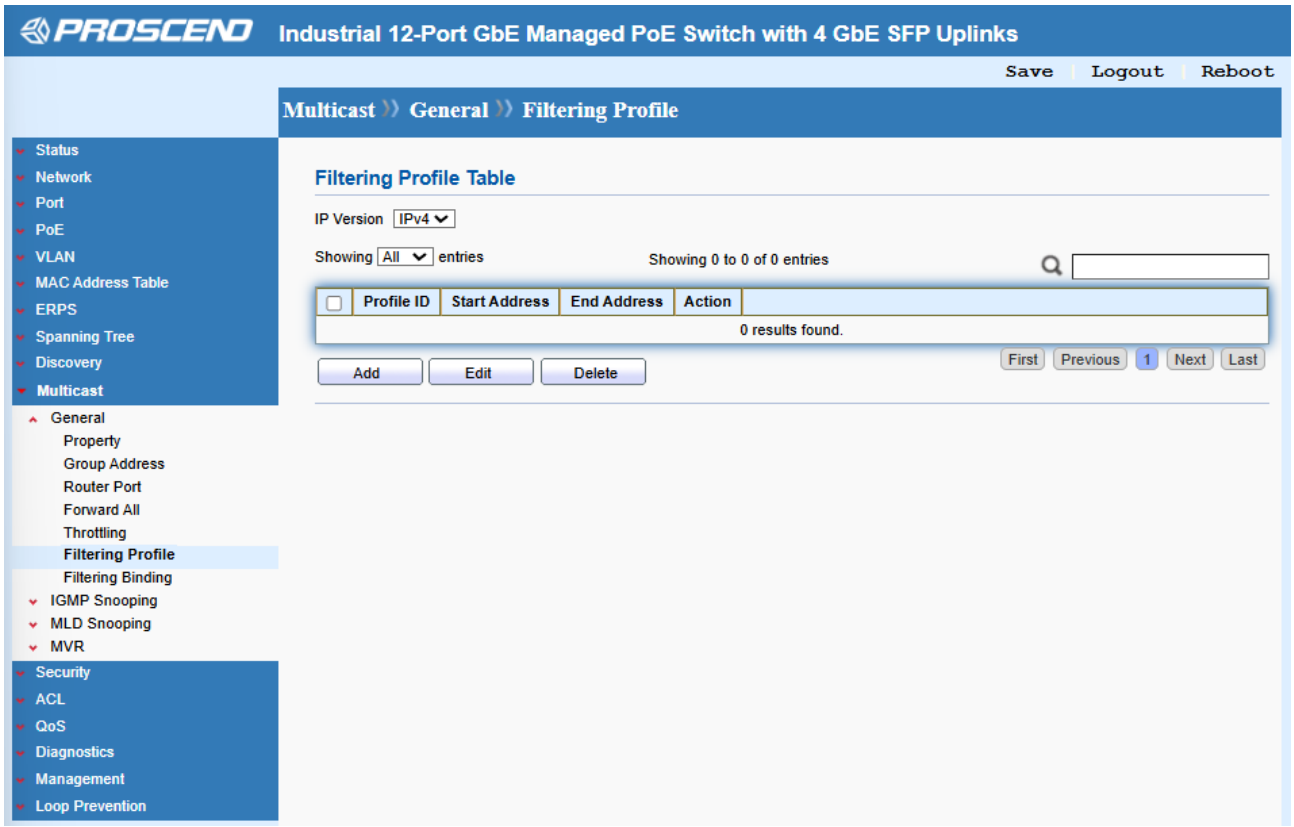
Item	Description
IP Version	Select the IP version which will be displayed on this page.
Edit	Edit the selected entry.



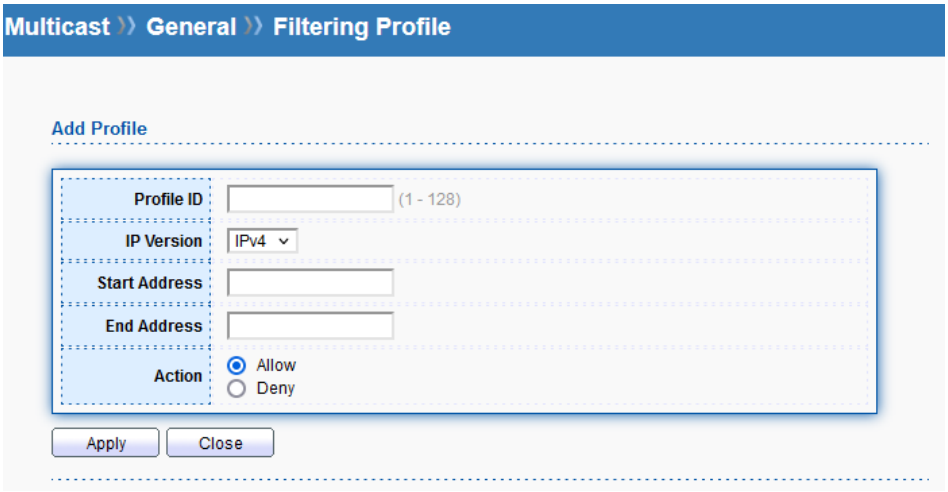
Item	Description
Port	The index number of selected port.
IP Version	The selected IP Version.
Max Group	Define the maximum number of IGMP group profile that a user on the switch can join. If “0” is entered, then such interface (port) can join all of the IGMP group profiles.
Exceed Action	**Deny**: It is default setting. The IGMP join report (for multicast service) received by such interface will be discarded. **Replace**: When it is selected, a new group with IGMP report received will replace the existing group.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

13.1.6 Filtering Profile

The filtering profile page allows to configure up to 128 IP-group (for multicast service) profiles (starting and ending point within an IP range shall be specified). Each IP group profile can be set for permission of / denial of network service respectively.



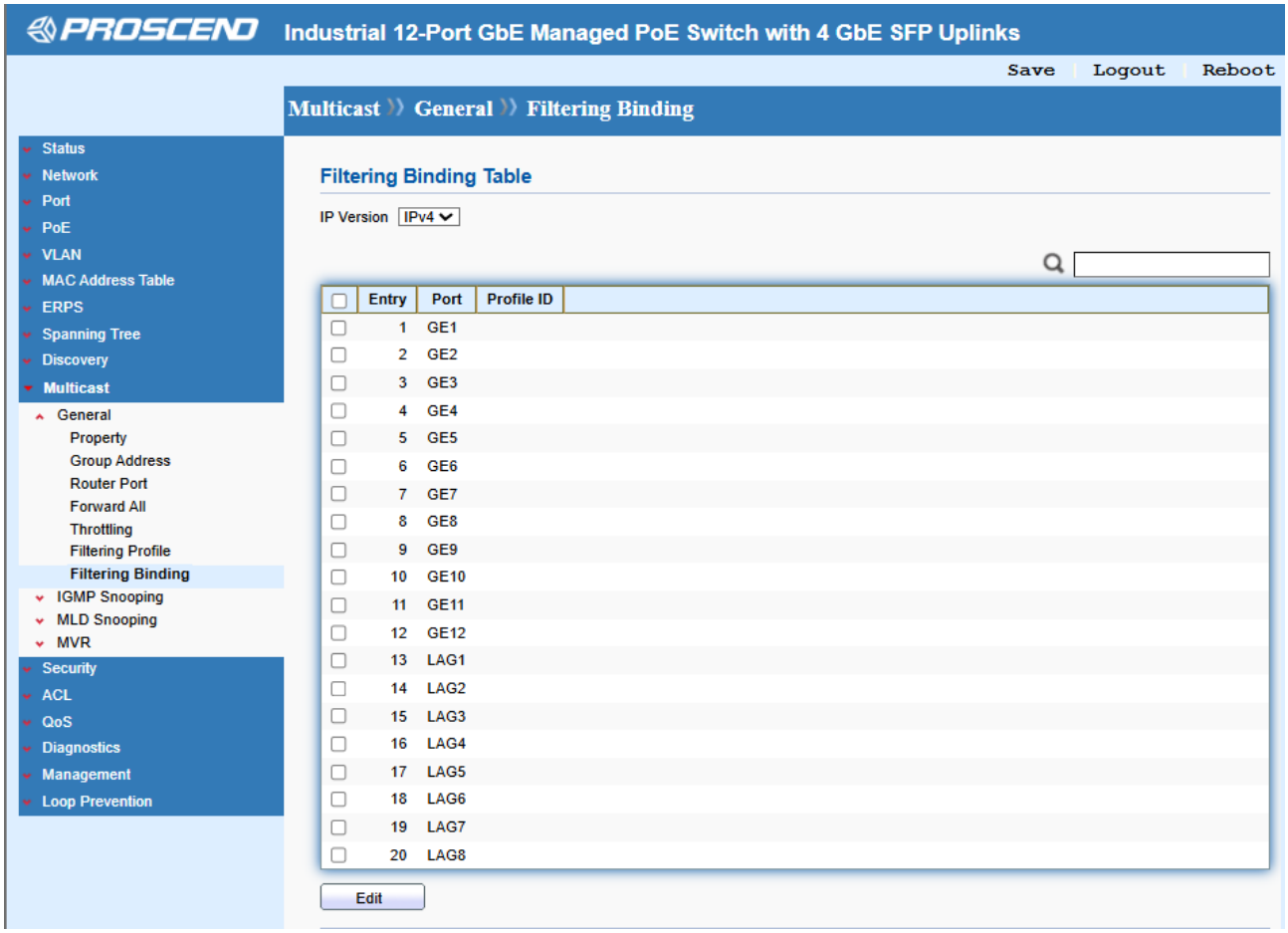
Item	Description
IP Version	Select the IP version which will be displayed on this page.
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the selected entry.



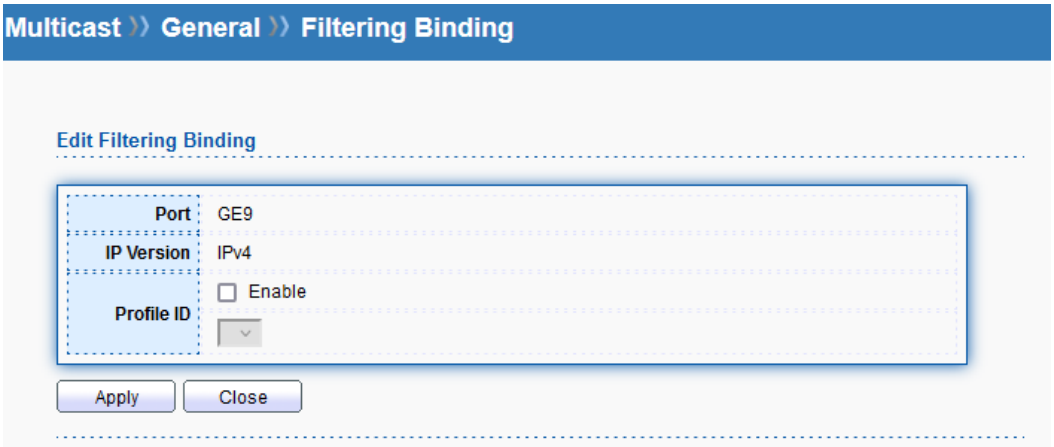
Item	Description
Profile ID	Enter the profile ID for IGMP snooping.
IP Version	Select the IP Version.
Start Address	Enter an IP address as the starting point for the IP range.
End Address	Enter an IP address as the ending point for the IP range.
Action	**Allow**: When it is selected, the request for multicast traffic will be forwarded to the multicast group normally. **Deny**: It is default setting. The forwarding request of multicast traffic will be discarded.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

13.1.7 Filtering Binding

This page allows to select a filtering profile for GE/LAG port to process multicast traffic.



Item	Description
IP Version	Select the IP version which will be displayed on this page.
Edit	Edit the selected entry.



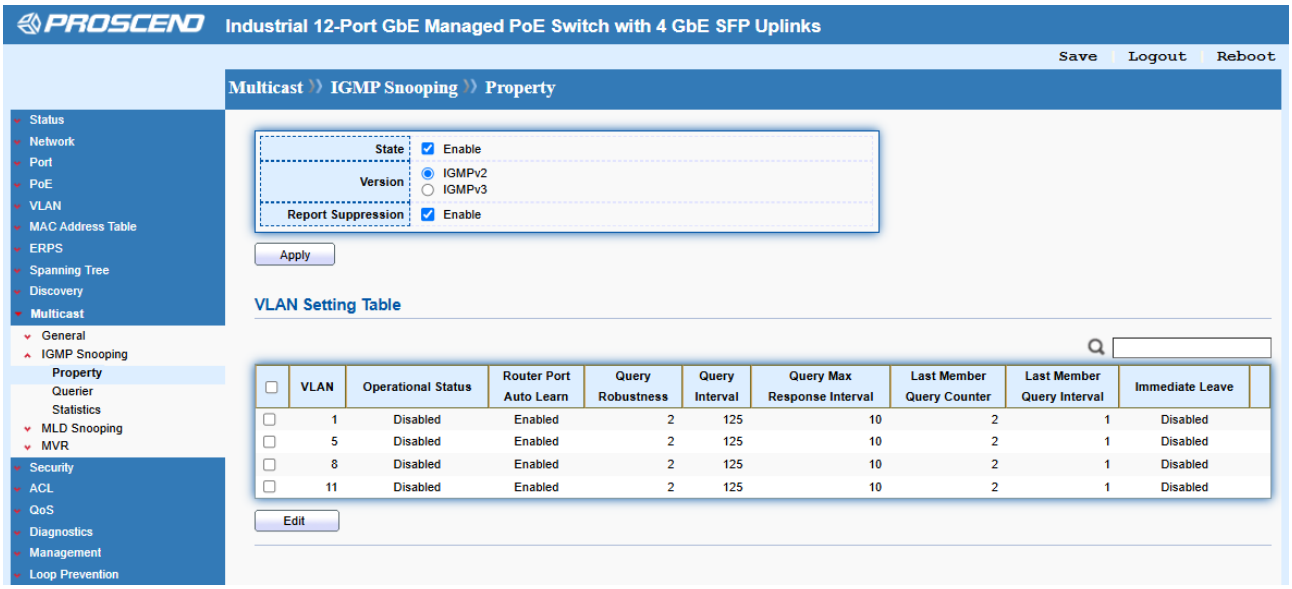
Item	Description
Port	The index number of selected port.
IP Version	The selected IP Version.
Profile ID	Enable of disable selected filtering profile for the selected port/interface.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

13.2 IGMP Snooping

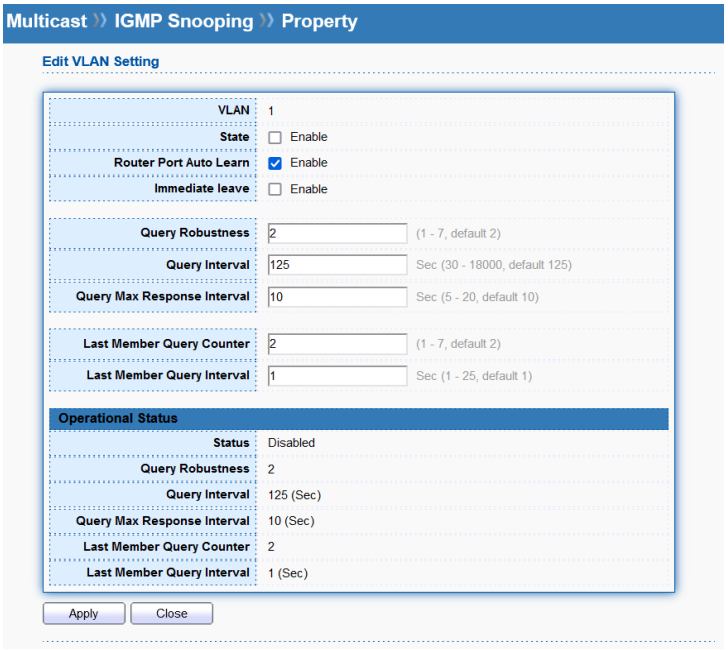
IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations, the switch maintains a map of which links need which IP multicast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

13.2.1 Property

This page allows to enable/disable IGMP function, select snooping version, and enable/disable snooping report suppression.



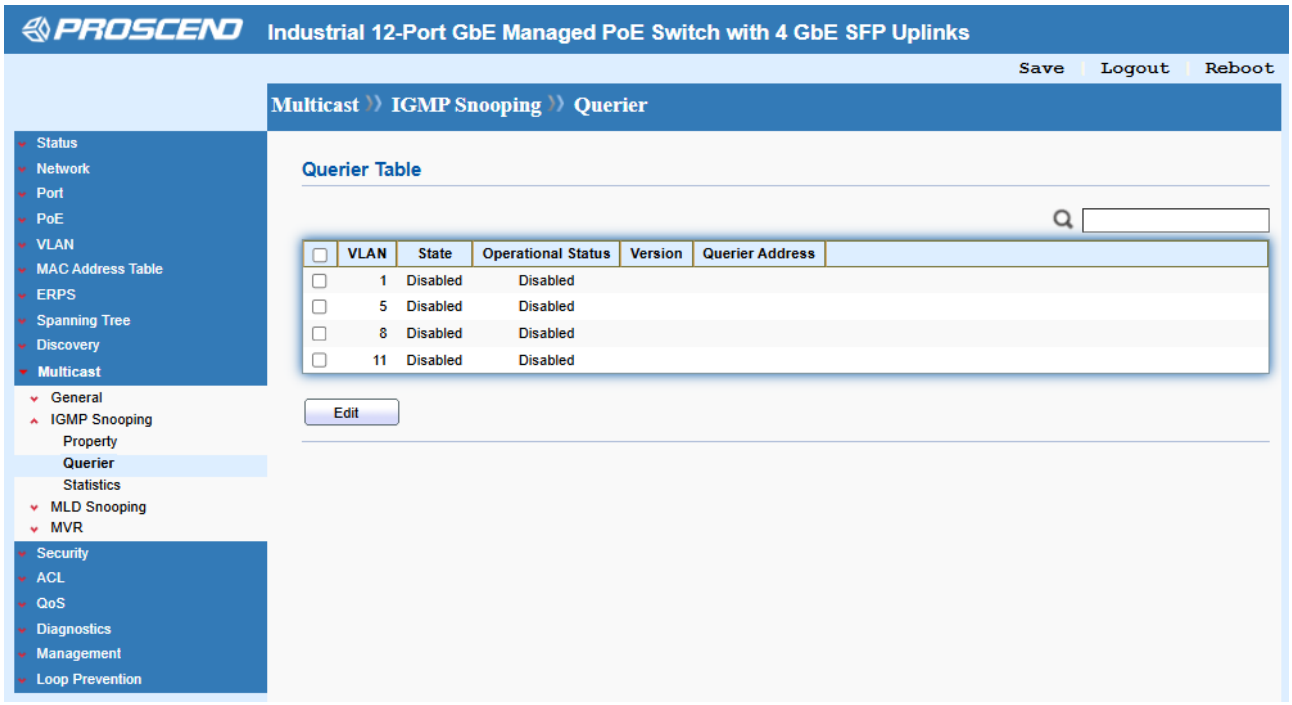
Item	Description
State	Enable or disable the IGMP snooping.
Version	Set the IGMP snooping Version. **IGMPv2**: Only support IGMP v2 packet. **IGMPv3**: Support v3 basic and v2.
Report Suppression	Enable to allow the switch to handle IGMP reports between router and host, suppressing bandwidth used by IGMP.
Apply	Apply the settings to the switch.
Edit	Edit the selected entry.

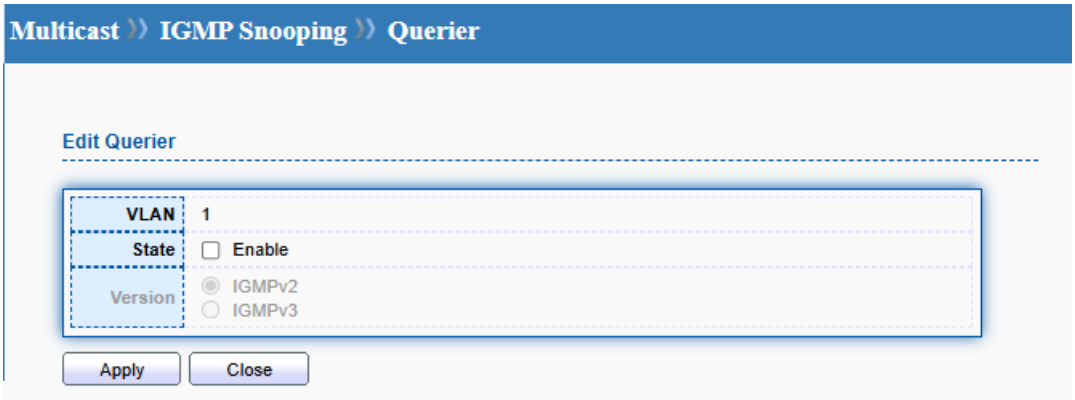


Item	Description
VLAN	The index number of selected VLAN ID.
State	Enable or disable the IGMP snooping function
Router Port Auto Learn	Set the enabling status of IGMP router port learning. Choose Enable to learn router port by IGMP query.
Immediate leave	Leave the multicast group immediately on the port & VLAN where leave message is sent from, regardless there is still a subscribed member or not. Click Enable to enable Fast leave function.
Query Robustness	Set a number which allows tuning for the expected packet loss on a subnet.
Query Interval	Set the interval for sending general query.
Query Max Response Interval	It specifies the maximum allowed time before sending a responding report in units of 1/10 second.
Last Member Query Counter	After querying for specified times (defined here) and still not receiving any response from the subscribed member, Switch will stop transmitting data to the related GE port(s).
Last Member Query Interval	The maximum time interval between counting each member query message with no responses from any subscribed member.
Operational Status	Display the current operation status of IGMP snooping.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

13.2.2 Querier

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



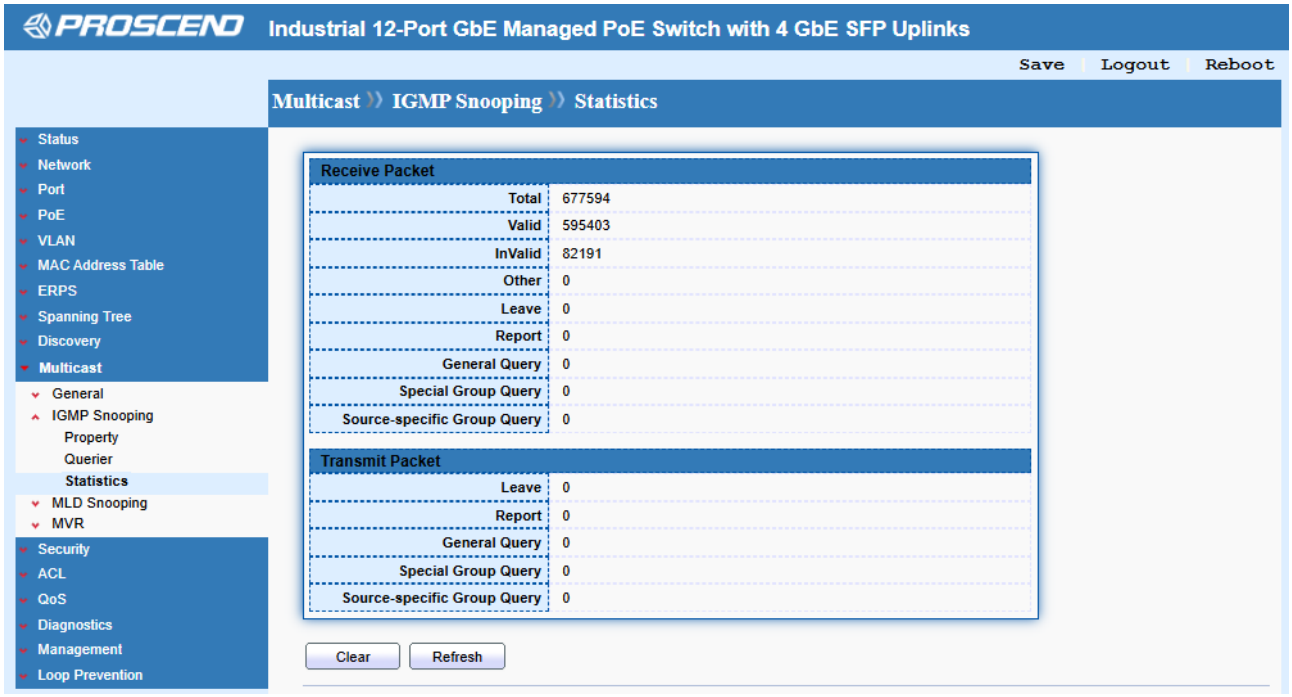


Item	Description
Edit	Edit the selected entry.
VLAN	The index number of selected VLAN ID.
State	Enable or disable the IGMP Querier on the chosen VLAN profile.
Version	Set the query version of IGMP Querier Election on the chosen VLANs. **IGMPv2**: Querier version 2.

	IGMPv3: Querier version 3.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

13.2.3 Statistics

This page displays the statistics of IGMP snooping.

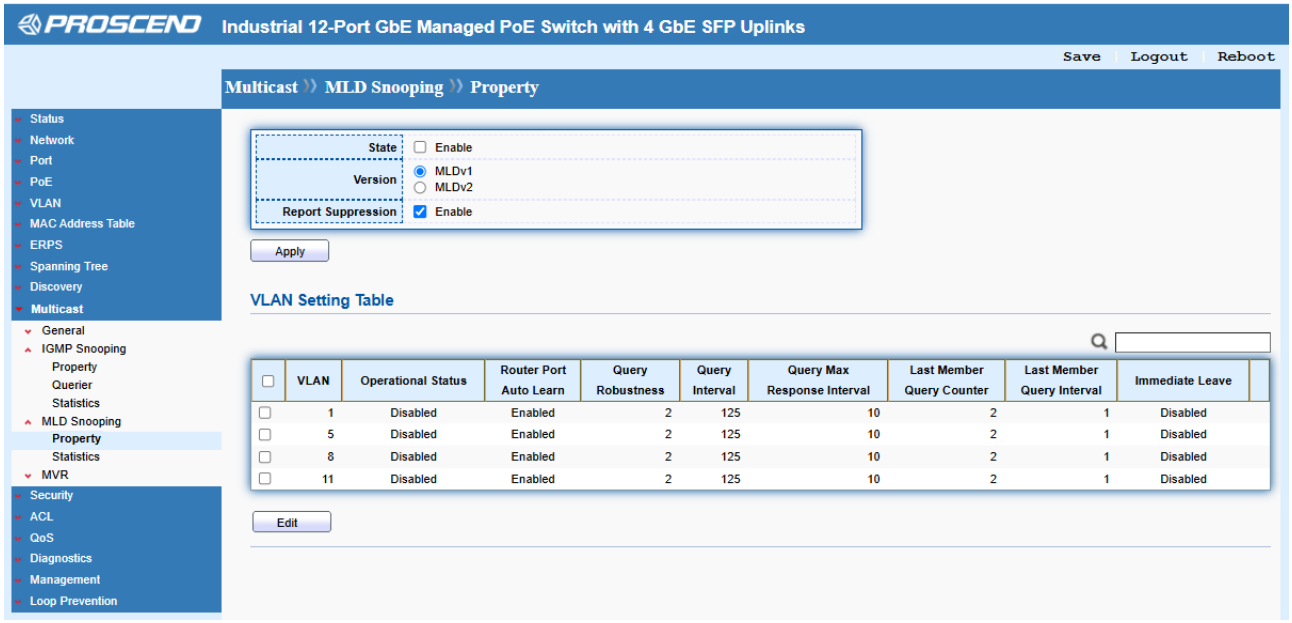


13.3 MLD Snooping

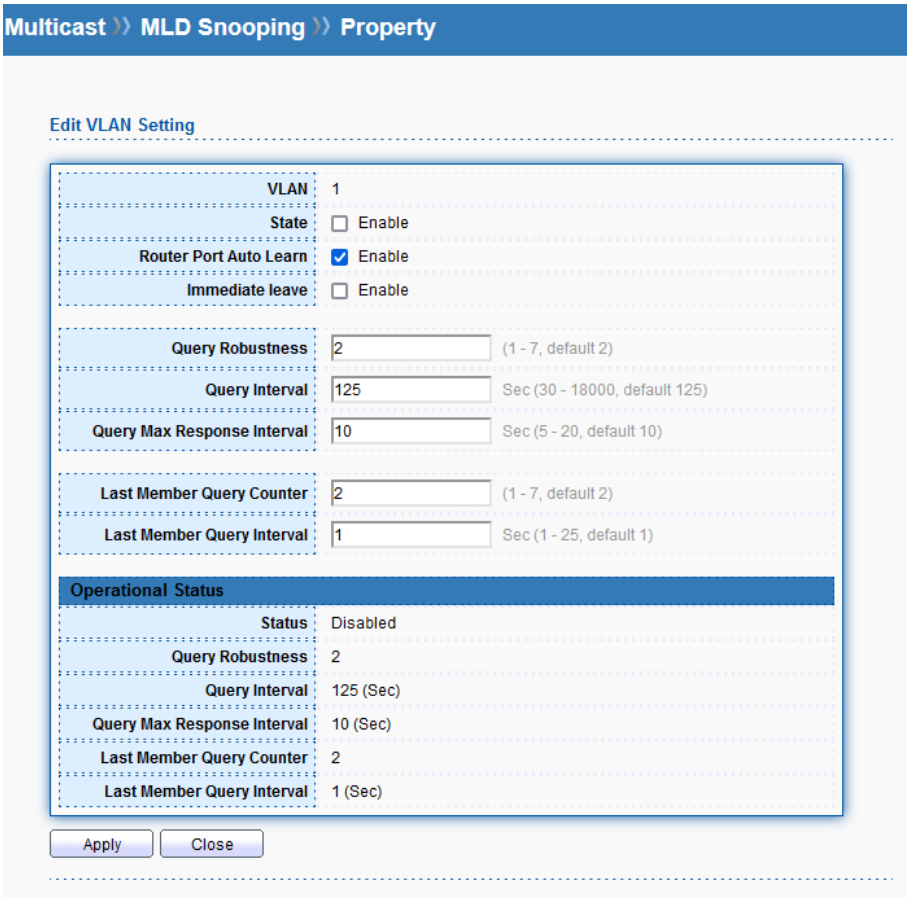
MLD snooping acts on IPv6 packets. MLD snooping is the process of listening to Multicast Listener Discovery network traffic. It can examine IPv6 packets and forward these packets to designate location via VLAN port members.

13.3.1 Property

This page allows to enable/disable MLD Snooping function, select snooping version, and enable/disable snooping report suppression.



Item	Description
State	Enable or disable the MLD snooping function.
Version	**MLDv1**: When it is selected, Switch will detect packets controlled by MLDv1 and bridge the traffic to IPv6 destination defined with multicast address(es). **MLDv2**: When it is selected, Switch will detect packets controlled by MLDv2 and forward the traffic to destination defined with multicast address(es).
Report Suppression	Enable or disable the function to handle MLD reports between router and host, suppressing bandwidth used by MLD.
Apply	Apply the settings to the switch.
Edit	Edit the selected entry.

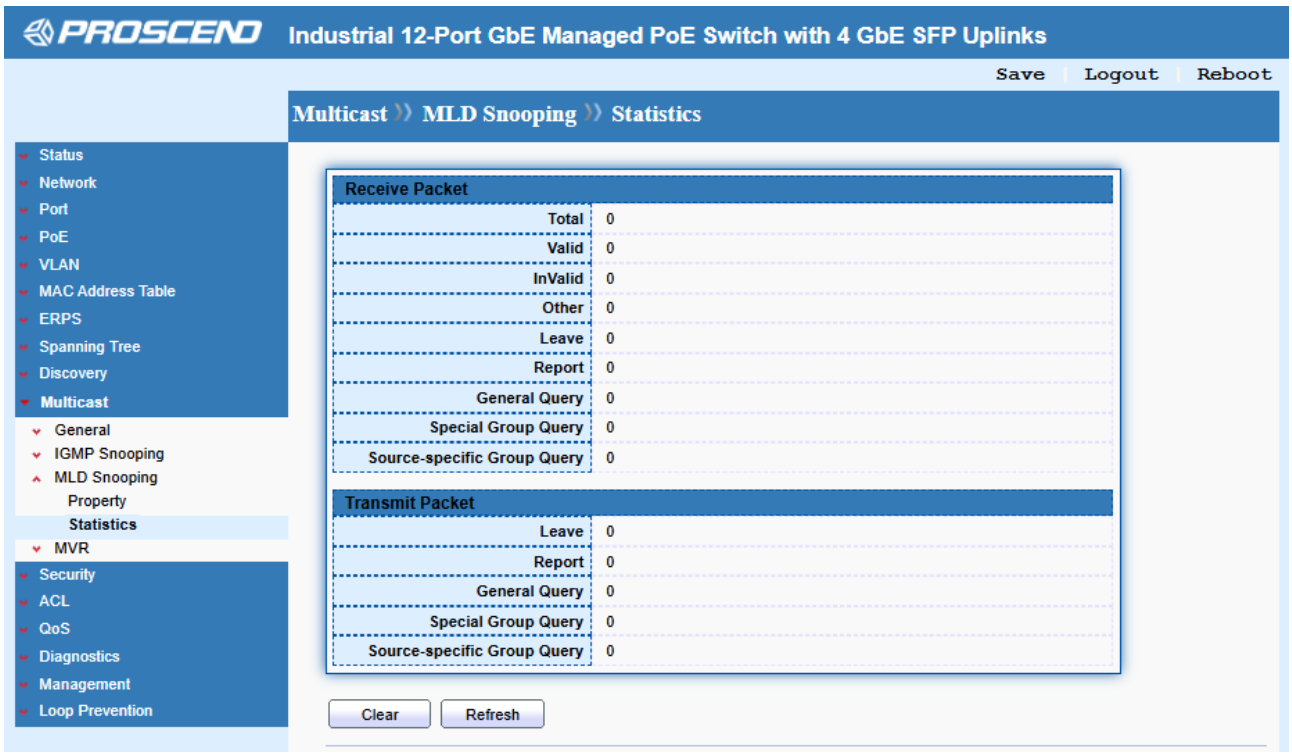


Item	Description
VLAN	The index number of VLAN entry.
State	Enable or disable the MLD snooping function for the selected VLAN ID.
Router Port Auto Learn	Enable or disable the function to handle MLD reports between router and host, suppressing bandwidth used by MLD.
Immediate Leave	Enable or disable the function of immediate leave. When the GE/LAG port receives the leave message, it will be removed from multicast group to speed up leave latency.
Query Robustness	Set a number which allows tuning for the expected packet loss on a subnet.
Query Interval	Specify the time interval for Switch to send out general MLD query to the host (responsible for responding).
Query Max Response Interval	Specify the maximum time interval for Switch to receive the query response from the host. If time is up and no response received, the packets will be blocked and discarded.
Last Member Query	After querying for specified times (defined here) and still not

Counter	receiving any response from the subscribed member, Switch will stop transmitting data to the related GE port(s).
Last Member Query Interval	The maximum time interval between counting each member query message with no responses from any subscribed member.
Operational Status	Display the current operational status.
Apply	Apply the settings to the switch.
Edit	Edit the selected entry.

13.3.2 Statistics

This page displays the statistics of MLD snooping.

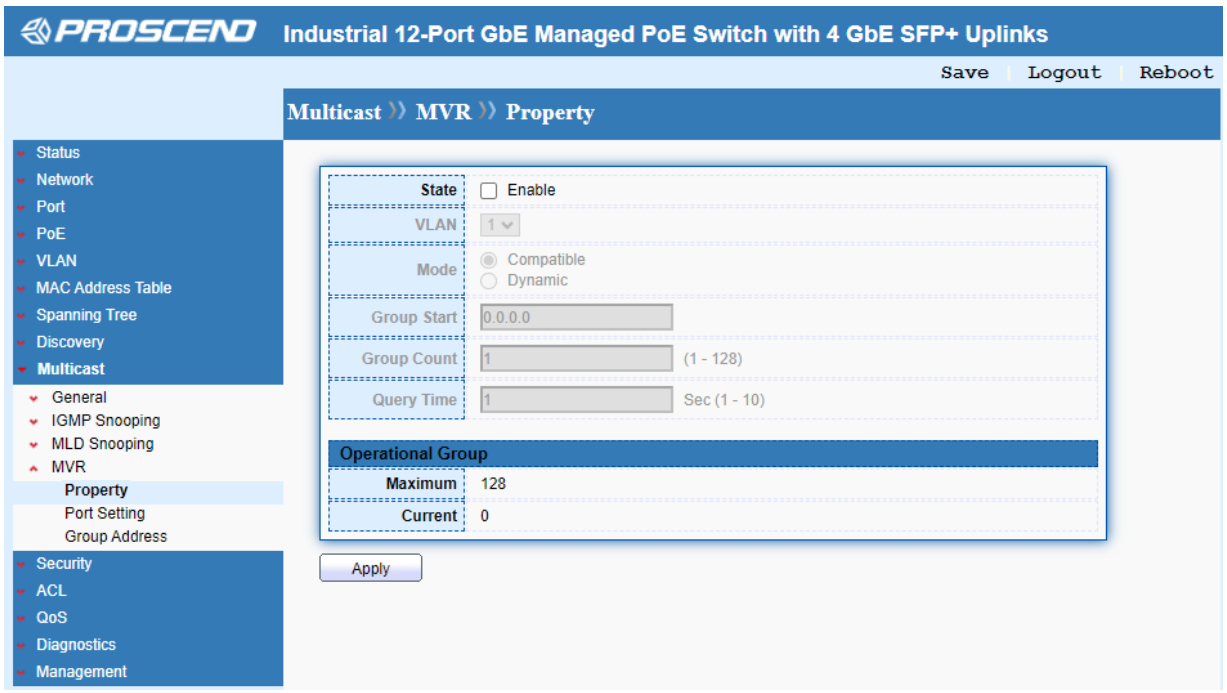


13.4 MVR

Multicast VLAN Registration (MVR) can route packets received in a multicast source VLAN to one or more destination VLANs. LAN users are in the destination VLANs and the multicast server is in the source VLAN. MVR can continuously send multicast stream for traffic in the multicast VLAN, but isolate the streams from the source VLANs for bandwidth and security reasons.

13.4.1 Property

This page allows the network administrator to configure general settings for MVR, such as enabling function, selecting VLAN ID (as source VLAN) and specify IP address(es) for receiver/LAN users.

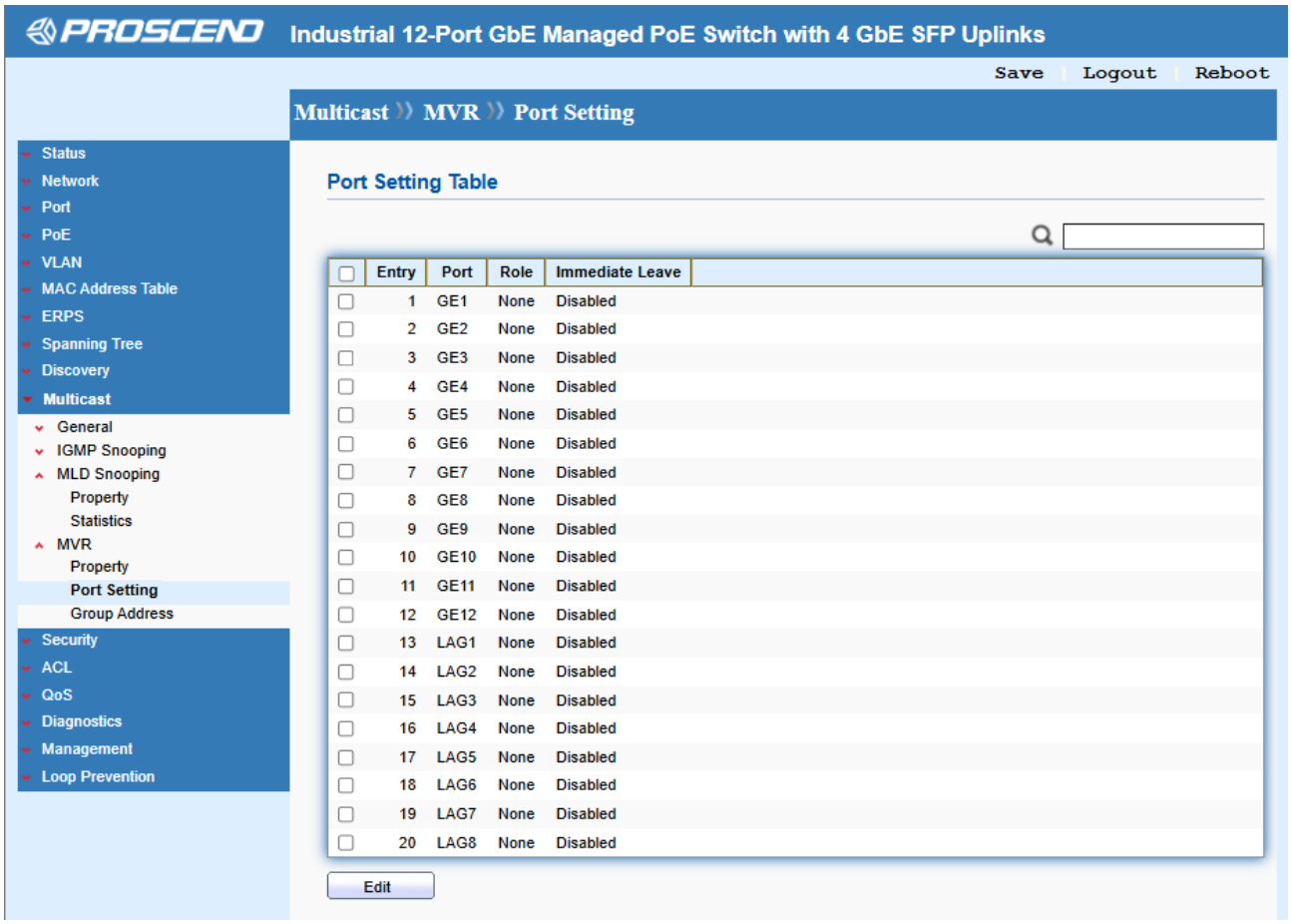


Item	Description
State	Enable or disable the MVR function.
VLAN	Choose one VLAN profile from the drop down list as multicast source VLAN which will receive multicast data. The default is VLAN 1.
Mode	**Compatible**: Multicast data received by MVR hosts (multicast server) will be forwarded to all MVR receiver ports. **Dynamic**: Multicast data received by MVR hosts (multicast server) on Switch will be forwarded from those MVR data and client ports grouped under MVR server.
Group Start	Enter an IP address. Any multicast data sent to this IP address will be sent to all source ports on Switch; and all receiver ports will accept /receive data from that multicast address.

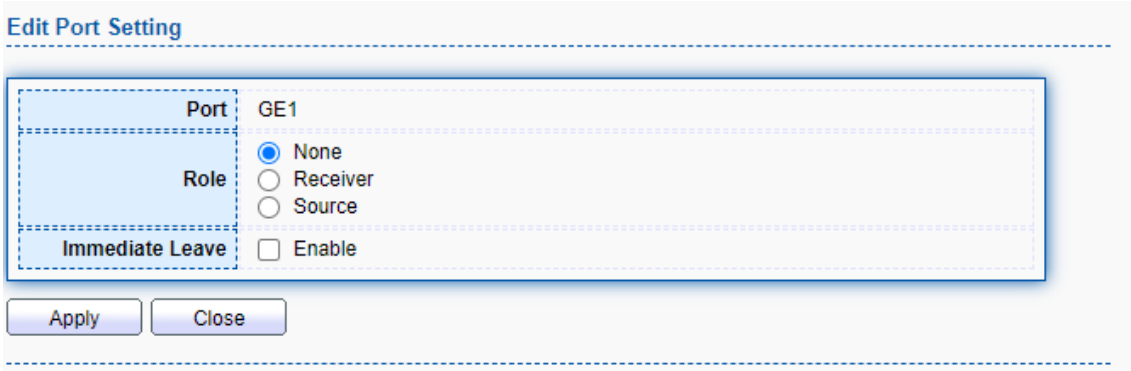
Group Count	Select a number to configure a contiguous series of MVR group addresses (the range for count is 1 to 128; the default is 1).
Query Time	Enter the value of the maximum time (1 – 10 seconds) to wait for IGMP report members on a receiver port before the port is removed from multicast group.
Operational Group	Display the current operational group.
Apply	Apply the settings to the switch.

13.4.2 Port Setting

It is necessary to specify destination port and source port (GE/LAG) for system to perform MVR operation.



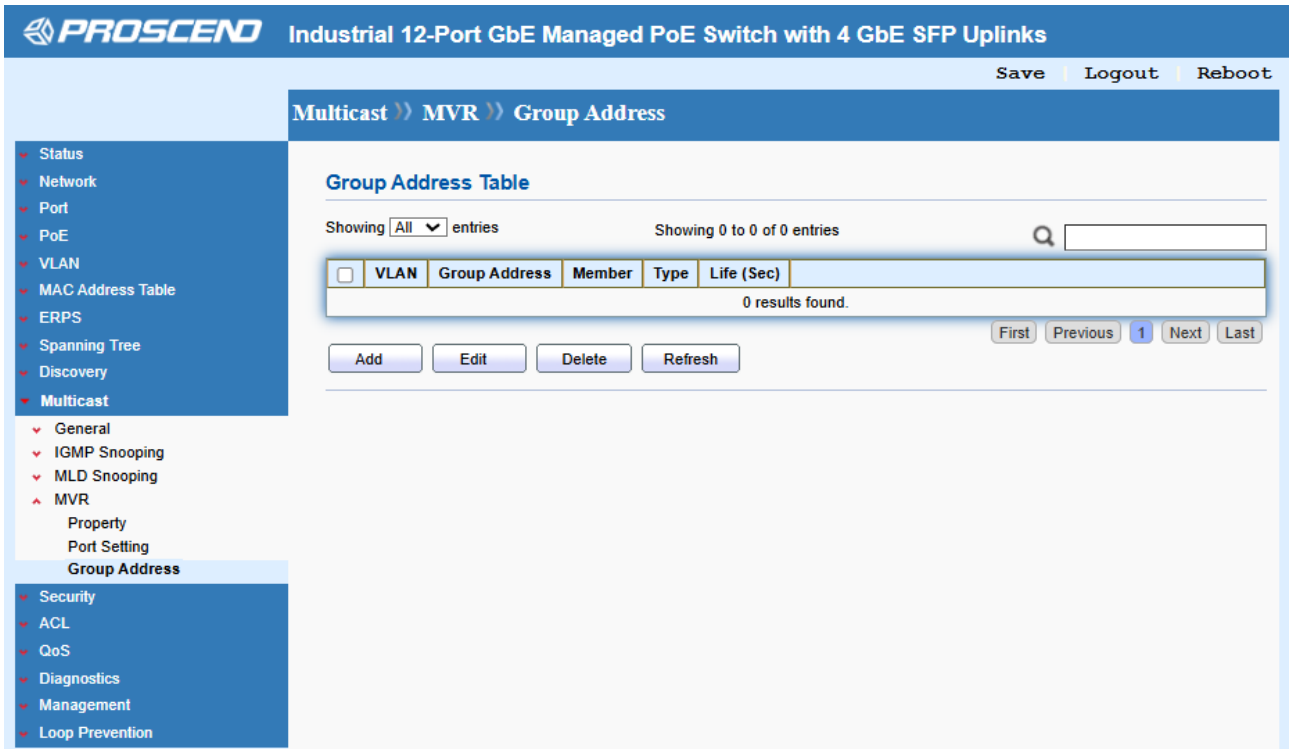
Item	Description
Edit	Edit the selected entry.



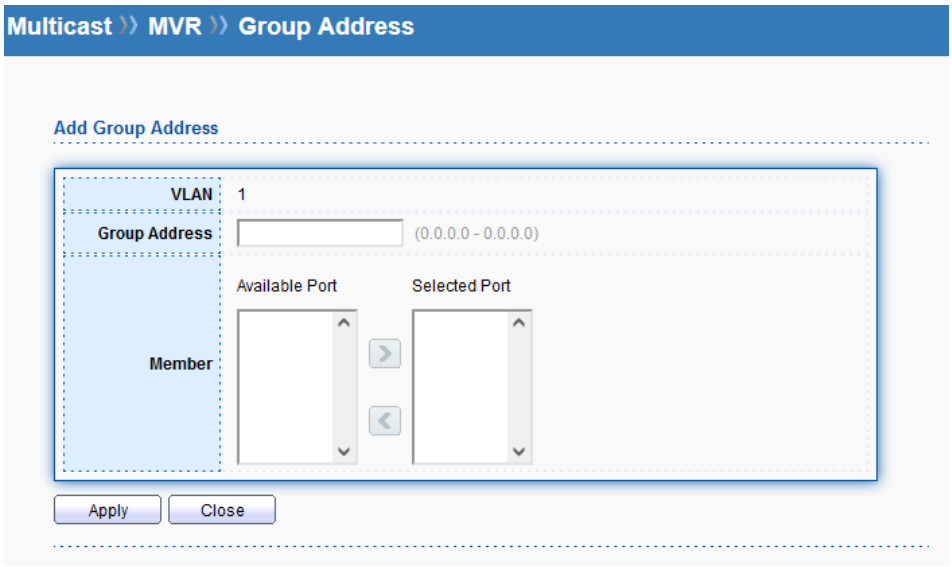
Item	Description
Port	The index number of selected port.
Role	**None**: Noting will be happed to the selected LAN port in MVR operation. **Receiver**: The selected port will be treated as destination port which will receive multicast data from the multicast server. **Source**: The selected port will be treated as source port which will send multicast data to the receiver port.
Immediate Leave	Enable or disable the function of immediate leave.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

13.4.3 Group Address

This page allows to configure IP address and specify port member for VLAN selected in **MVR** ➔**Property** page.



Item	Description
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the selected entry.
Refresh	Refresh the MVR Group Address table.

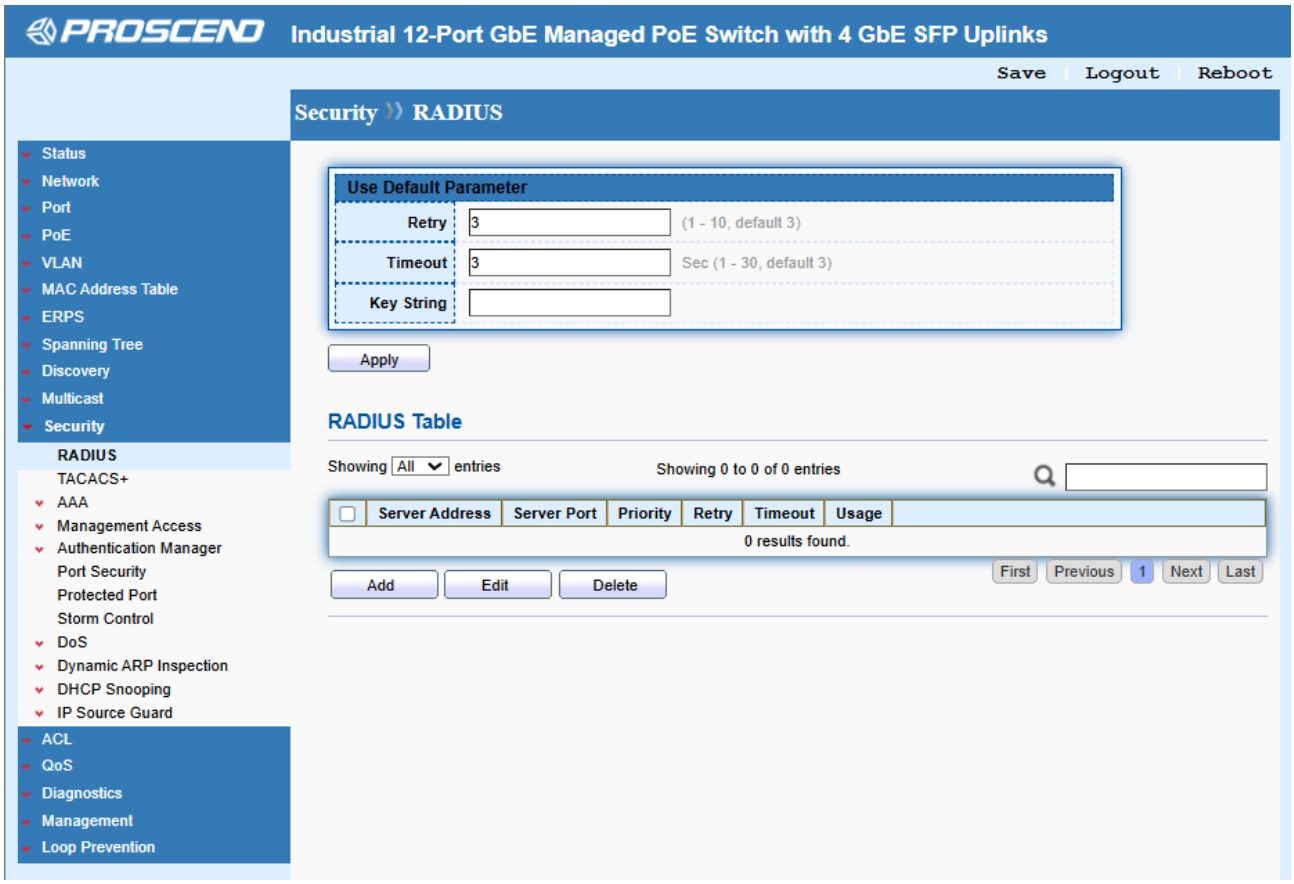


Item	Description
VLAN	The index number of selected VLAN ID.
Group Address	Define a range of IP address(es) with the format of “xxx.xxx.xxx.xxx – xxx.xxx.xxx.xxx”.
Member	Choose GE/LAG port to be grouped under the selected VLAN.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

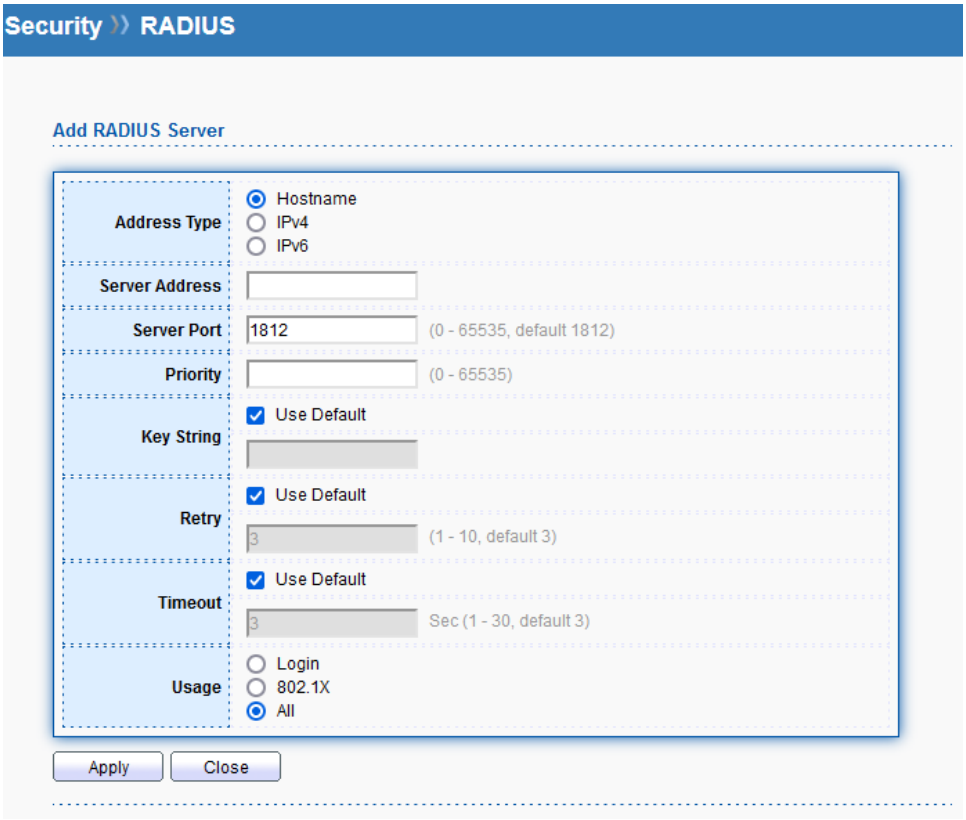
14 Security

14.1 RADIUS

This page allows to add and configure multiple RADIUS servers.



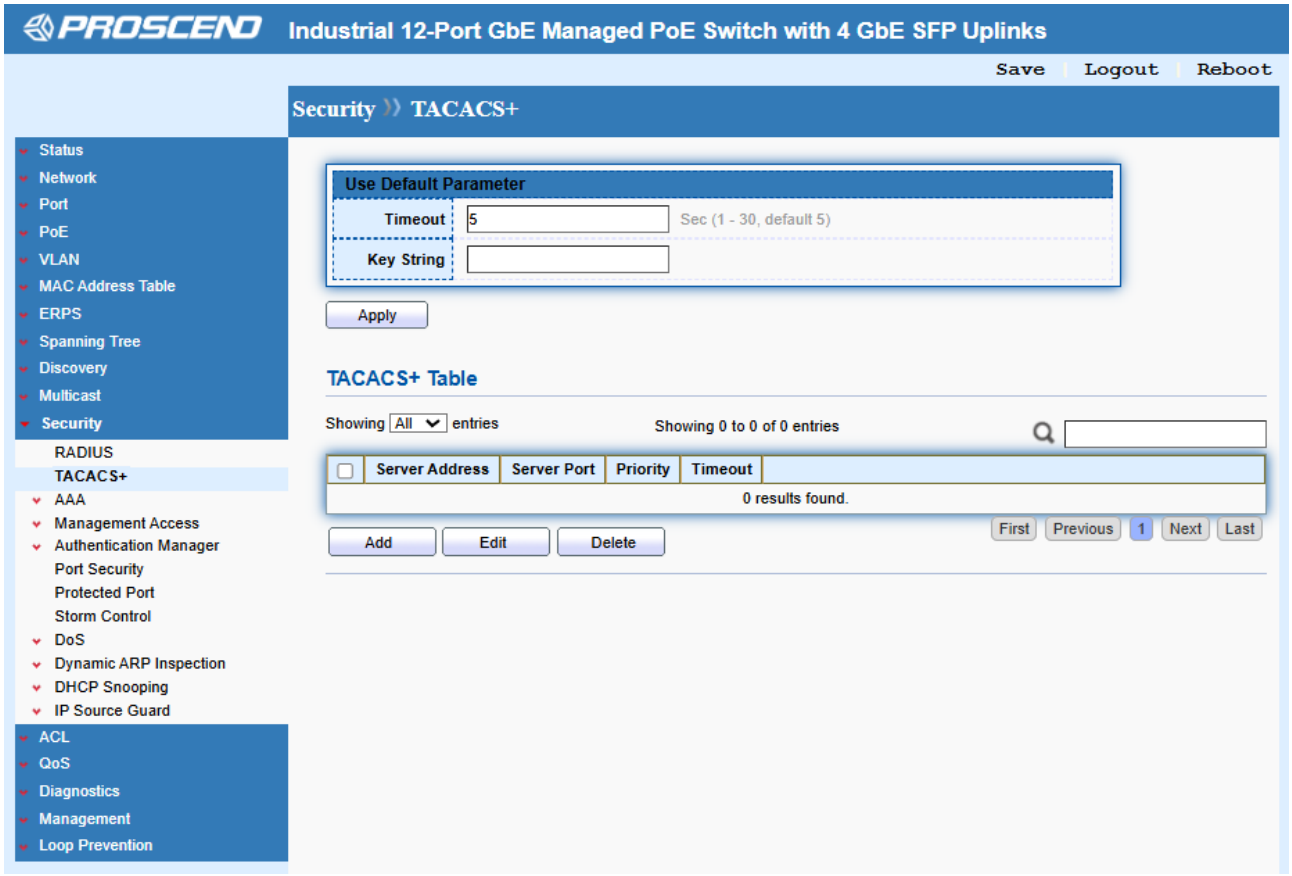
Item	Description
Retry	The retry time before the server being considered not reachable.
Timeout	Set the time (in seconds) before the server being considered lost connection.
Key String	Enter the string used to encrypt and authenticate with RADIUS server.
Apply	Apply the settings to the switch.
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the selected entry.



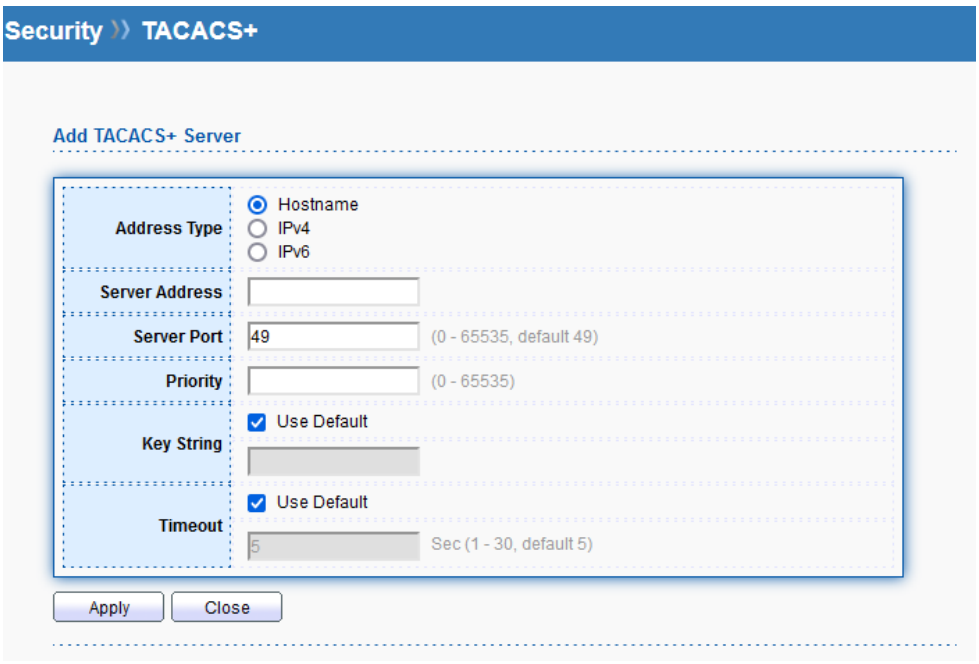
Item	Description
Address Type	Specify whether switch uses a hostname to resolve address by DNS to connect to server, or directly connect using IPv4 address.
Server Address	Enter the server's address corresponding with address type given.
Server Port	Enter the port number used by RADIUS server.
Priority	Specify the priority that switch uses this server. The higher number, the lower priority. Switch will start with lowest priority.
Key String	Enter the key string used for encrypting and authenticating with server.
Retry	The retry time before the server being considered not reachable.
Timeout	Set the time (in seconds) before the server being considered lost connection.
Usage	Specify whether you would like to use this server for switch login authentication or 802.1x access port authentication, or both.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

14.2 TACACS+

This page allows to add and configure multiple TACACS+ server.



Item	Description
Timeout	Set the time (in seconds) before the server being considered lost connection.
Key String	Enter the string used to encrypt and authenticate with RADIUS server.
Apply	Apply the settings to the switch.
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the selected entry.

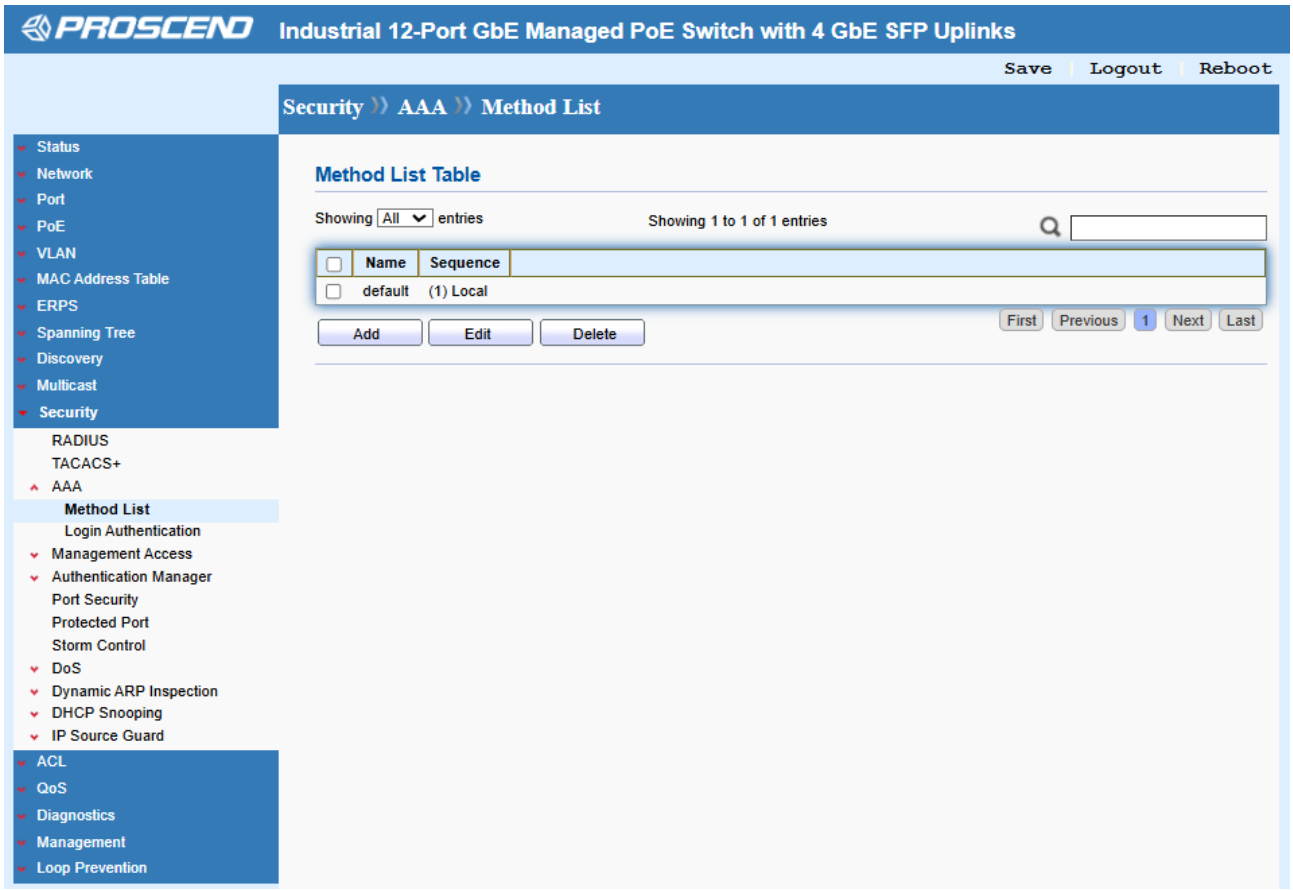


Item	Description
Address Type	Specify whether switch uses a hostname to resolve address by DNS to connect to server, or directly connect using IPv4 address.
Server Address	Enter the server's address corresponding with address type given.
Server Port	Enter the port number used by TACACS+ server.
Priority	Specify the priority that switch uses this server. The higher number, the lower priority. Switch will start with lowest priority.
Key String	Enter the key string used for encrypting and authenticating with server.
Timeout	Set the time (in seconds) before the server being considered lost connection.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

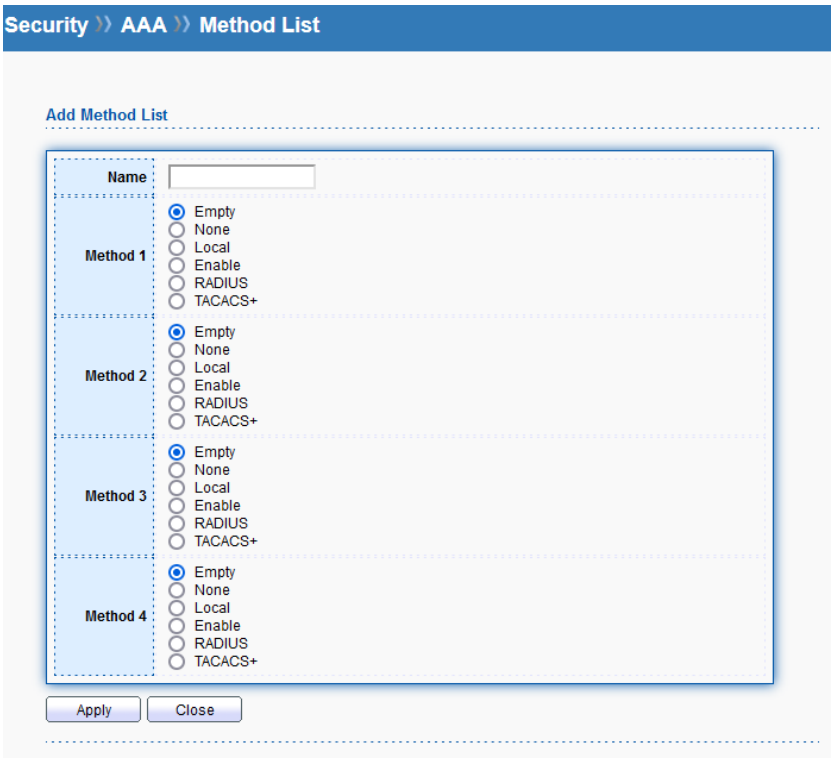
14.3 AAA

14.3.1 Method List

This page allows to create method list for applying on management service.



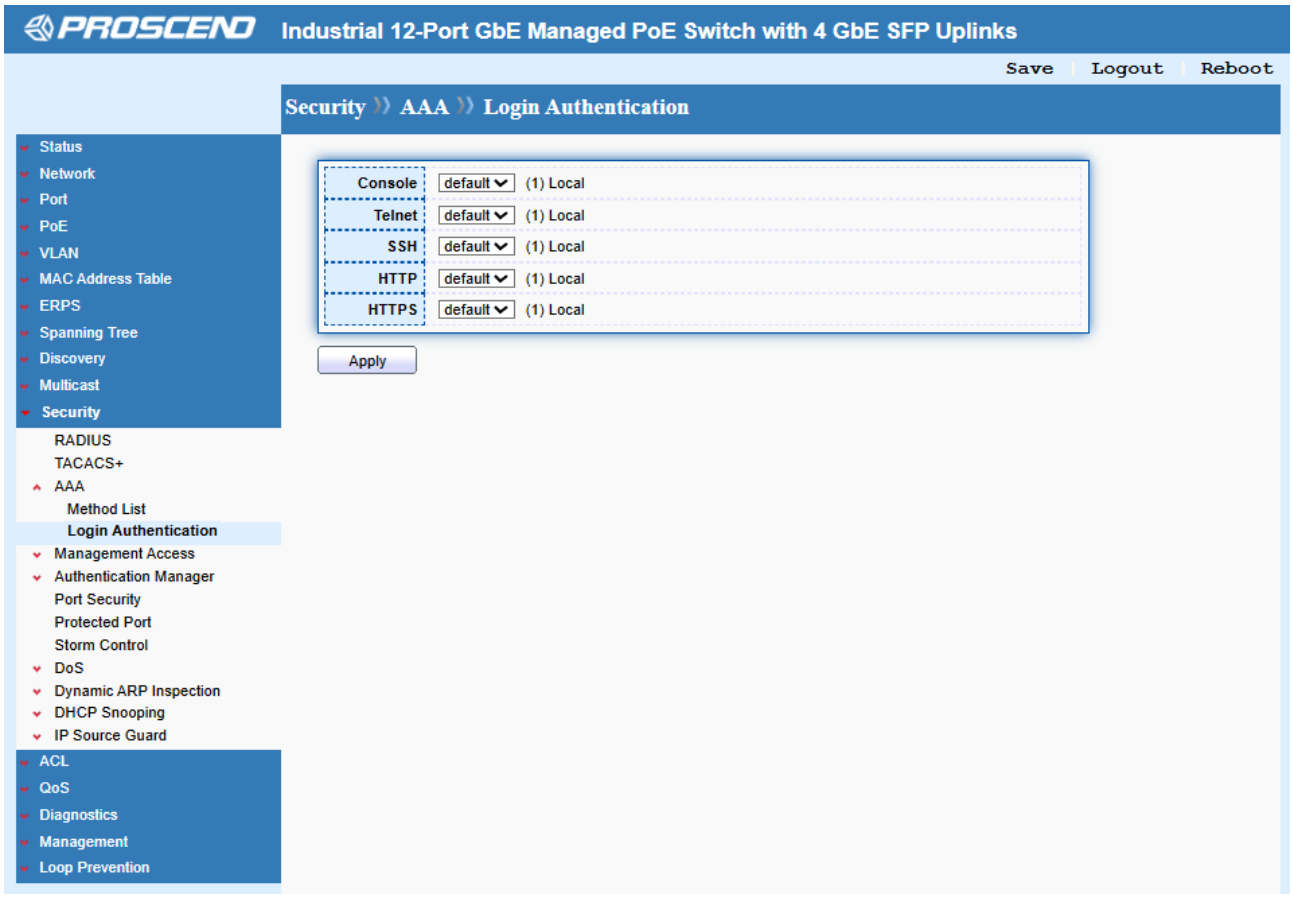
Item	Description
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the selected entry.



Item	Description
Name	Enter a name for creating a method.
Method Profile	Available methods include Local, RADIUS and TACACS+.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

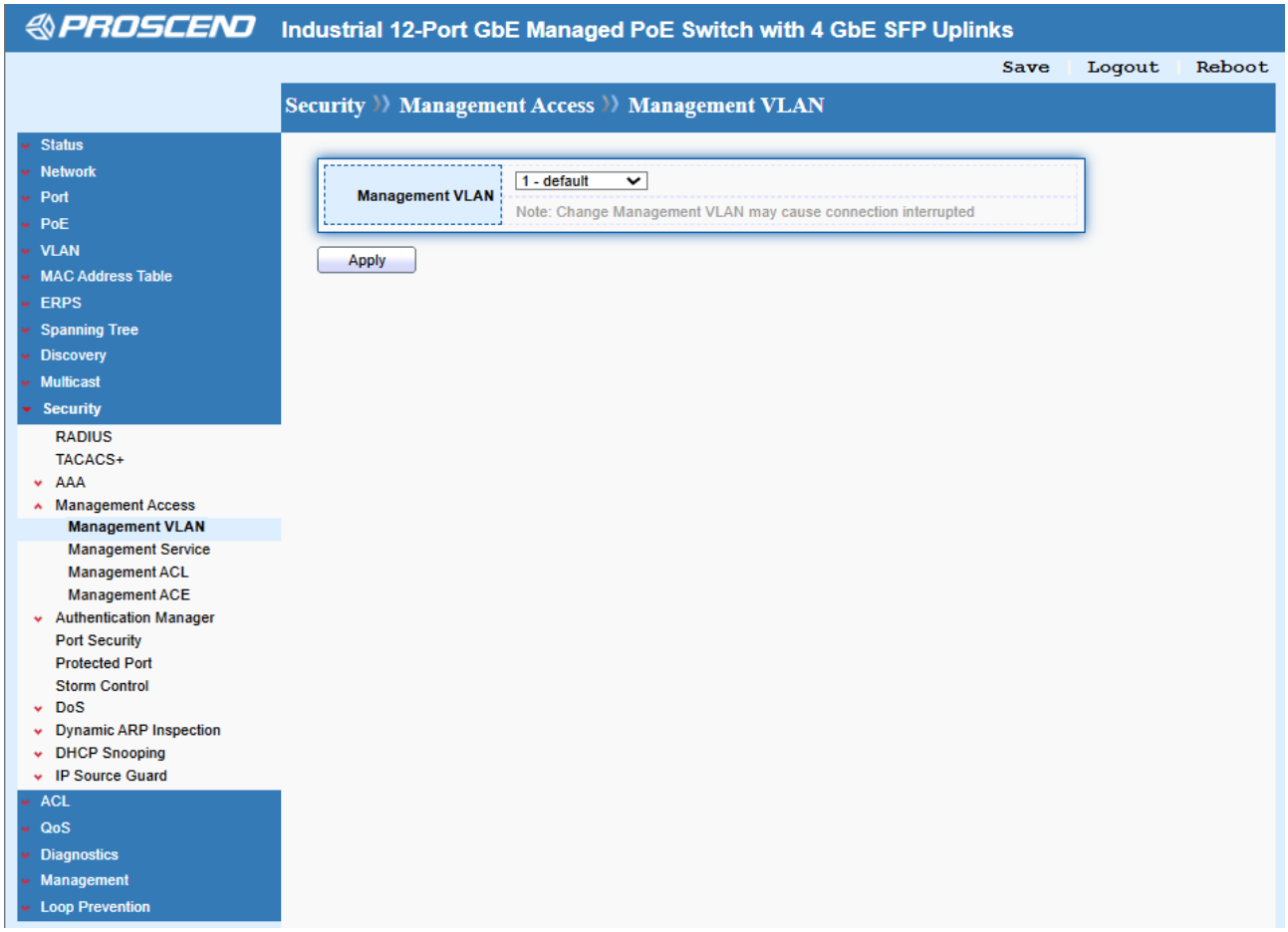
14.3.2 Login Authentication

This page allows to select created method profile for each management service.



14.4 Management Access

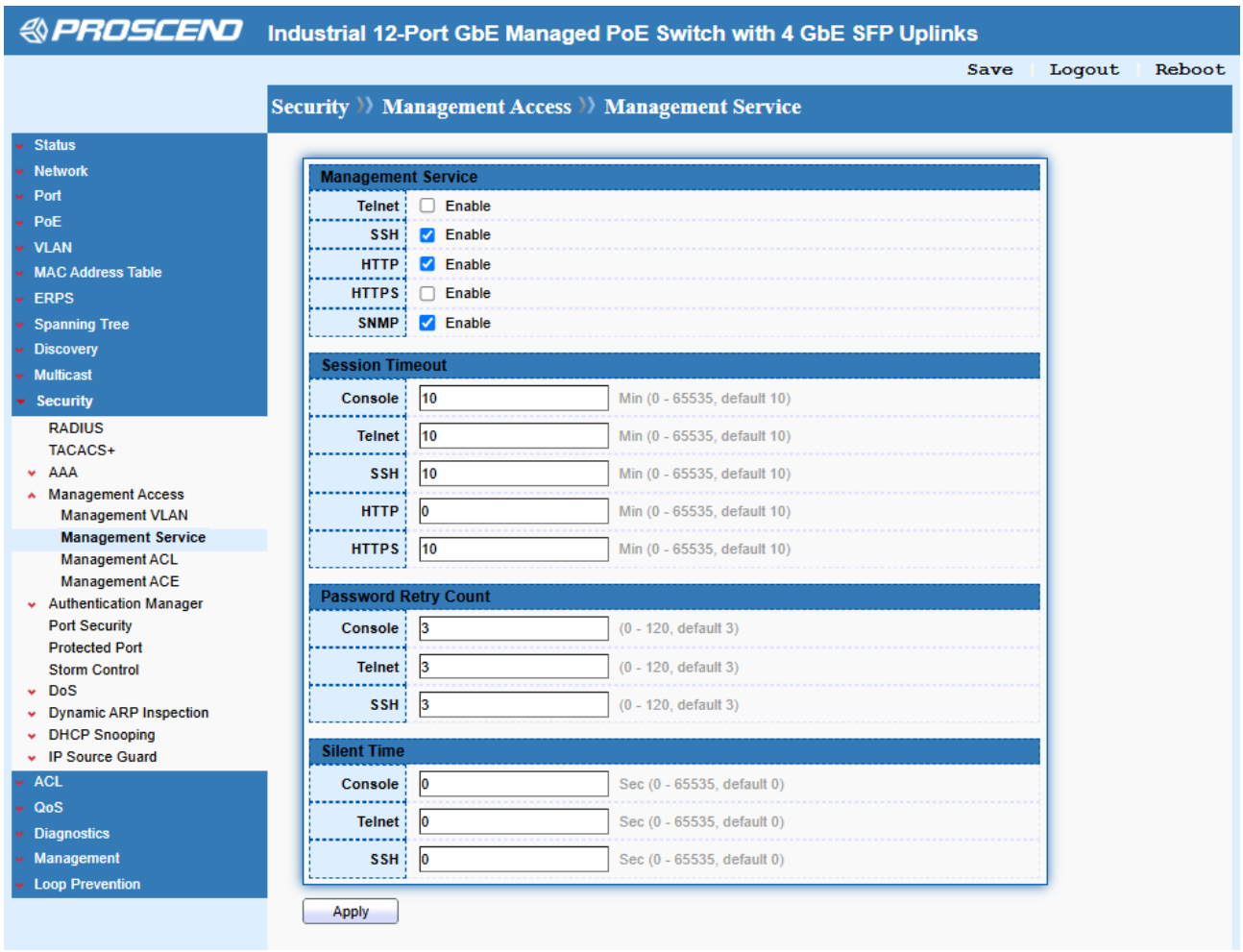
14.4.1 Management VLAN



Item	Description
Management VLAN	Select the VLAN ID that will be used for management.
Apply	Apply the settings to the switch.

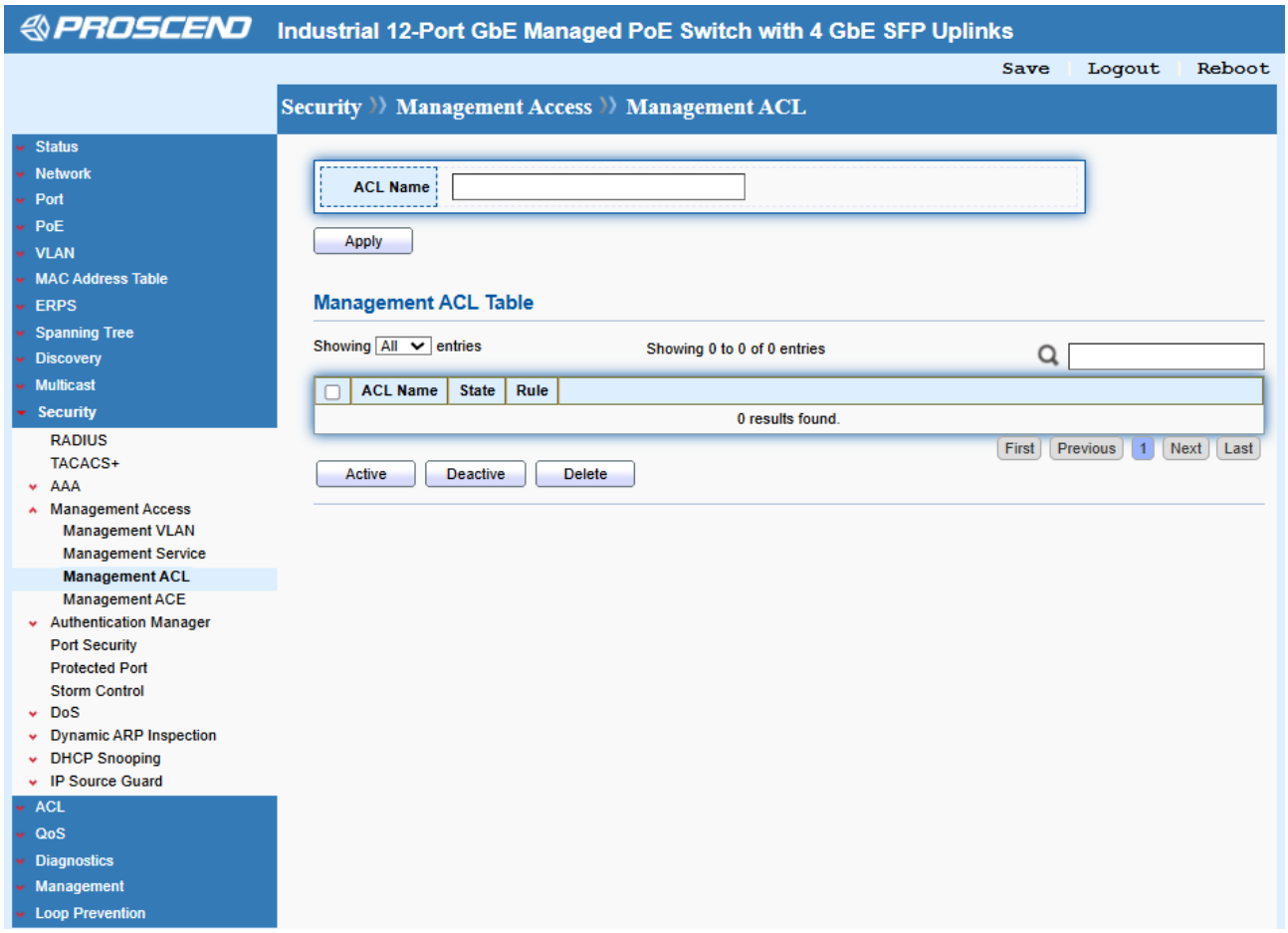
14.4.2 Management Service

This page allows to enable or disable the management service of Switch.



14.4.3 Management ACL

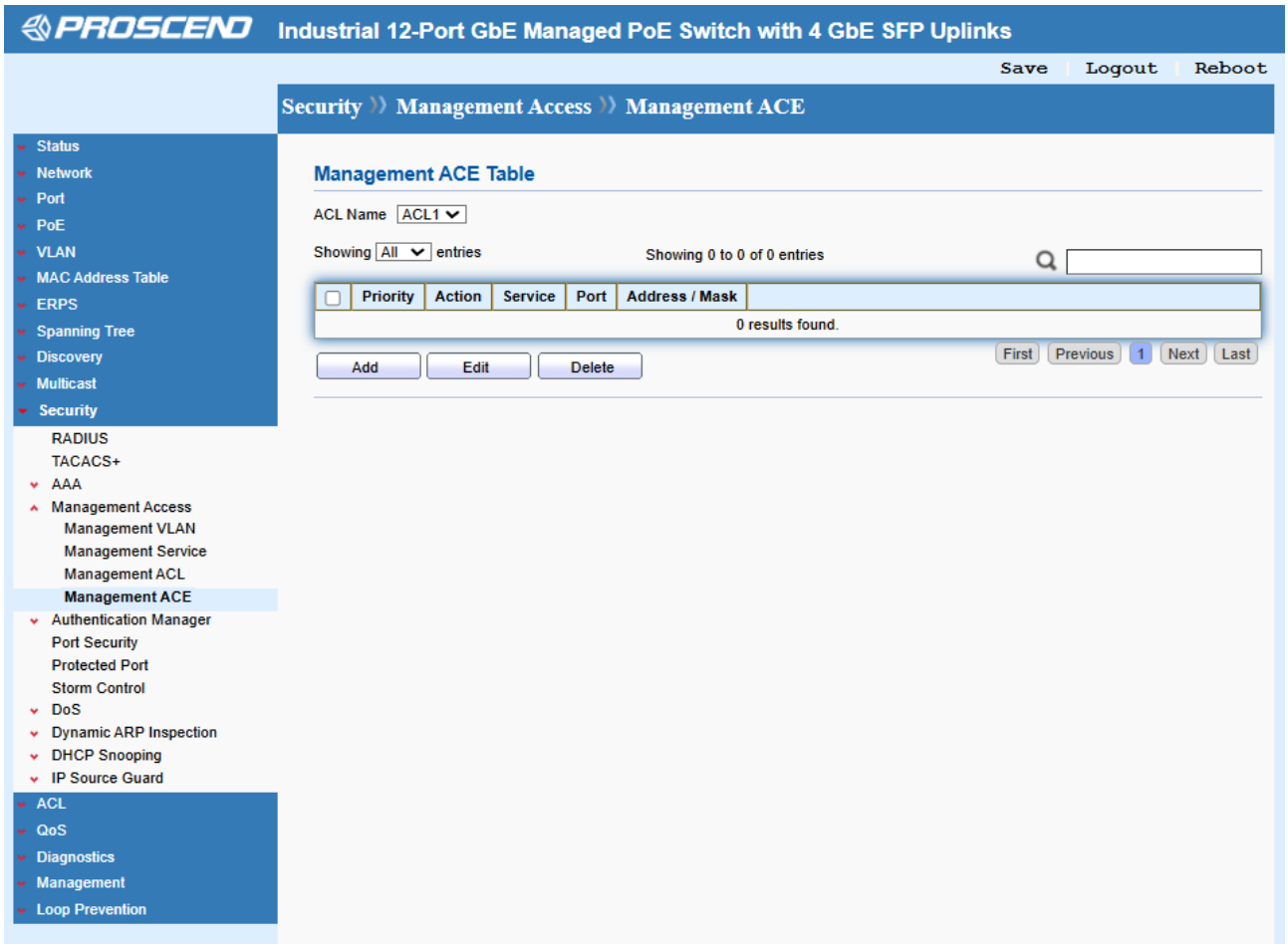
This page allows to add, edit, and delete Management Access Control profiles.



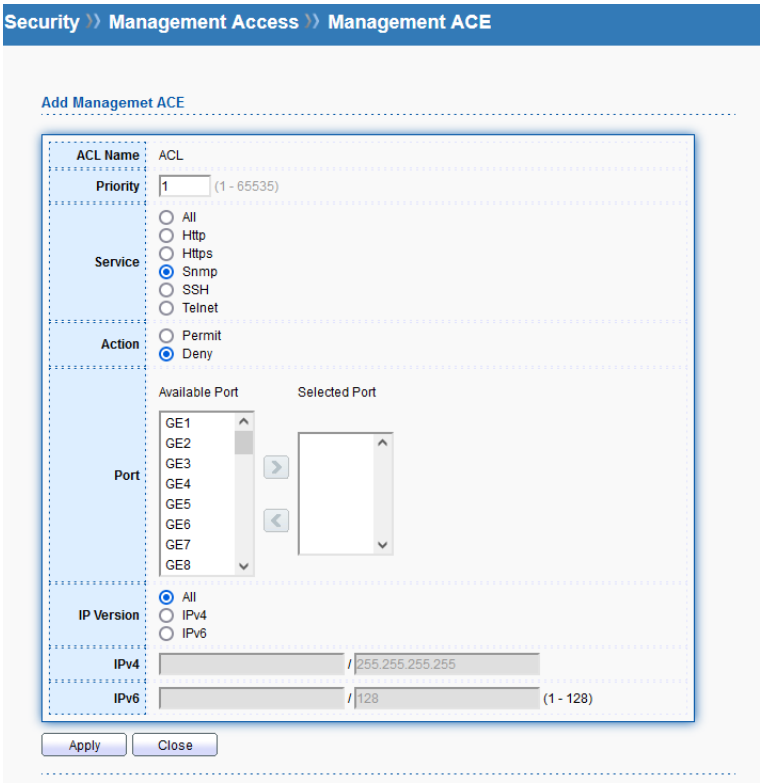
Item	Description
ACL Name	Enter a name to create a profile for ACL.
Apply	Apply the settings to the switch.
Active	Activate the selected entry.
Deactive	Deactivate the selected entry.
Delete	Delete the selected entry.

14.4.4 Management ACE

This page allows to add, edit, or remove Access Control Entries (ACE) of the Management Access Control profiles. However, only the ACE of inactive profiles can be modified, and before configuring ACE, at least one ACL profile should be created.



Item	Description
ACL Name	Use the drop-down list to select the inactive ACL profile you would like to modify.
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the selected entry.



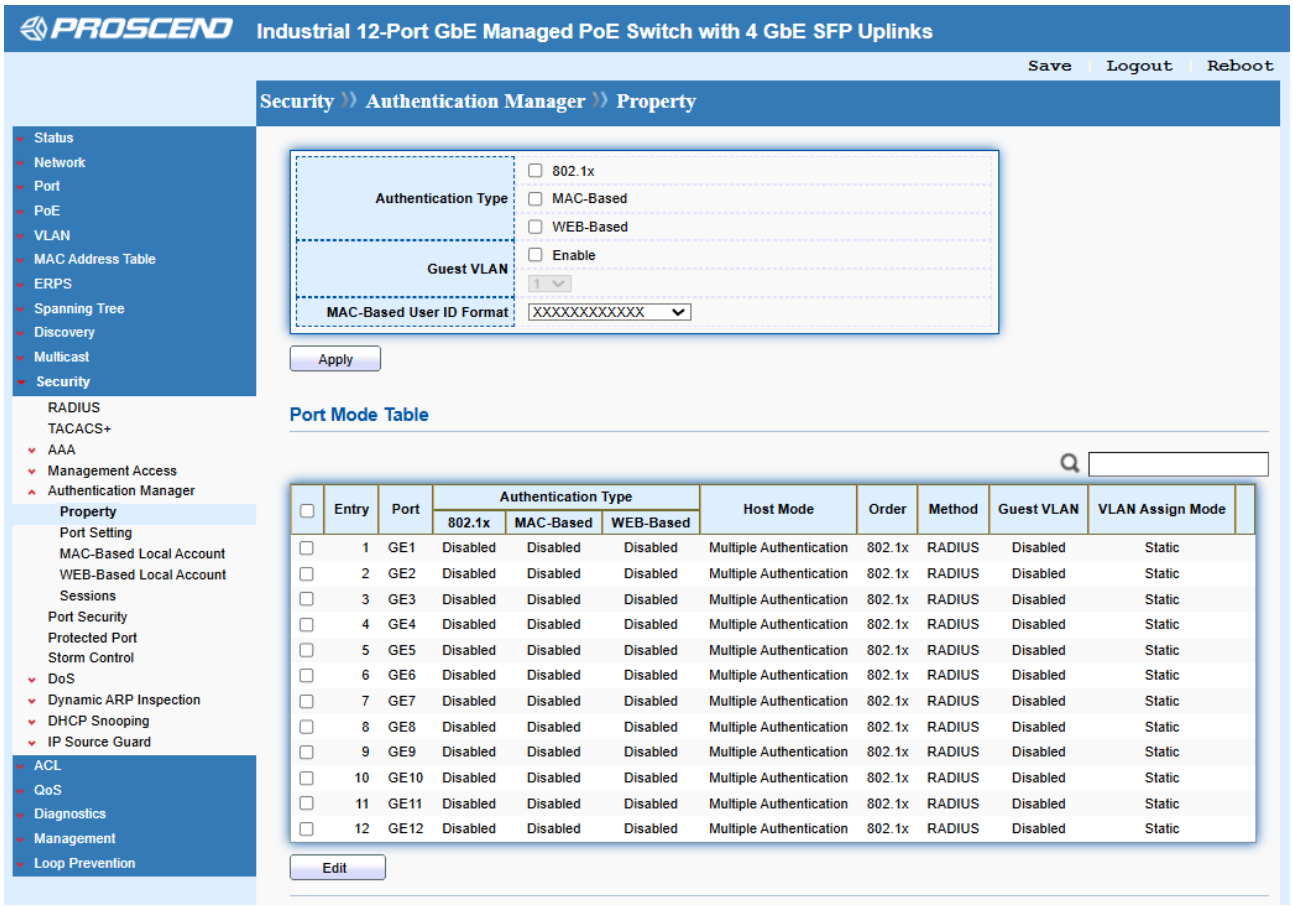
Item	Description
ACL Name	The name of selected profile.
Priority	Specify a priority number (1 to 65535) for such rule. The lower the number, the higher the priority.
Service	Choose the service type you would like to control the access.
Action	**Permit**: Incoming / outgoing data which meets ACE rule is allowed to pass through. **Deny**: Incoming / outgoing data which meets ACE rules will be blocked.
Port	Select the ports to which the ACL should be applied.
IP Version	**All**: All the IP address should be applied. **IPv4**: Specify the IPv4 address / subnet. **IPv6**: Specify the IPv6 address / subnet.
IPv4	Enter the IPv4 address / subnet to which the ACE rule should apply.
IPv6	Enter the IPv6 address / subnet to which the ACE rule should apply.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

14.5 Authentication Manager

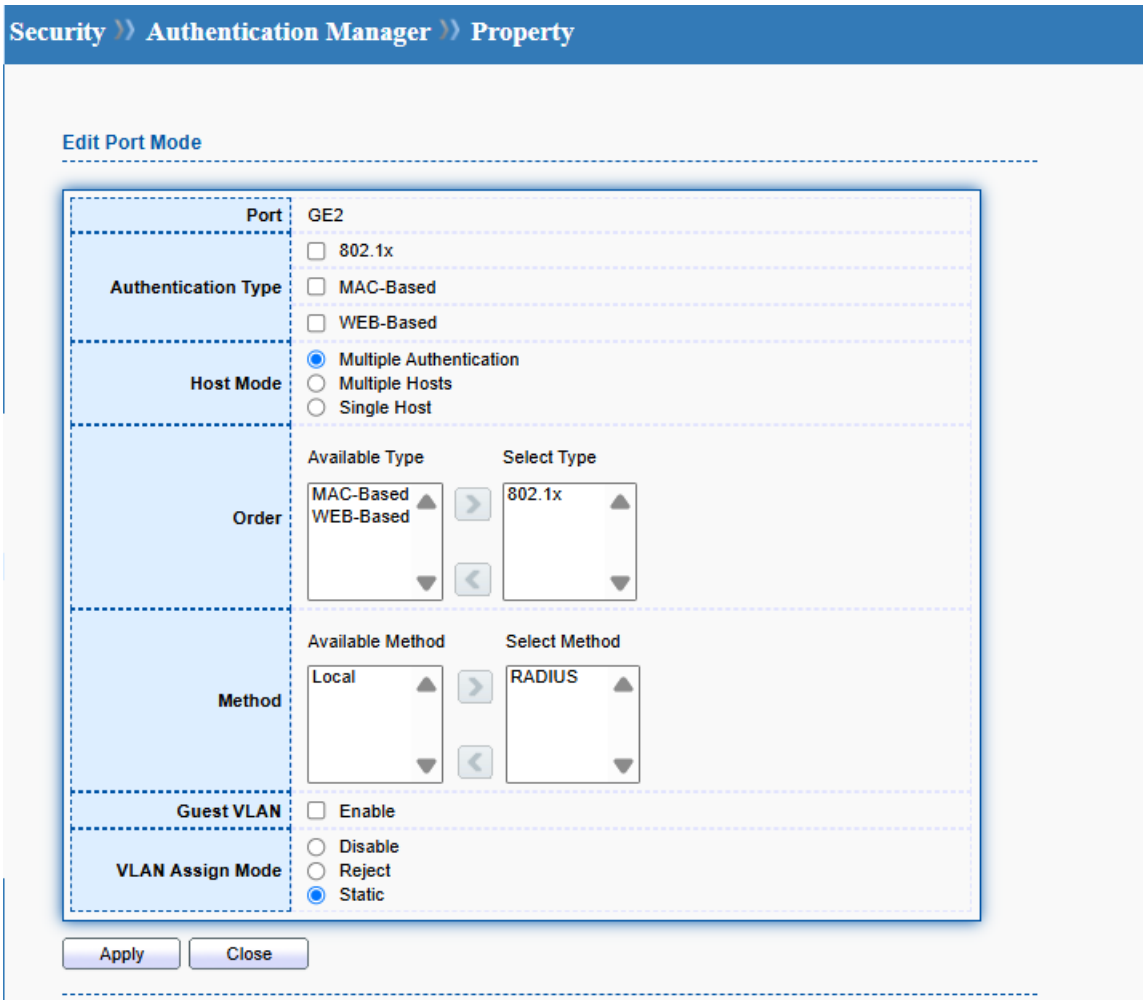
The authentication manager allows you to configure securely access from any host connected to physical ports. You may apply multiple ways of authentication to each port.

14.5.1 Property

The switch supports 802.1x and MAC-based authentication methods. In Global Settings page, you can specify authentication type, enable Guest VLAN function, specify a VID and select format for MAC address entry.



Item	Description
Authentication Type	Specify the type that will be used for authentication.
Guest VLAN	Check to enable a Guest VLAN for those have not successfully authenticated with any given methods. Choose one of the VLAN ID as a Guest VLAN.
MAC-Based User ID Format	Specify how the MAC-based user ID should be expressed in EAP message between AAA server and switch.
Apply	Apply the settings to the switch.
Edit	Edit the selected port(s).

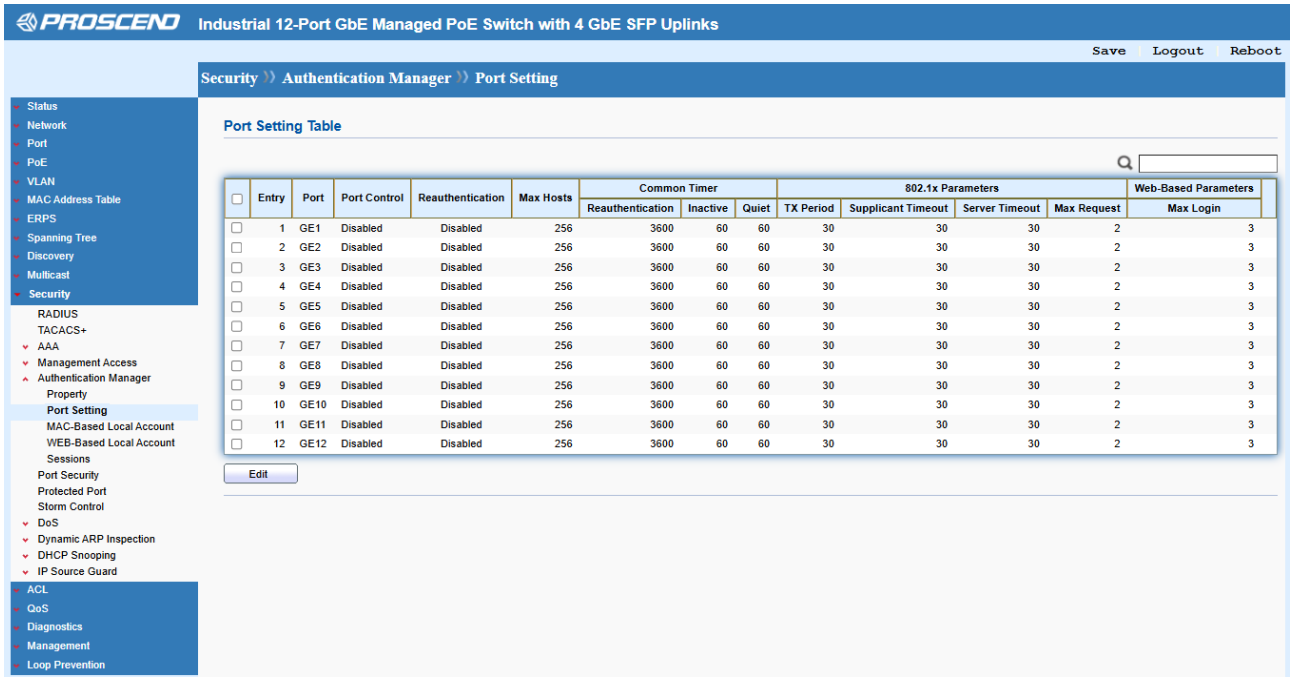


Item	Description
Port	The index number of selected port.
Authentication Type	Specify the type that will be used for authentication.
Host Mode	**Multiple Authentication**: Each host are authenticated individually. **Multiple Hosts**: Authentication is done on port basis, only one authenticated host is required; other hosts connected to this port can access freely as authenticated host. **Single Host**: Only one host can be authenticated, and access the port.
Order	Specify available authentication types of AAA server (or local) you wish to have on this port.
Method	Specify available methods of AAA server (or local) you wish to have

	on this port.
Guest VLAN	Check Enable to enable Guest VLAN on this port for those unauthenticated traffic.
VLAN Assign Mode	**Disable**: Switch will ignore the VLAN assignment from the RADIUS server and keep the original VLAN of the host. **Reject**: Switch will reject the host if it does not receive the VLAN information from RADIUS server. **Static**: Switch will use the VLAN assignment from the RADIUS server if it receives the information. If there is no VLAN information, it will keep the original VLAN of the host.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

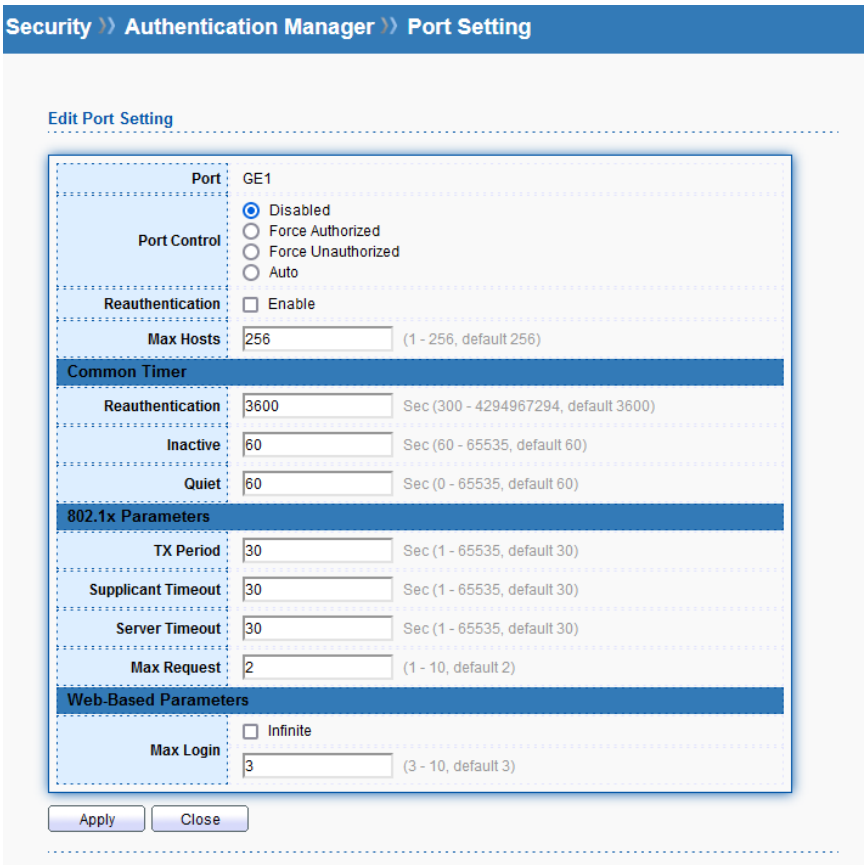
14.5.2 Port Setting

This page allows to controls port setting, based on 802.1X, for Ethernet port authentication.



Entry	Port	Port Control	Reauthentication	Max Hosts	Common Timer			802.1x Parameters				Web-Based Parameters
					Reauthentication	Inactive	Quiet	TX Period	Supplicant Timeout	Server Timeout	Max Request	Max Login
1	GE1	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
2	GE2	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
3	GE3	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
4	GE4	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
5	GE5	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
6	GE6	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
7	GE7	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
8	GE8	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
9	GE9	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
10	GE10	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
11	GE11	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
12	GE12	Disabled	Disabled	256	3600	60	60	30	30	30	2	3

Item	Description
Edit	Edit the selected port(s).

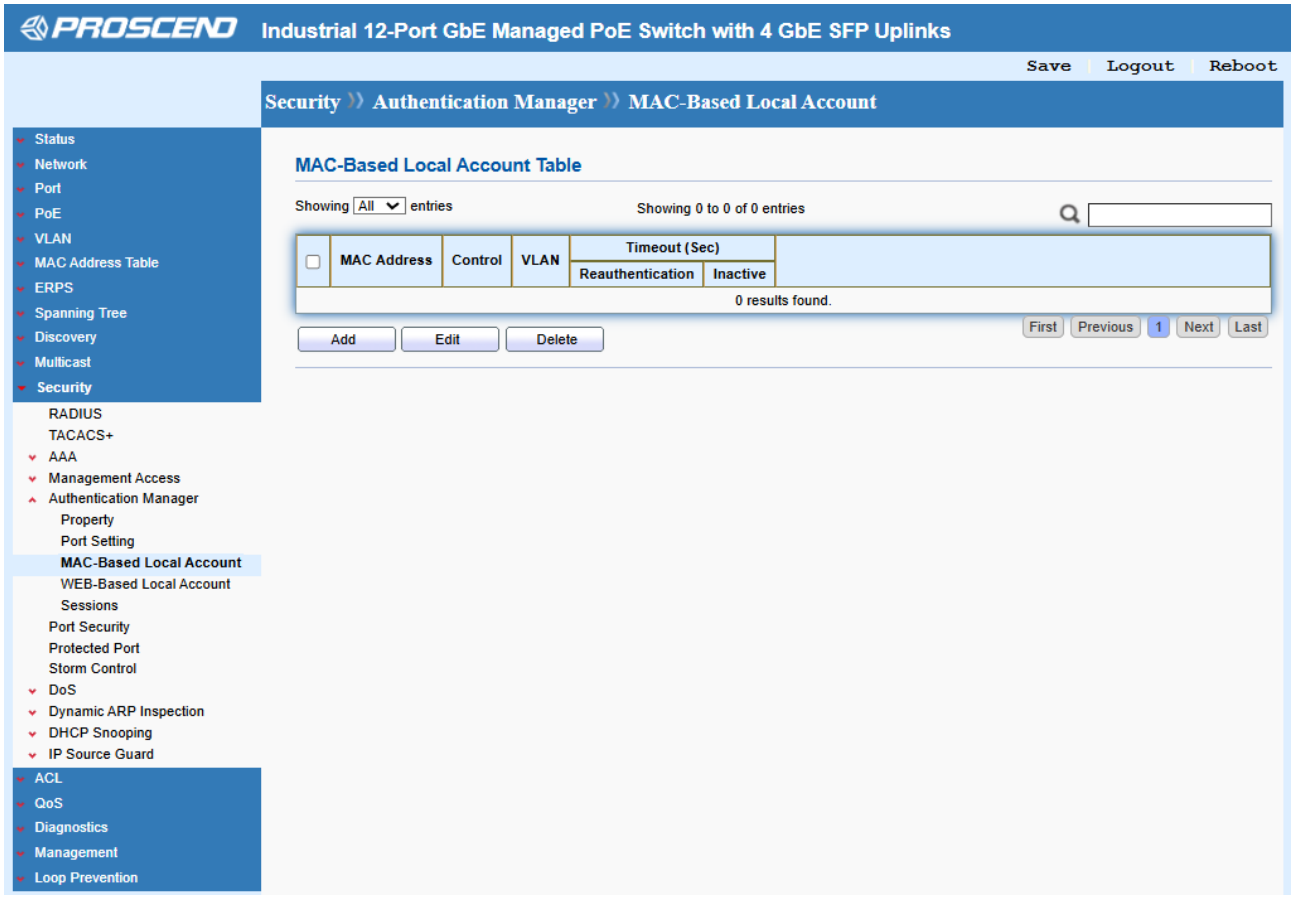


Item	Description
Port	The index number of selected port.
Port Control	**Disabled**: Disable any authentication requirement for port access. All clients are allowed to access the network. **Force Authorized**: Port will be considered authorized. All clients are allowed to access the network. **Force Unauthorized**: Port will be considered un-authorized. All clients are NOT allowed to access the network. **Auto**: Port will be considered authorized or unauthorized based on the authentication results of the host.
Reauthentication	The hosts via the selected GE port will be re-authenticated periodically once it is enabled.
Max Hosts	If Multiple Authentication mode is selected as Host Mode, the total number of hosts cannot exceed the maximum number of hosts configured here.
Common Timer	
Reauthentication	Enter a time period. When the time is up, the host shall return to initial state and prepare to pass authentication procedure again.

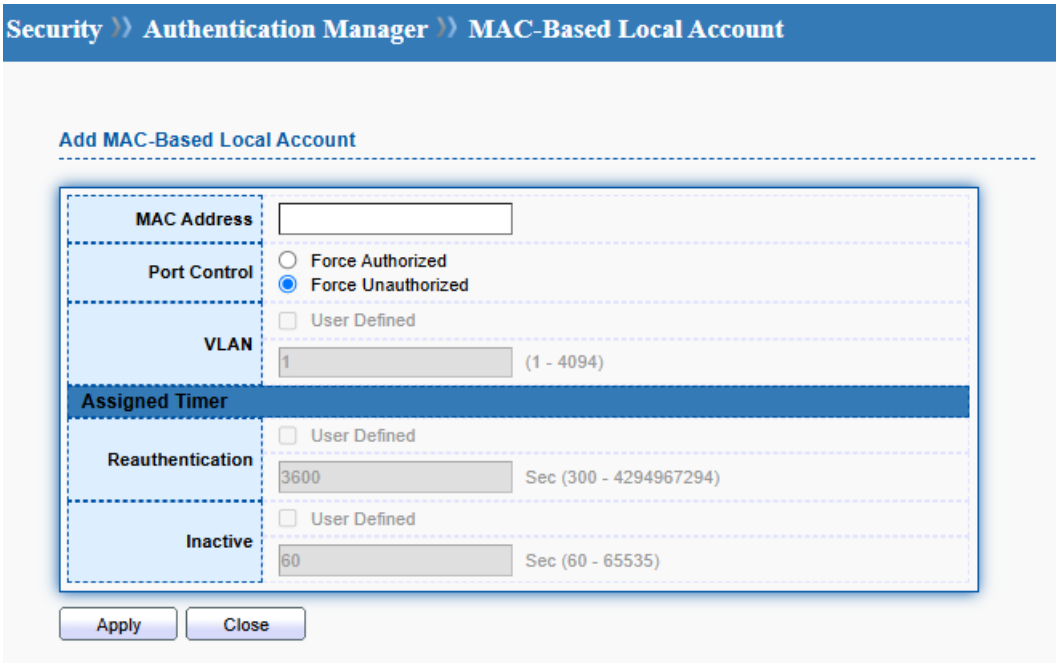
	Default is 3600 seconds.
Inactive	When there is no packet coming from the authenticated host, the system will start the inactive timer. After inactive timeout, the host will be unauthorized and corresponding session will be deleted. In Multiple Hosts mode, the packet is counted on the authorized host only and not all packets on the port.
Quiet	When a GE port is disabled just because authentication fails several times, the host connected to that port will be blocked for a period of time configured in quiet period. Later, after the time period set in this field, the host will be allowed to perform authentication again.
802.1x Parameters	
TX Period	Set the period for host to re-send EAP (Ethernet Automatic Protection) requests. Default value is 30 (seconds).
Supplicant Timeout	Set a period of time for the maximum number of EAP requests will be sent. If a response from the host is not received by Switch after the defined period (supplicant timeout), the authentication process will be started again.
Server Timeout	Set a period of time for the server. The EAP requests shall be resent to the supplicant within the time; otherwise, the time setting will lapse and the requests won't be sent out.
Max Request	Set the maximum time interval for EAP request sent out.
Web-Based Parameters	
Max Login	Set the maximum login request.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

14.5.3 MAC-Based Local Account

This page allows to create profiles by entering MAC address of the hosts to be authenticated.



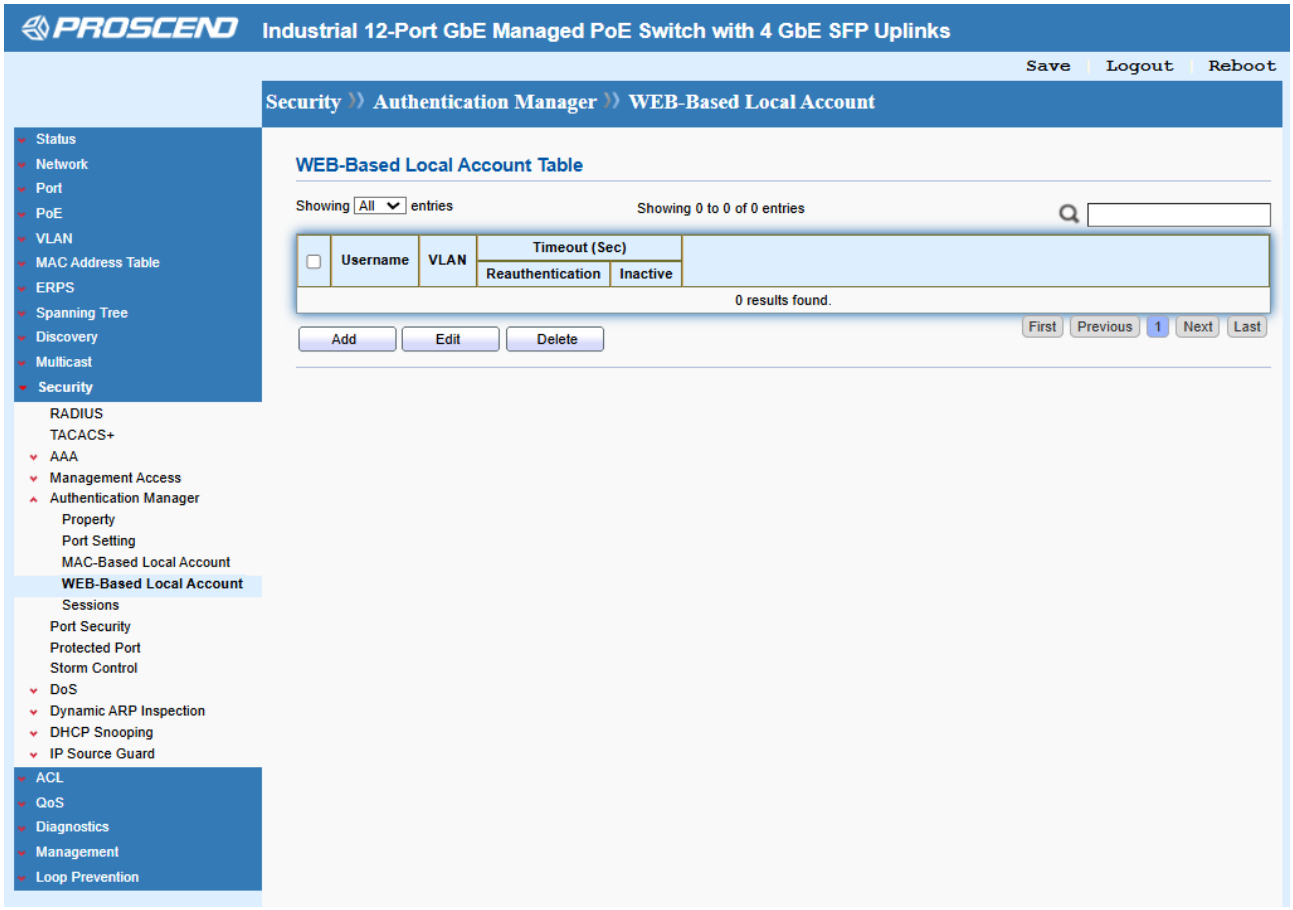
Item	Description
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the selected entry.



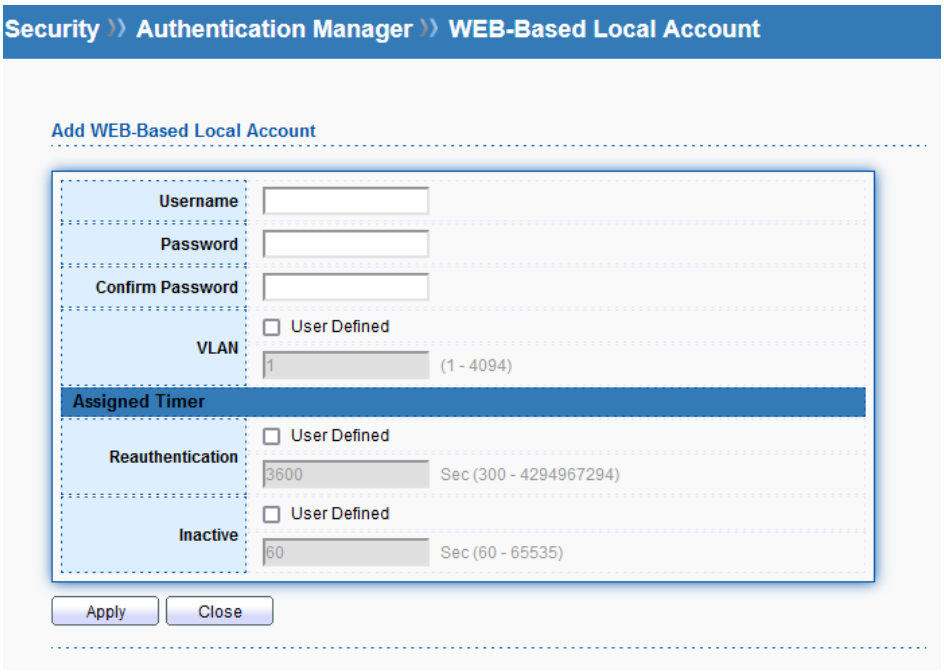
Item	Description
MAC Address	Enter the MAC address of the host.
Port Control	Specify a control type for the host. **Force Authorized**: Click it to forcefully authenticate the host specified above. **Force Unauthorized**: The host specified above will not be authenticated by Switch.
VLAN	Check it to specify which VLAN will be assigned by the host of this account. **Force Authorized only.**
Assigned Timer	
Reauthentication	Check it to specify the time this account required to be authenticated again after authentication taken place.
Inactive	Check it to specify the time of inactive this account becoming log-off.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

14.5.4 WEB-Based Local Account

This page allows to create profiles by entering user account of the hosts to be authenticated.



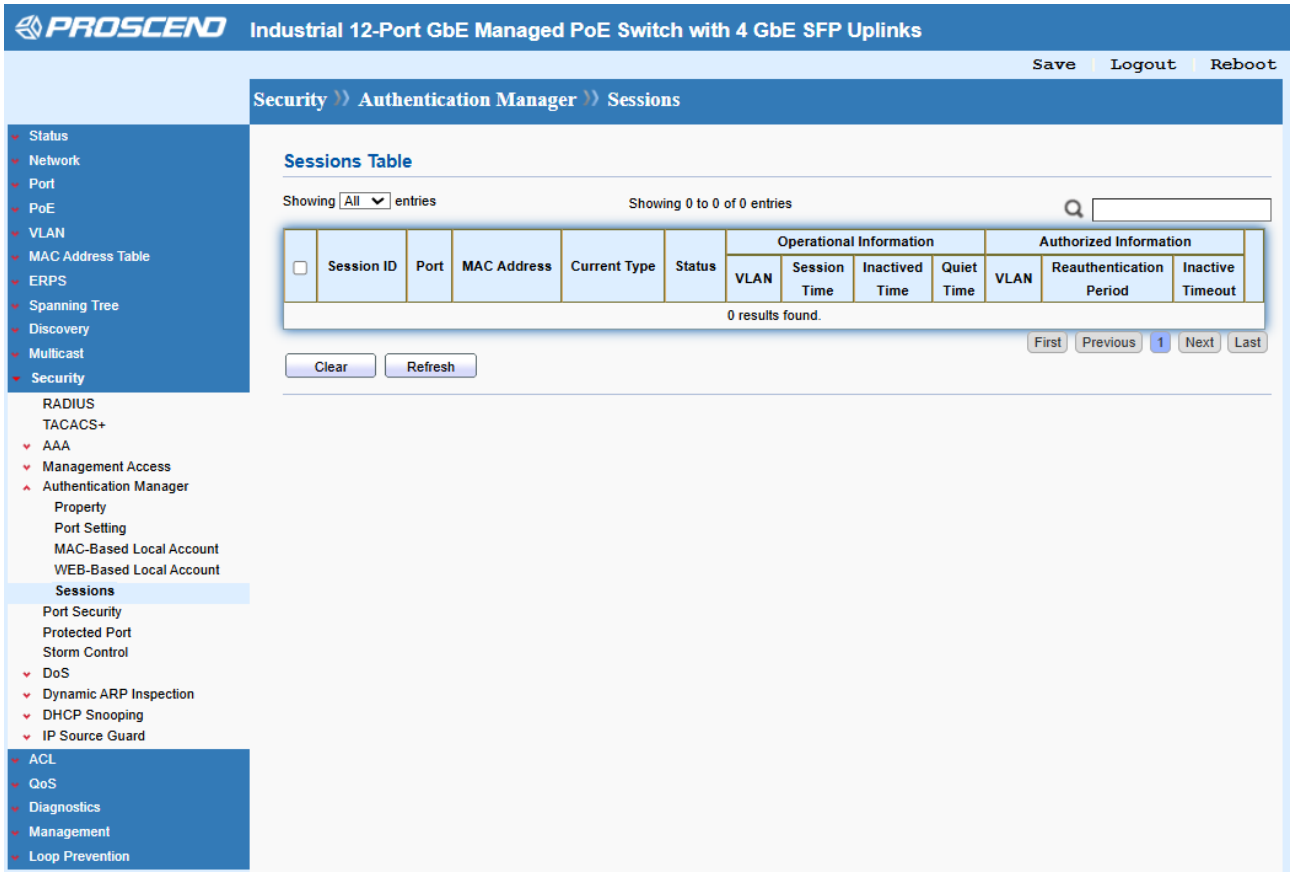
Item	Description
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the selected entry.



Item	Description
Username	Enter the username of the host.
Password	Enter the password.
Confirm Password	Enter the password again.
VLAN	Check it to specify which VLAN will be assigned by the host of this account.
Assigned Timer	
Reauthentication	Check it to specify the time this account required to be authenticated again after authentication taken place.
Inactive	Check it to specify the time of inactive this account becoming log-off.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

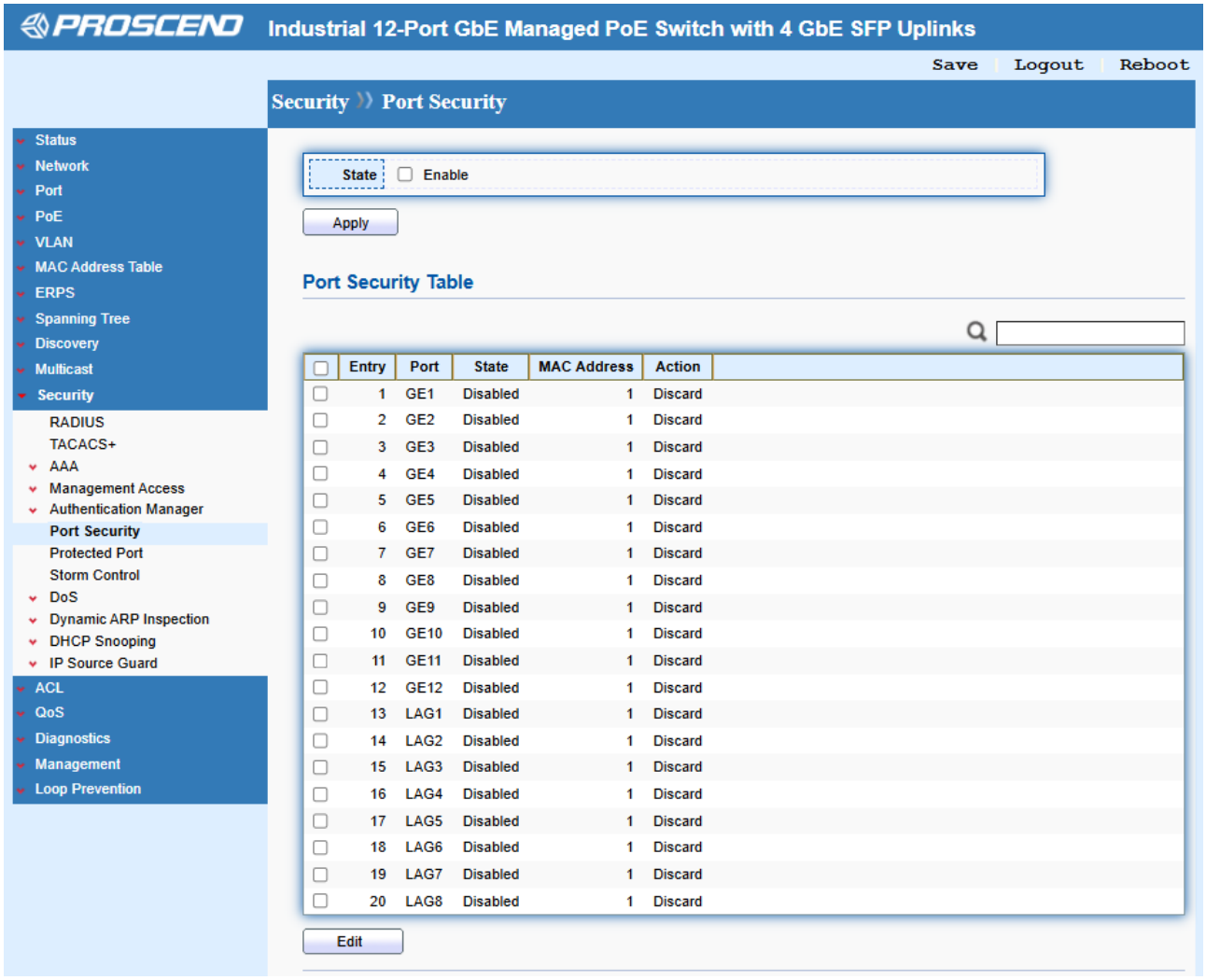
14.5.5 Sessions

This page displays information related to the host authenticated by Switch.

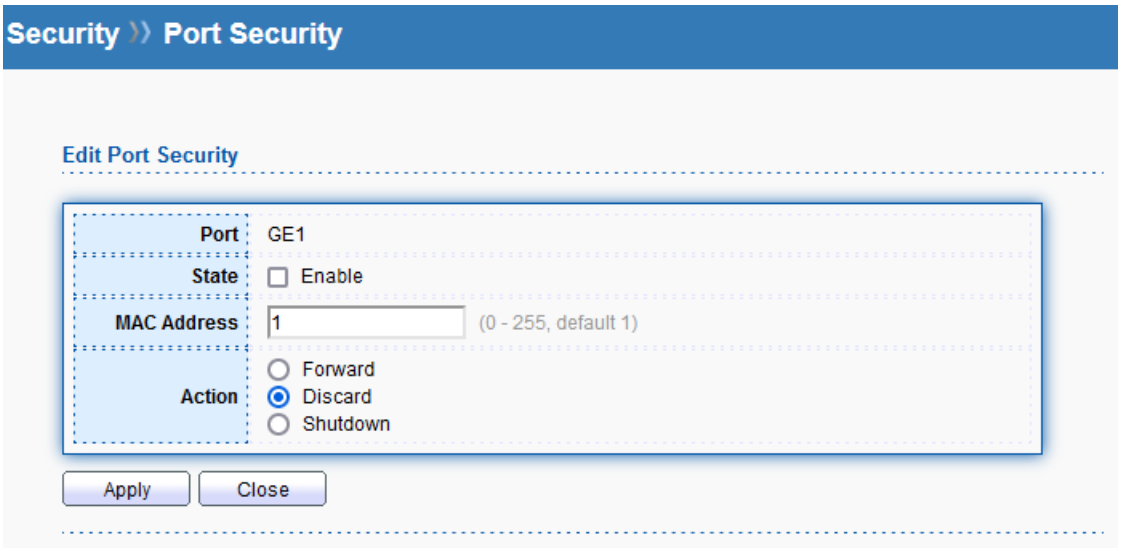


14.6 Port Security

This page allows to configure security settings for each port interface (GE port /LAG group). When port security is enabled for each interface, related action will be performed once detecting that the number of MAC address exceeds the limit.



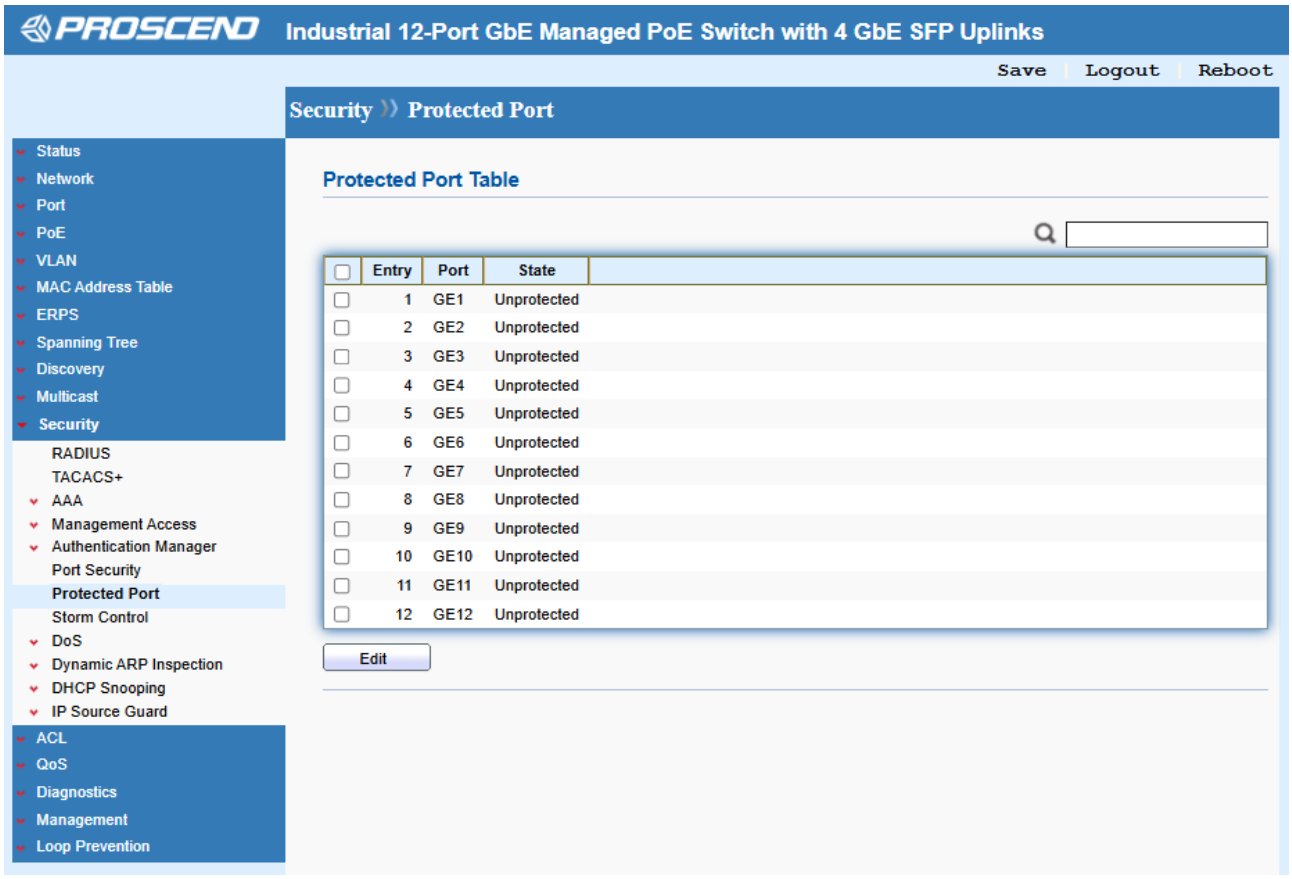
Item	Description
State	Enable or disable port security function on the switch.
Apply	Apply the settings to the switch.
Edit	Delete the selected port.



Item	Description
Port	The index number of selected port.
State	Enable or disable port security function on the selected port(s)
MAC Address	Enter the maximum number of MAC addresses that the port is allowed to learn.
Action	Select an action to perform when there is an unknown MAC address on the port. **Forward**: Forward a packet whose source MAC is unknown to the switch. **Discard**: Discard a packet whose source MAC is unknown to the switch. **Shutdown**: Shutdown this port when a packet with unknown source MAC is received.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

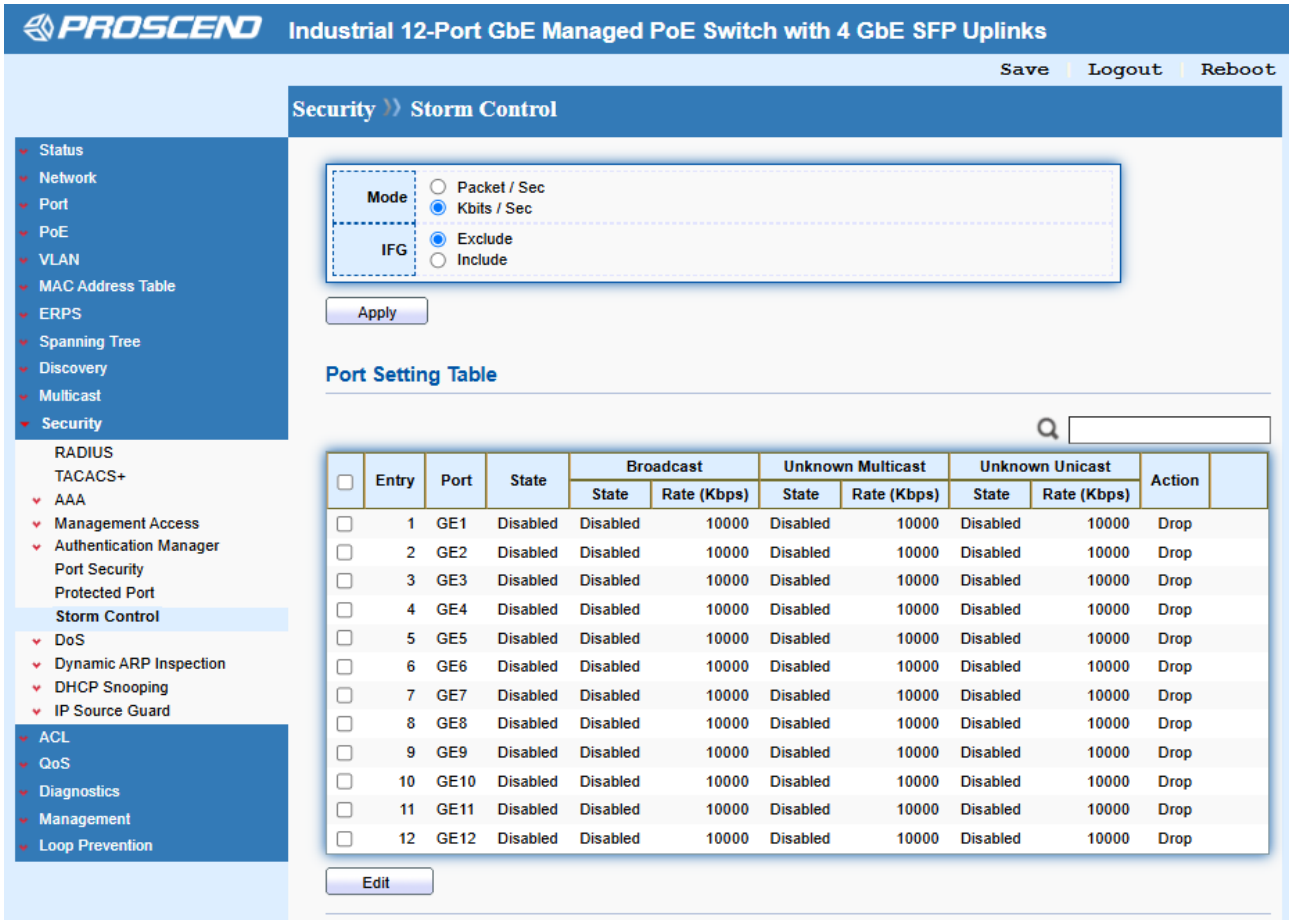
14.7 Protected Port

This page allows to enable port protection.



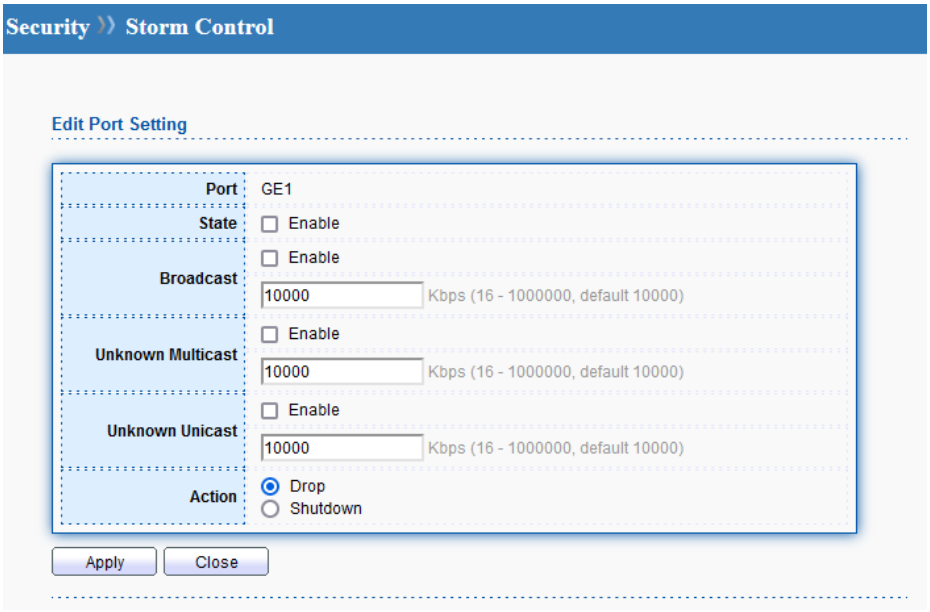
14.8 Storm Control

This page allows to configure general settings for Storm Control.



Item	Description
Mode	Select the mode of storm control. **Packet/sec:** Storm control rate will be calculated by packet-based. **Kbits/sec:** Storm control rate will be calculated by octet-based.
IFG	Select the rate calculation with/without 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.
Apply	Apply the settings to the switch.

Edit	Edit the settings of selected port.



Item	Description
Port	The index number of selected port.
State	Enable or disable the storm control function on the selected port(s)
Broadcast	Specify the storm control rate for Broadcast packet. Value of storm control rate, Unit: Kbps (Kbits per-second). The range is from 16 to 1000000.
Unknown Multicast	Specify the storm control rate for unknown multicast packet. Value of storm control rate, Unit: Kbps (Kbits per-second). The range is from 16 to 1000000.
Unknown Unicast	Specify the storm control rate for unknown multicast packet. Value of storm control rate, Unit: Kbps (Kbits per-second). The range is from 16 to 1000000.
Action	Select the state of setting. **Drop**: Packets exceed storm control rate will be dropped. **Shutdown**: Port exceeds storm control rate will be shutdown.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

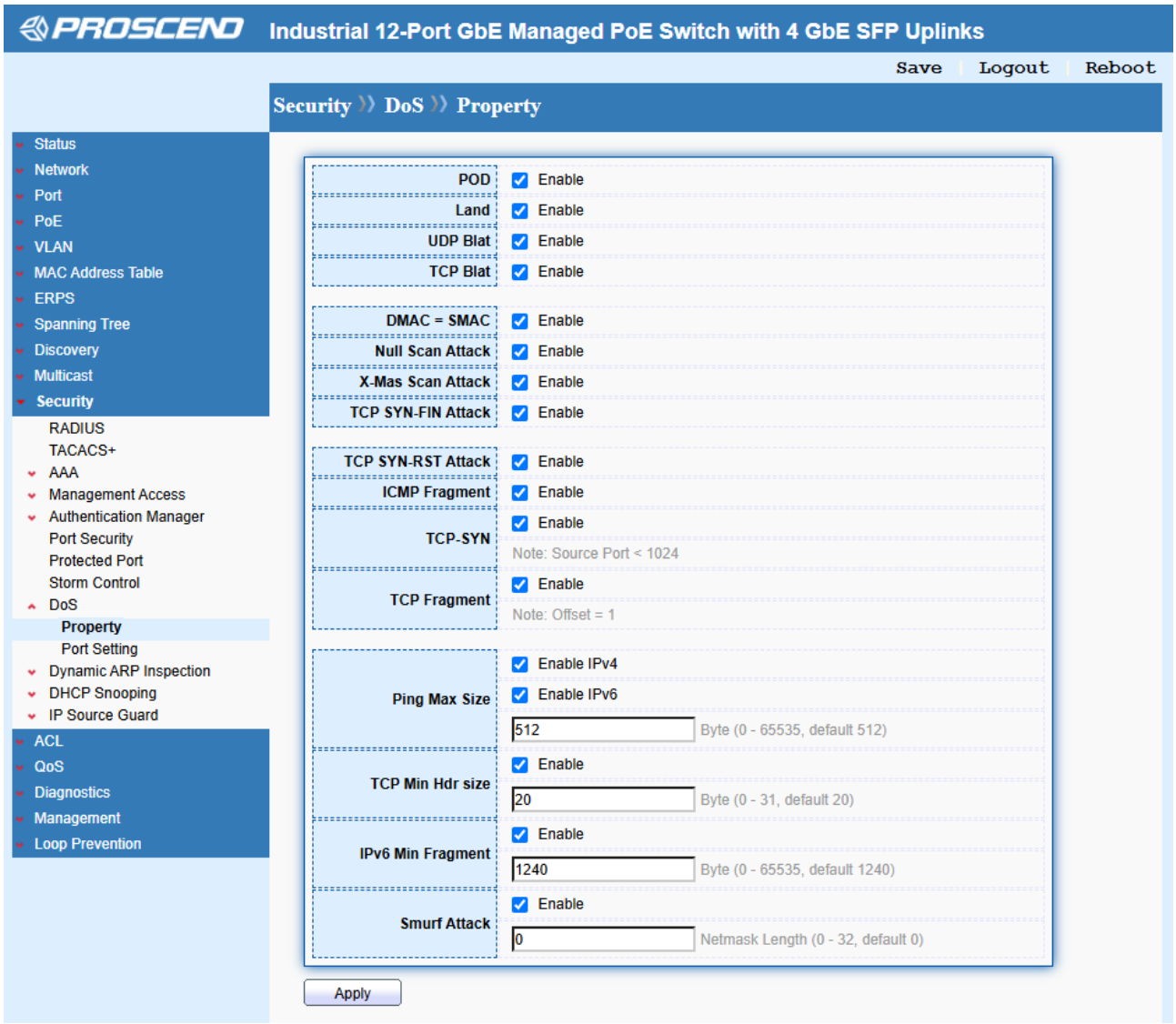
14.9 DoS

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 Setting enables activating the security suite.

14.9.1 Property

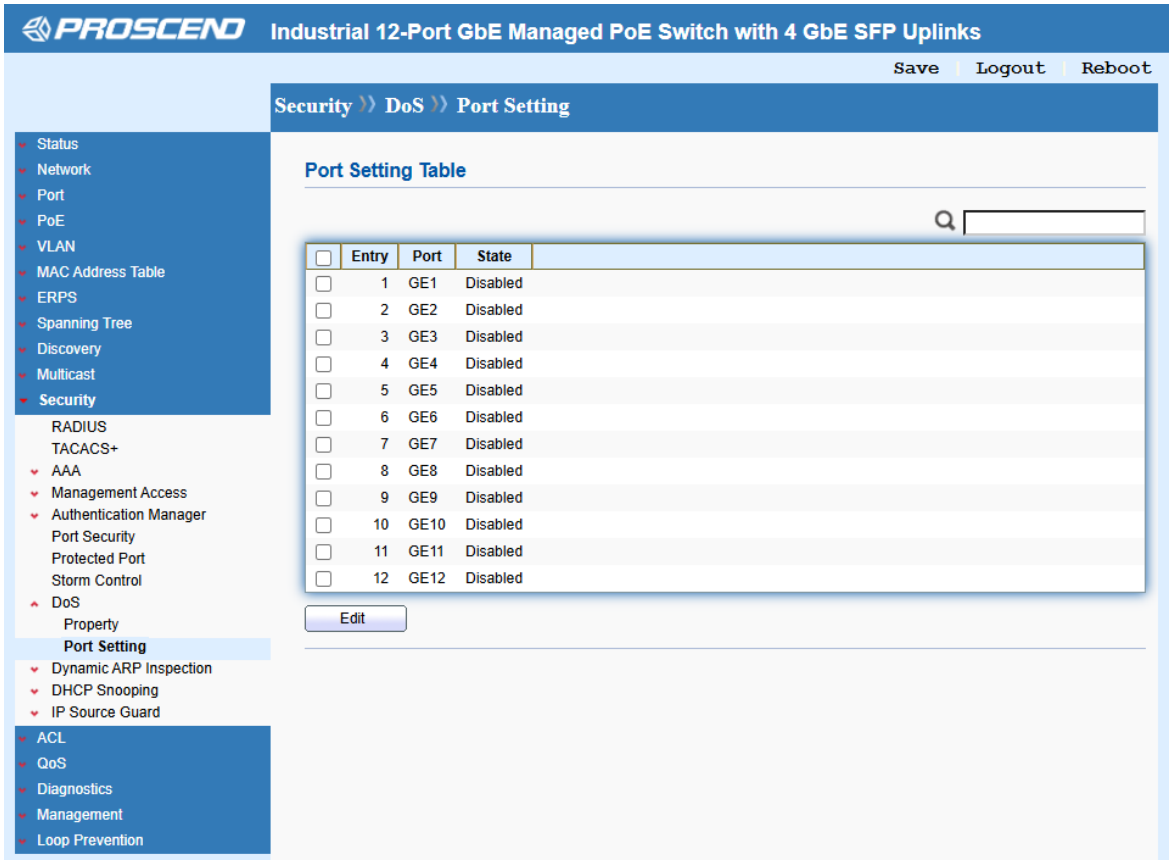
This page allows to configure DoS setting to enable/disable DoS function for global setting.



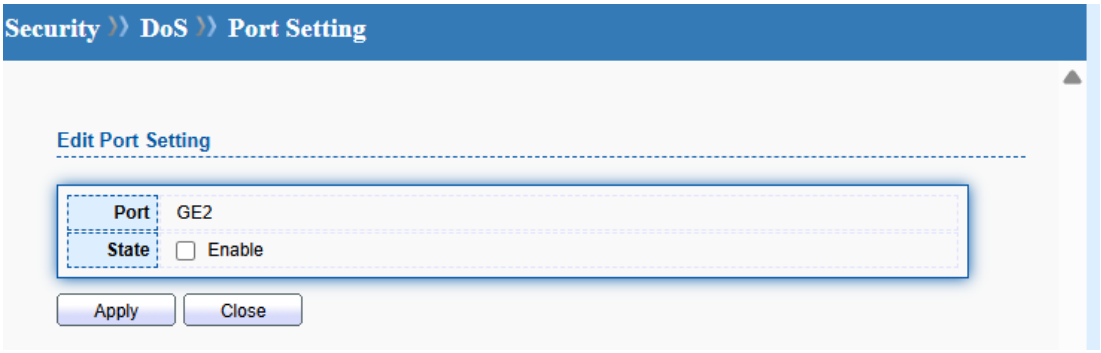
Item	Description
POD	Avoid ping of death attack. Ping packets that length is larger than 65536 bytes.
Land	Drop the packets if the source IP address is equal to the destination IP address.
UDP Blat	Drop the packets if the UDP source port equals to the UDP destination port.
TCP Blat	Drop the packages if the TCP source port is equal to the TCP destination port.
DMAC = SMAC	Drop the packets if the destination MAC address is equal to the source MAC address.
Null Scan Attack	Drop the packets with NULL scan.
X-Mas Scan Attack	Drop the packets if the sequence number is zero, and the FIN, URG and PSH bits are set.
TCP SYN-FIN Attack	Drop the packets with SYN and FIN bits set.
TCP SYN-RST Attack	Drop the packets with SYN and RST bits set.
ICMP Fragment	Drop the fragmented ICMP packets.
Ping Max Size	Determine the IPv4/IPv6 PING packet with the length. Determine the IPv4/IPv6 PING packet with the length. 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	Check 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	Check the minimum size of IPv6 fragments, and drop the packets smaller than the minimum size. The valid range is from 0 to 65535 bytes, and default value is 1240 bytes.
Smurf Attack	Avoid smurf attack. The length range of the net mask is from 0 to 323 bytes, and default length is 0 byte.
Apply	Apply the settings to the switch.

14.9.2 Port Setting

This page allows to configure and display the state of DoS protection for interfaces.



Item	Description
Edit	Edit the settings of selected port.



Item	Description
Port	The index number of selected port.
State	Enable or disable the DoS protection on the selected port(s)
Apply	Apply the settings to the switch.

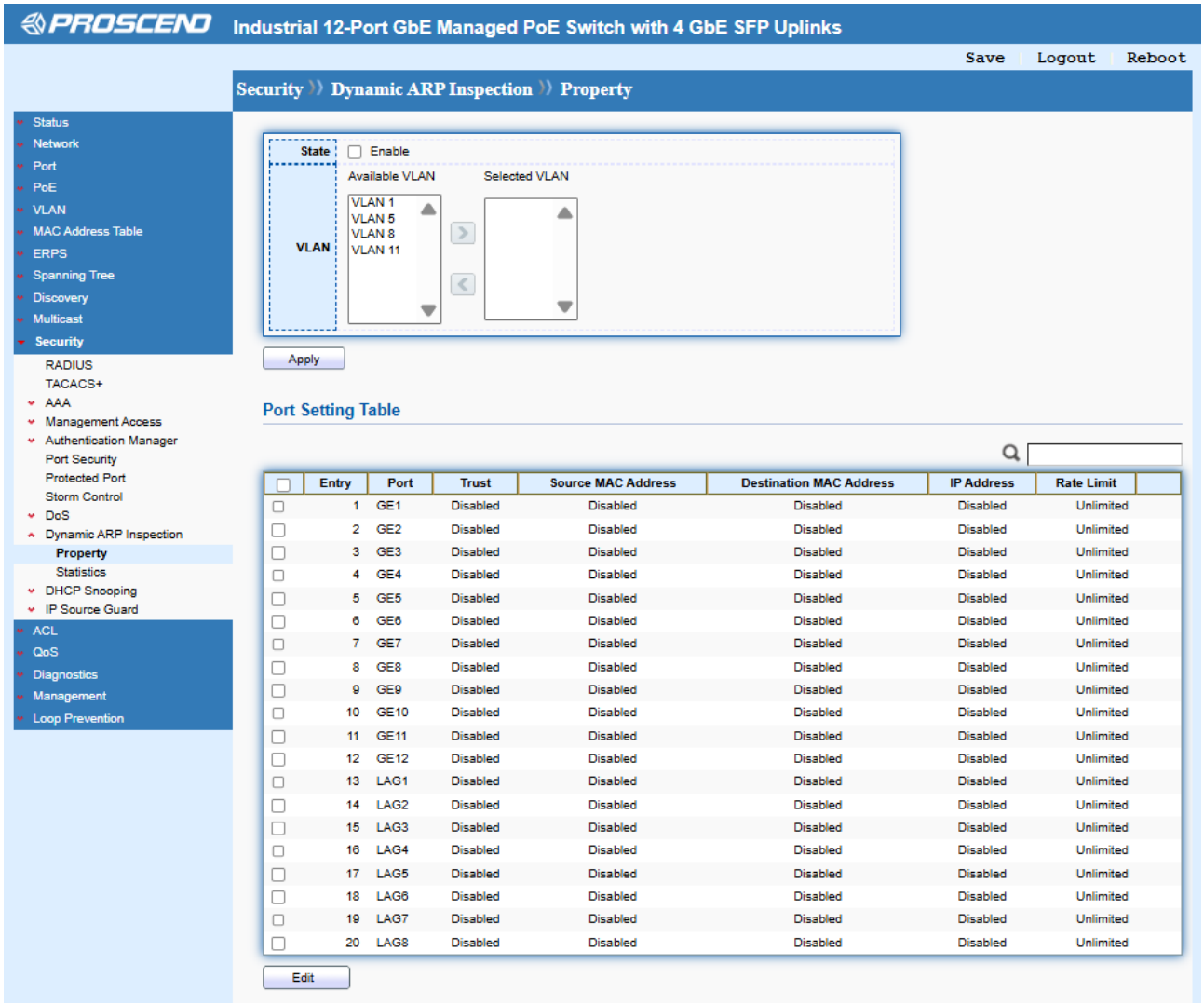
Close	Close the setting page and back to previous page.

14.10 Dynamic ARP Inspection

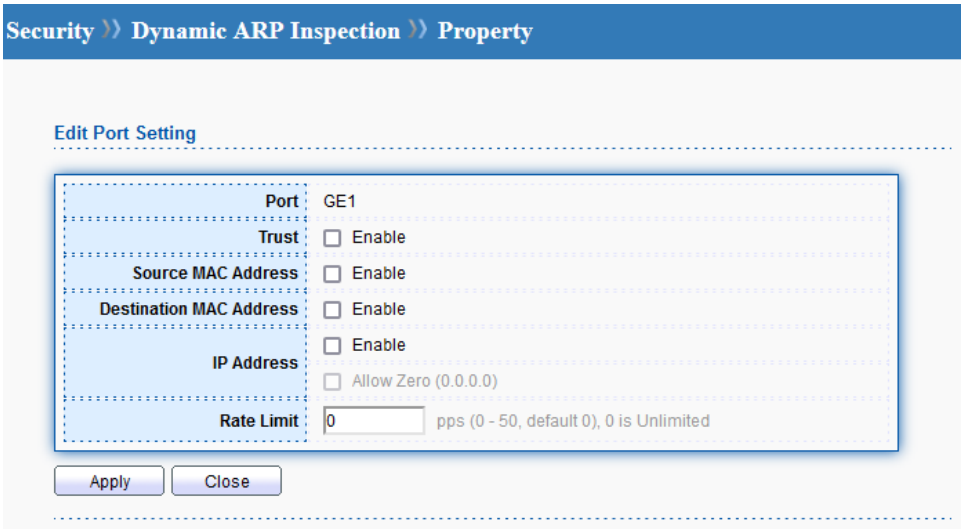
Dynamic ARP inspection (DAI) can prevent ARP spoofing attacks by validating ARP packet in a network. It can intercept, record, and discard ARP packets with invalid IP-to-MAC address bindings; and then protect the network against malicious attacks.

14.10.1 Property

This page allows to configure global property settings for the function of Dynamic ARP Inspection.



Item	Description
State	Check the box to enable global property settings.
VLAN	Select VLAN profile(s) to apply the function of Dynamic ARP Inspection.
Apply	Apply the settings to the switch.
Edit	Edit the settings of selected port.

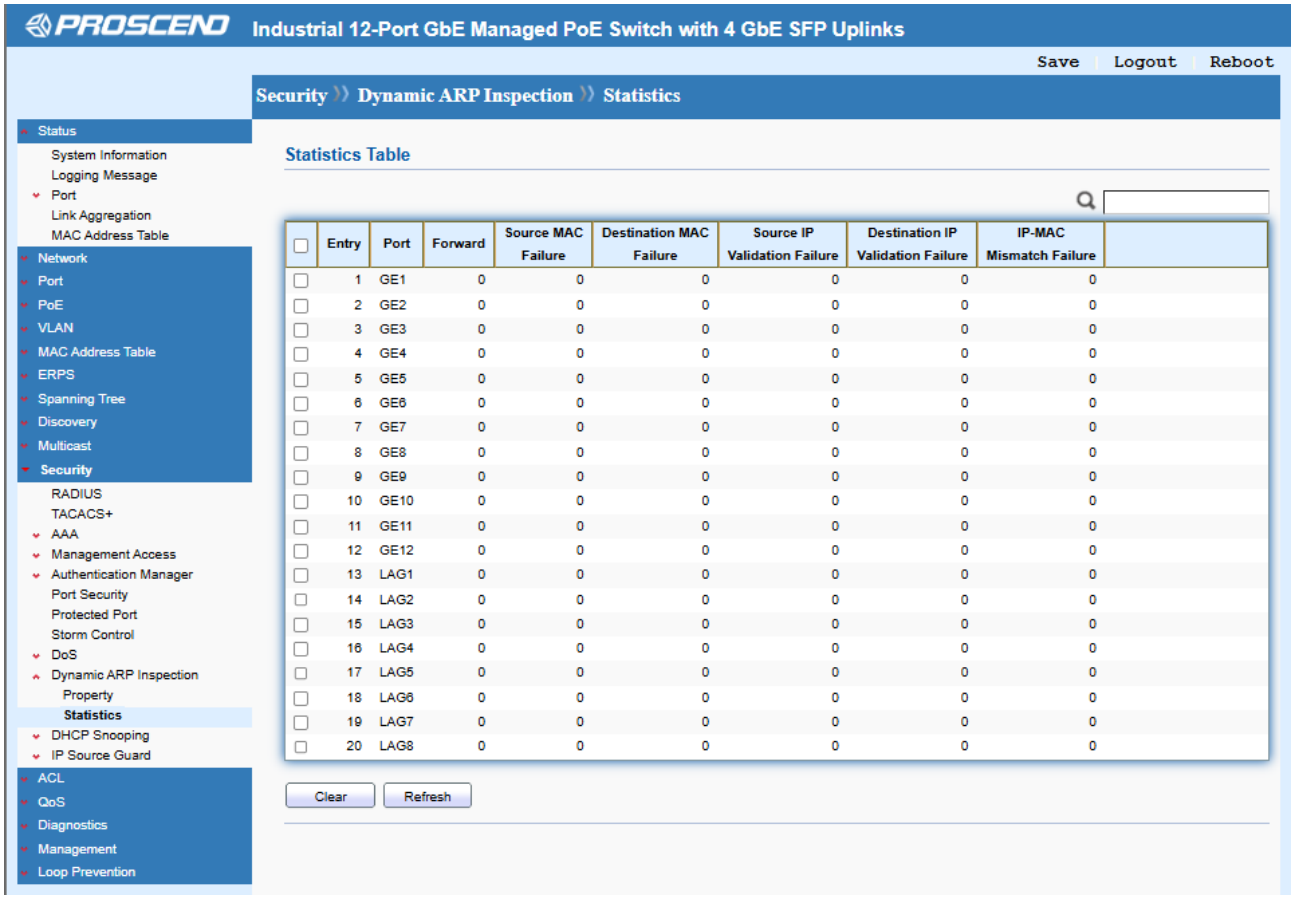


Item	Description
Port	The index number of selected port.
Trust	Enable the function of DAI for the port(s) selected above.
Source MAC Address	Check it to enable the function of source MAC address validation mechanism for the selected port(s).
Destination MAC Address	Check it to enable the function of destination MAC address validation mechanism for the selected port(s).
IP Address	Check it to enable the function of IP address validation mechanism for the selected port(s). Allow Zero – The IP address of “0.0.0.0” can be applied to the selected port(s) if it is enabled.
Rate Limit	Use the drop down list to choose a rate limitation value (0~50) for the selected port(s).

Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

14.10.2 Statistics

This page displays all statistics recorded by Dynamic ARP Inspection function.

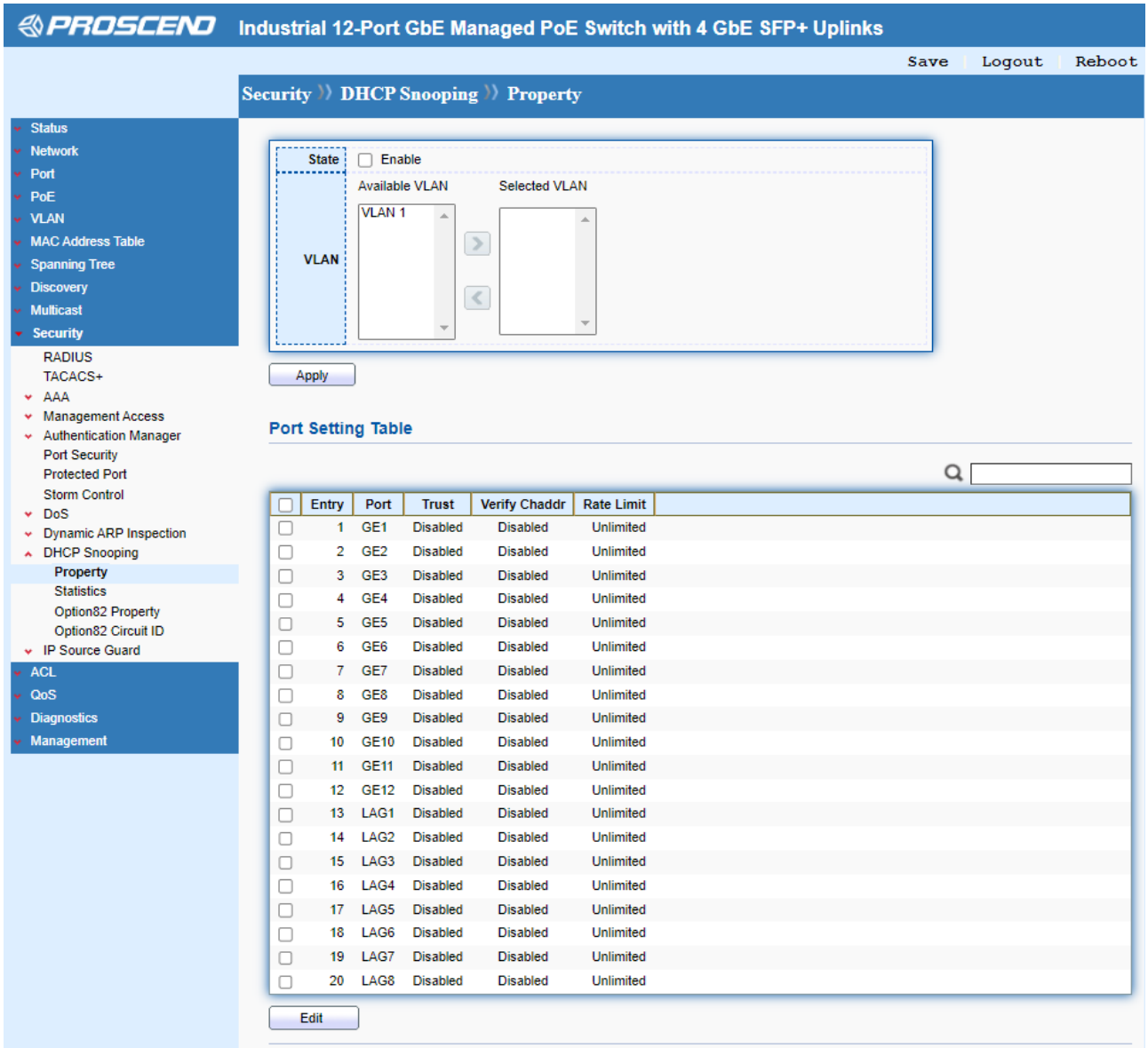


14.11 DHCP Snooping

DHCP snooping is able to validate DHCP messages obtained from untrusted sources and filter out invalid message. For DHCP snooping to function properly, it is suggested to connect DHCP servers to Switch through trusted interfaces; because untrusted DHCP messages will be forwarded to trusted interfaces only.

14.11.1 Property

This page allows to configure global property settings for the function of DHCP snooping Inspection. In default, DHCP snooping is inactive on all VLANs. You can enable such feature on a single VLAN or a range of VLANs.



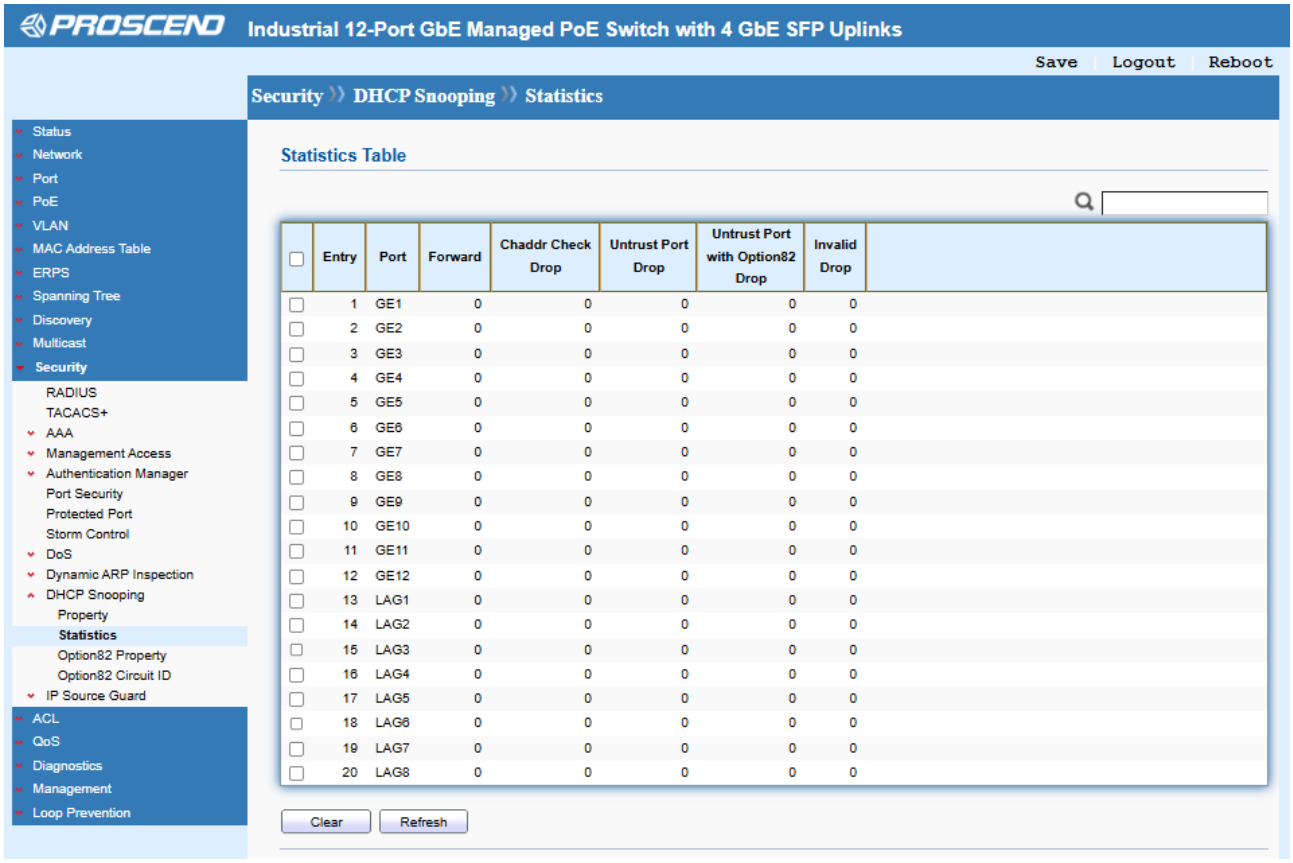
Item	Description
State	Check the box to enable global property settings.
VLAN	Select VLAN profile(s) to apply the function of DHCP Snooping Inspection.
Apply	Apply the settings to the switch.
Edit	Edit the settings of selected port.



Item	Description
Port	The index number of selected port.
Trust	Check it to make the port(s) selected above as trusted interface.
Verify Chaddr	Check it to enable chaddr (client hardware address) validation of GE/LAG port. All DHCP packets will be checked if the client hardware MAC address is the same as source MAC in Ethernet header or not. Default is disabled.
Rate Limit	Input rate limitation (0~300) of DHCP packets. The unit is “pps”. “0” means unlimited. Default is unlimited.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

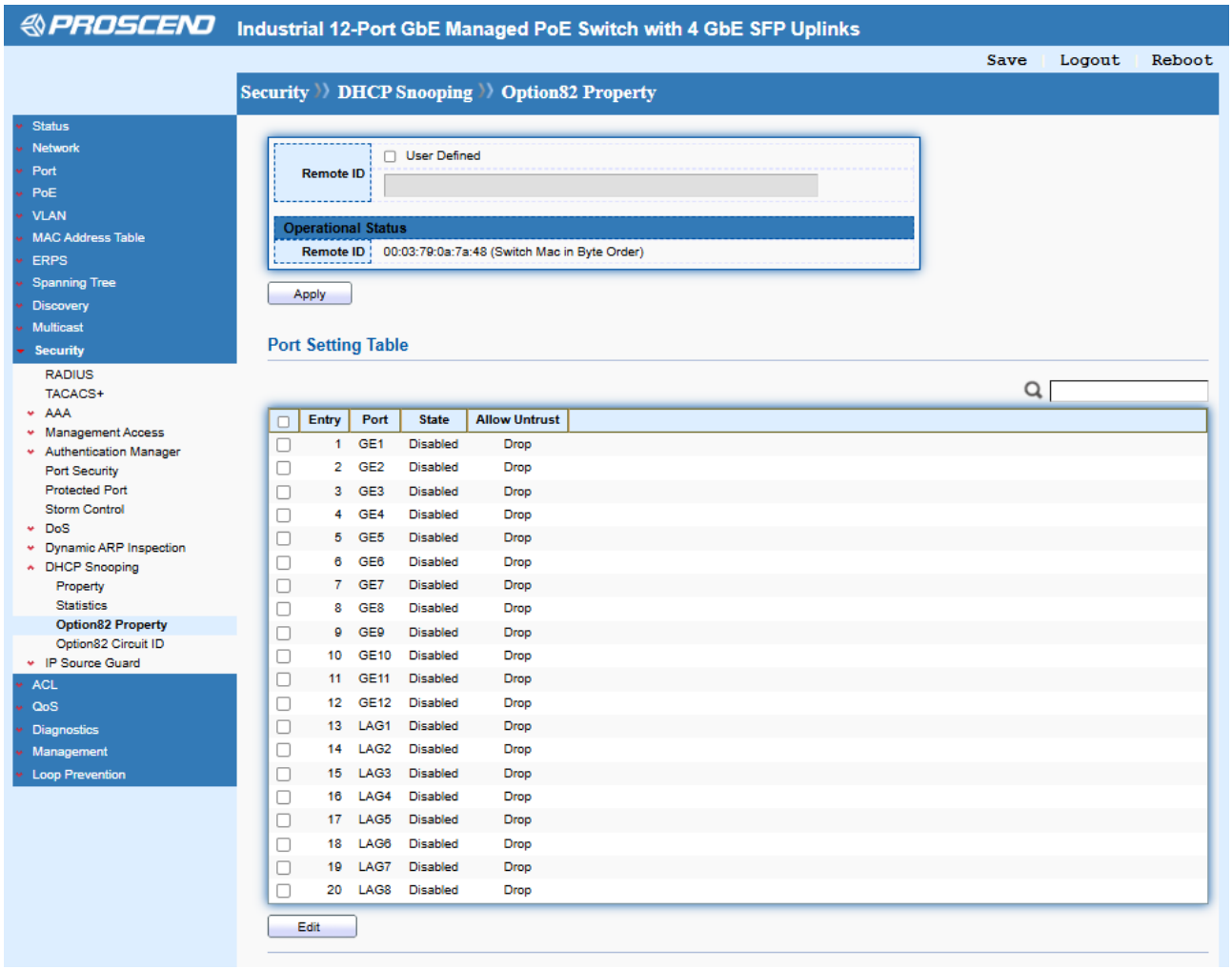
14.11.2 Statistics

This page displays all statistics recorded by DHCP snooping function.

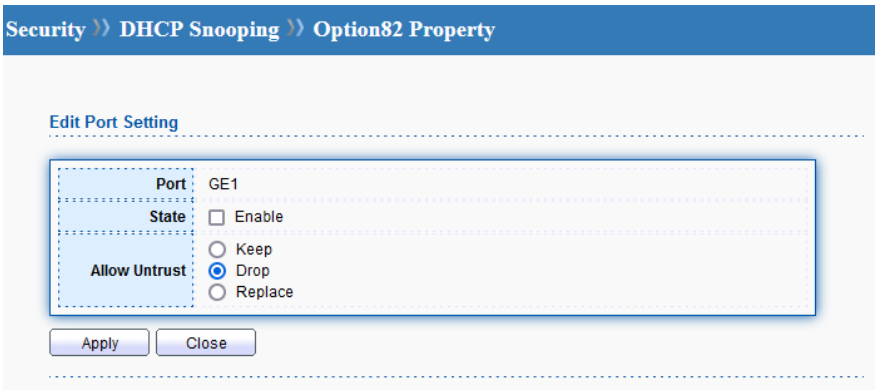


14.11.3 Option82 Property

You can use information settings including Remote ID and Circuit ID for Option82 Property, also known as the DHCP relay agent, to protect Switch against spoofing attacks



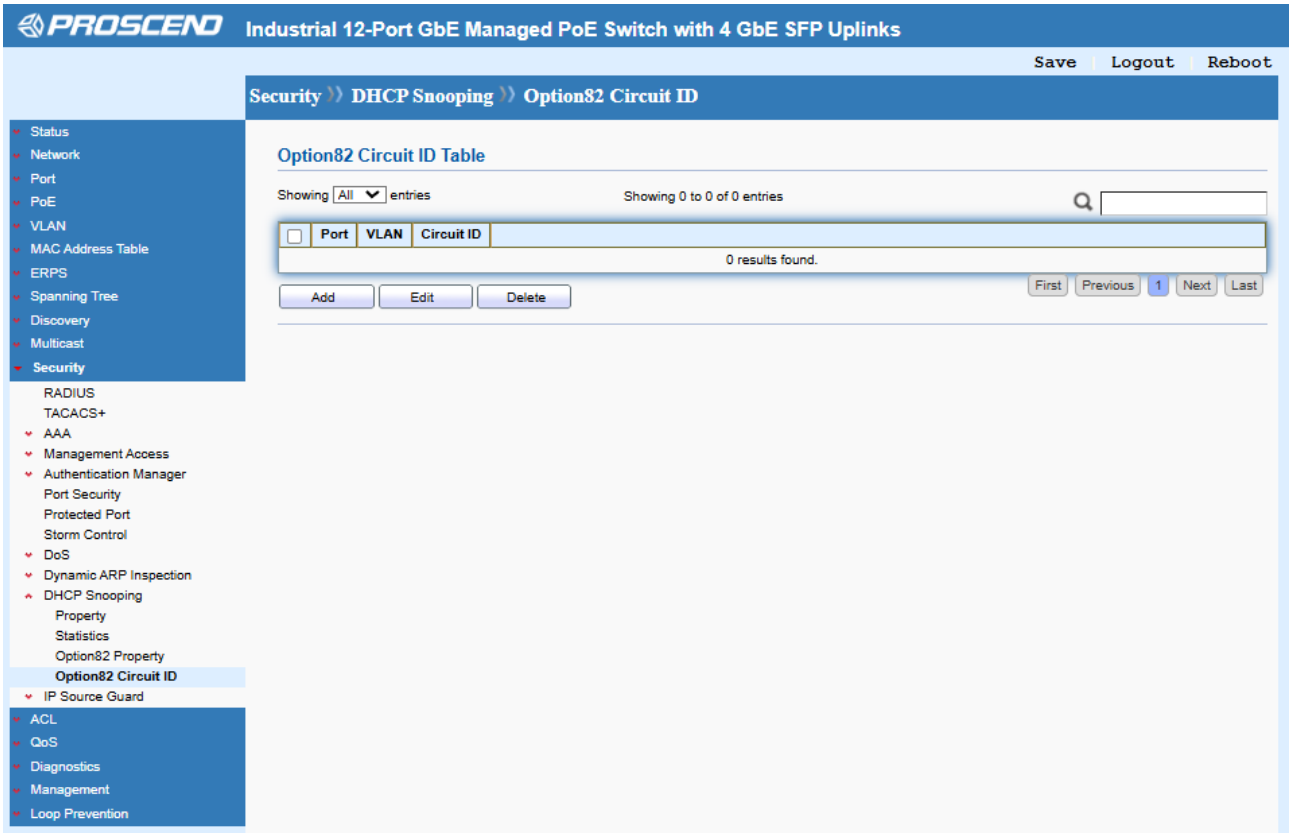
Item	Description
Remote ID	The string specified here is used to identify the remote host. User Defined – Check it and manually enter ASCII text string in the entry box.
Apply	Apply the settings to the switch.
Edit	Edit the settings of selected port.



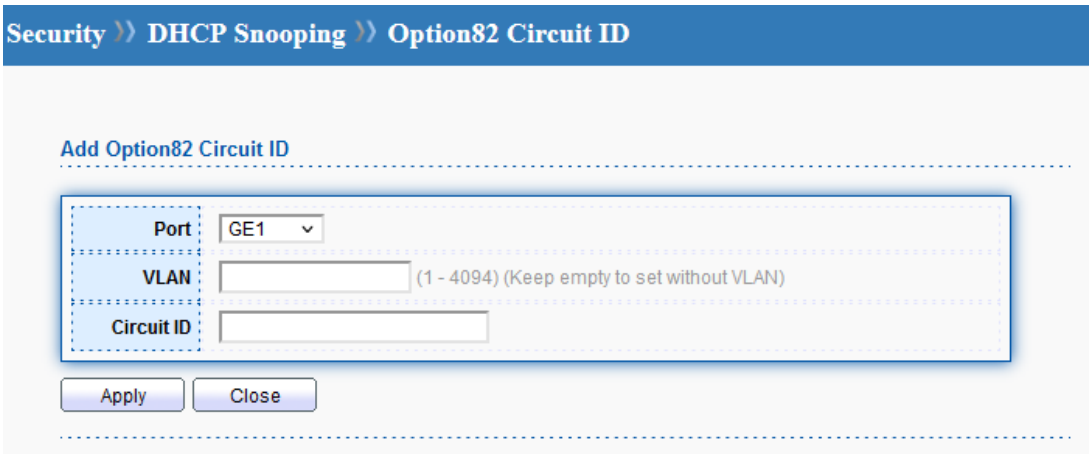
Item	Description
Port	The index number of selected port.
State	Check it to make the port(s) selected above apply the settings configured in this page.
Allow Untrust	Untrusted packets detected by Switch will be performed by the action determined here. **Keep**: Packets are allowed to pass through. **Drop**: Packets are blocked and discarded. Default is Drop. **Replace**: Packets will be replaced.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

14.11.4 Option82 Circuit ID

This page allows to setup string as circuit ID for DHCP option82 setting. Circuit ID shall be combined with VLAN name (or VLAN ID number) and interface name (GE/LAG port).



Item	Description
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the selected entry.



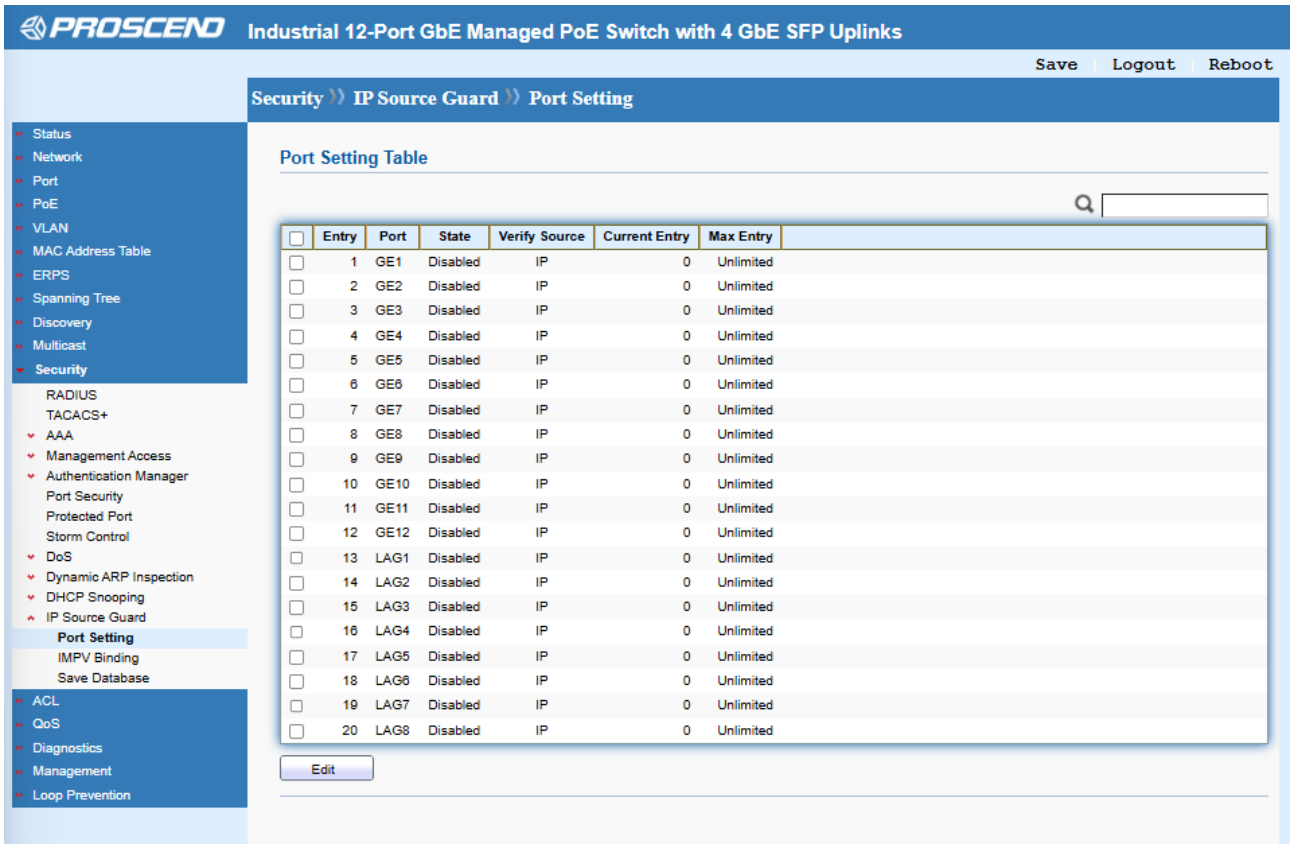
Item	Description
Port	Use the drop down list to select the port for applying DHCP snooping, Option82 Property function.
VLAN	Choose a number as VLAN ID which is easy to be identified for a packet containing with it. It is optional setting.
Circuit ID	Enter ASCII text string in the entry box. Later, any packet passes through the specified interface will be inserted with such information.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

14.12 IP Source Guard

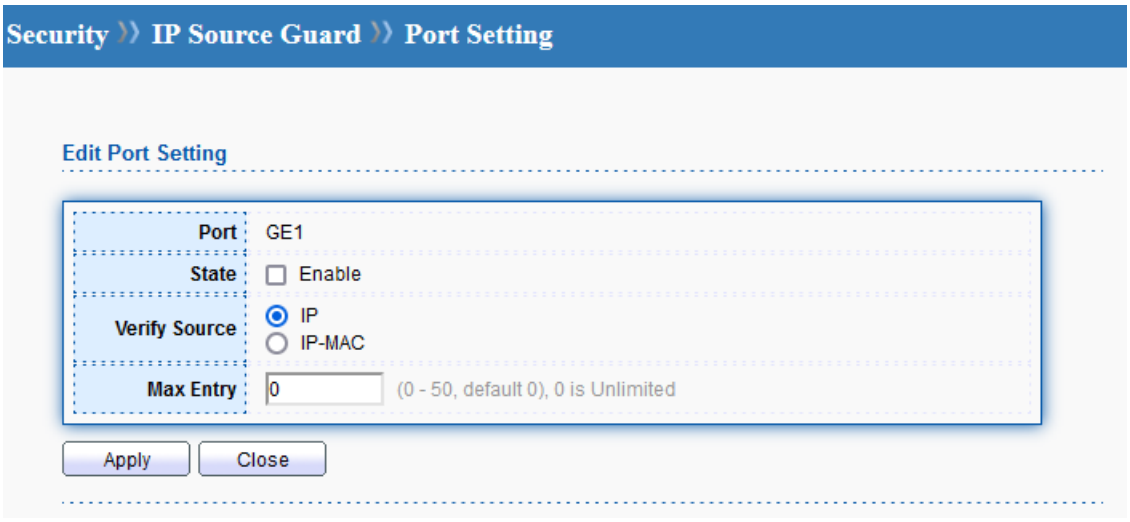
By using the source IP address filtering function, IP source guard can prevent a malicious host from feigning a legal host with its IP address and performing malicious attack.

14.12.1 Port Setting

IP source guard is a port-based feature. Therefore, it is necessary to configure detailed settings for each GE/LAG port interface separately.



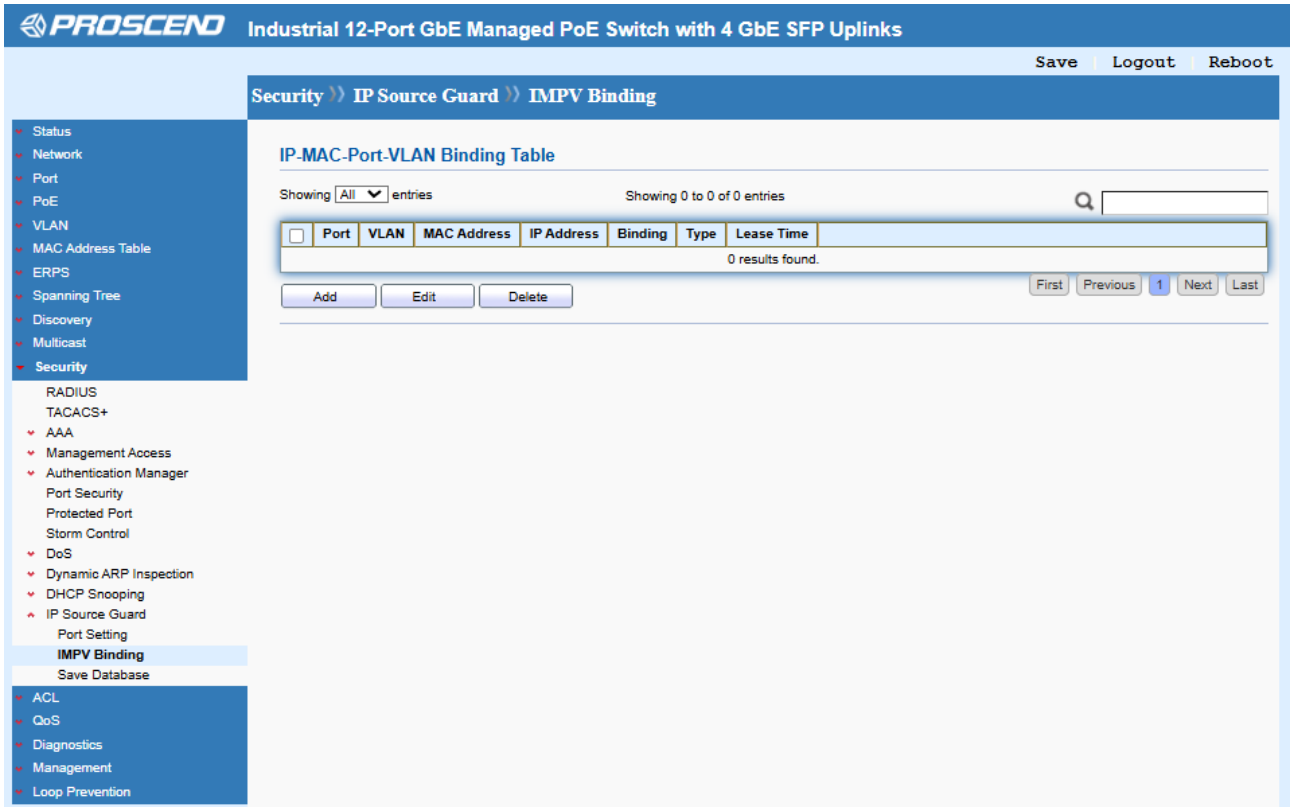
Item	Description
Edit	Edit the settings of selected port.



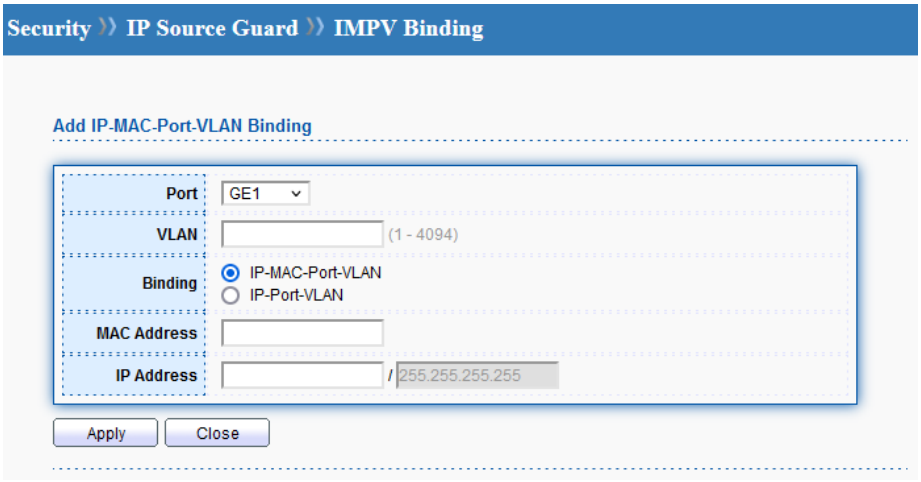
Item	Description
Port	The index number of selected port.
State	Check it to make the port(s) selected above apply the settings configured in this page.
Verify Source	Specify the type of source IP for the packet coming from. **IP**: Only the packet with specified IP address will be verified. **IP-MAC**: Only the packet with specified IP address and MAC address will be verified.
Max Entry	Define the number (0~50) for the port. The default is 0 (no limit).
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

14.12.2 IMPV Binding

This page allows to set the filtering conditions (binding type, MAC address, IPv4 address) for packets through the specified LAN port.



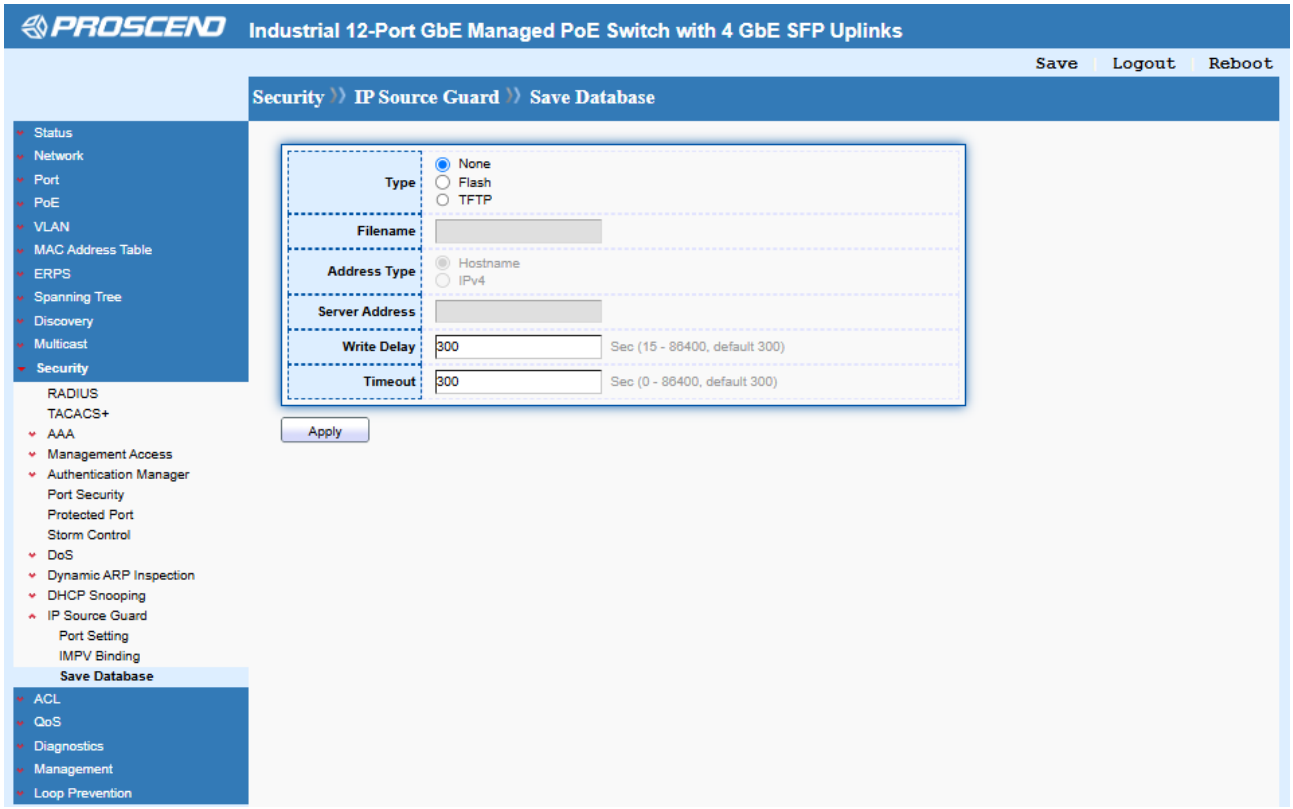
Item	Description
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the selected entry.



Item	Description
Port	Use the drop down list to select the port for applying IMPV Binding function.
VLAN	Choose a number as VLAN ID which is easy to be identified for a packet containing with it. It is optional setting.
Binding	Select the binding type for such feature. **IP-MAC-Port-VLAN**: Packets will be allowed to pass through the port interface if they meet the conditions specified by IP address, MAC address, Port setting and VLAN ID setting. **IP-Port-VLAN**: Packets will be allowed to pass through the port interface if they meet the conditions specified by IP address, Port setting and VLAN ID setting.
MAC Address	Enter the MAC address of the device connecting to the port interface selected above.
IP Address	Enter the IP address with mask address of the device connecting to the port interface selected above.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

14.12.3 Save Database

This page allows to write the database to FLASH or remote TFTP server. Set timeout interval for abortion. Set delay timer for writing to URL.

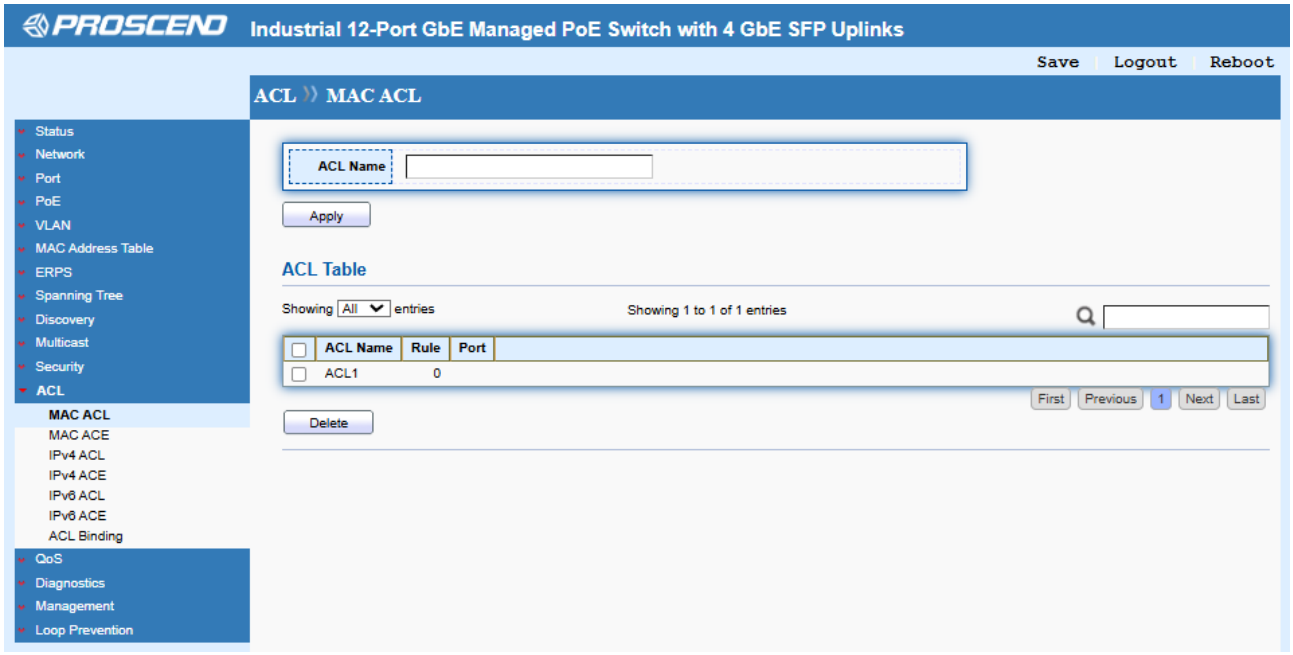


15 ACL

The Access Control List (ACL) is a sequential list of permits or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rule match, the frame is accepted.

15.1 MAC ACL

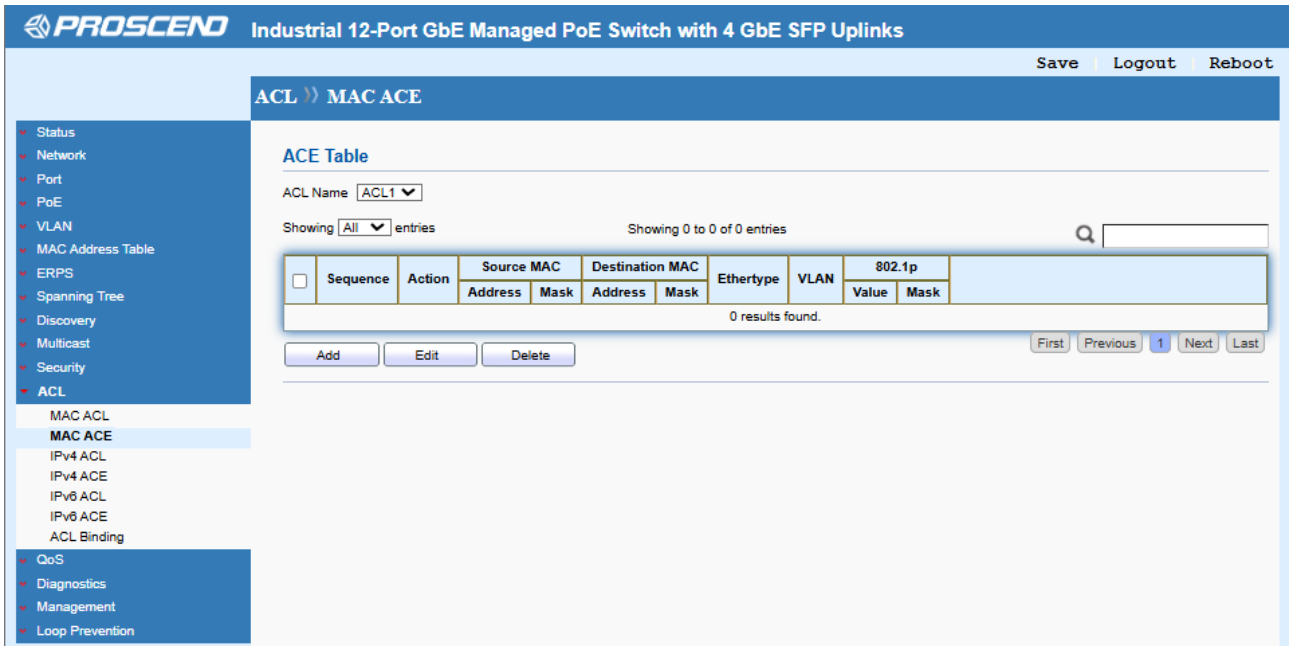
The function is used to show the Access Control List (ACL) based on Layer 2 filtering, the MAC layer. The ACL is composed by many Access Control Element (ACE) rules. You can create a new ACL here; then add multiple ACEs.



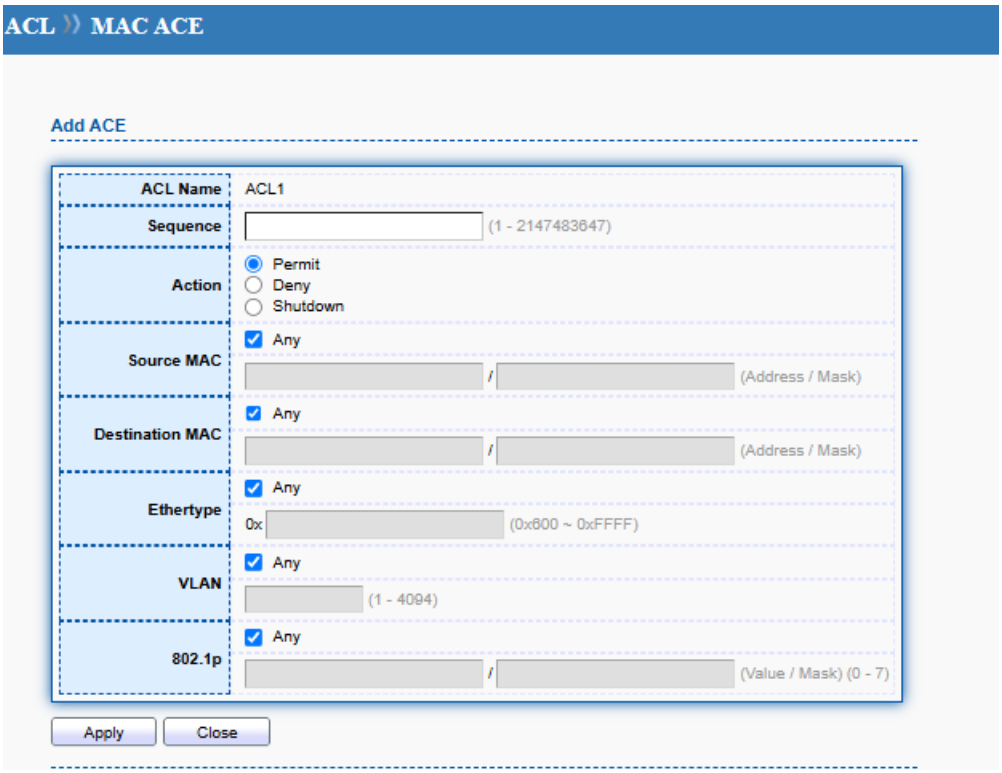
Item	Description
ACL Name	Enter the name for creating ACL profile.
Apply	Apply the settings to the switch.
Delete	Delete the selected entry.

15.2 MAC ACE

This page shows ACE based on MAC address. You may choose ACL, permit, and deny particular packet or frame, even shutdown the port.



Item	Description
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the selected entry.

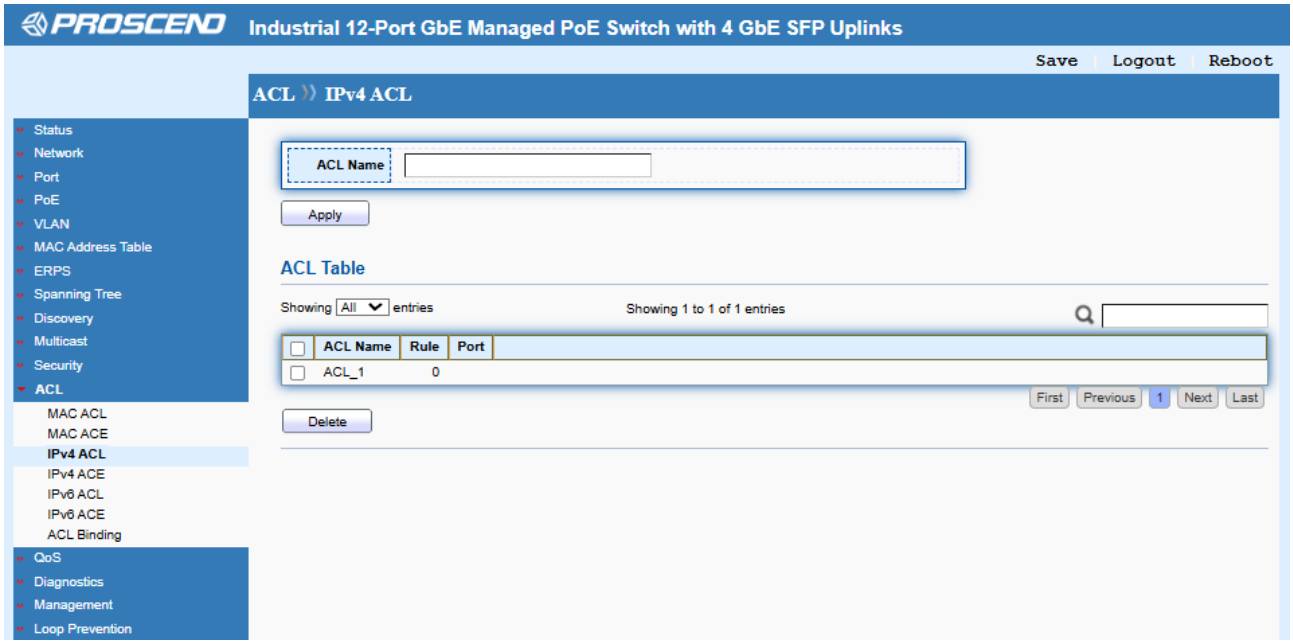


Item	Description
ACL Name	The name of selected ACL profile.
Sequence	Assign a sequence number to this ACE. The sequence is used to identify which one of ACEs in an ACL is firstly used to match ingress packets. The switch port bound with an ACL use the contained ACE rules, start with the one with lower sequence number to match the packet first.
Action	Select the action applied to the packet matched this ACE. Permit or deny the packets into switch core, or shutdown the port for stopping further transmission.
Source MAC	Specify the source MAC address for filtering. **Any**: All packets will be filtered. Or, enter the IP address to filter the packets coming from that address.
Destination MAC	Specify the destination MAC address for filtering. **Any**: All packets will be filtered. Or, enter the IP address to filter the packets coming from that address.

Ethertype	Specify Ethernet type for filtering. Select Any. Or, enter the value with the format of “0x600 ~ 0xFFF”.
VLAN	Specify VLAN profile for filtering. Select Any. Or, enter a VLAN number. The packets coming from the VLAN specified here will be filtered by Vigor device.
802.1p	Specify the 802.1p priority value for filtering. Select Any, or a number from 0 to 7.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

15.3 IPv4 ACL

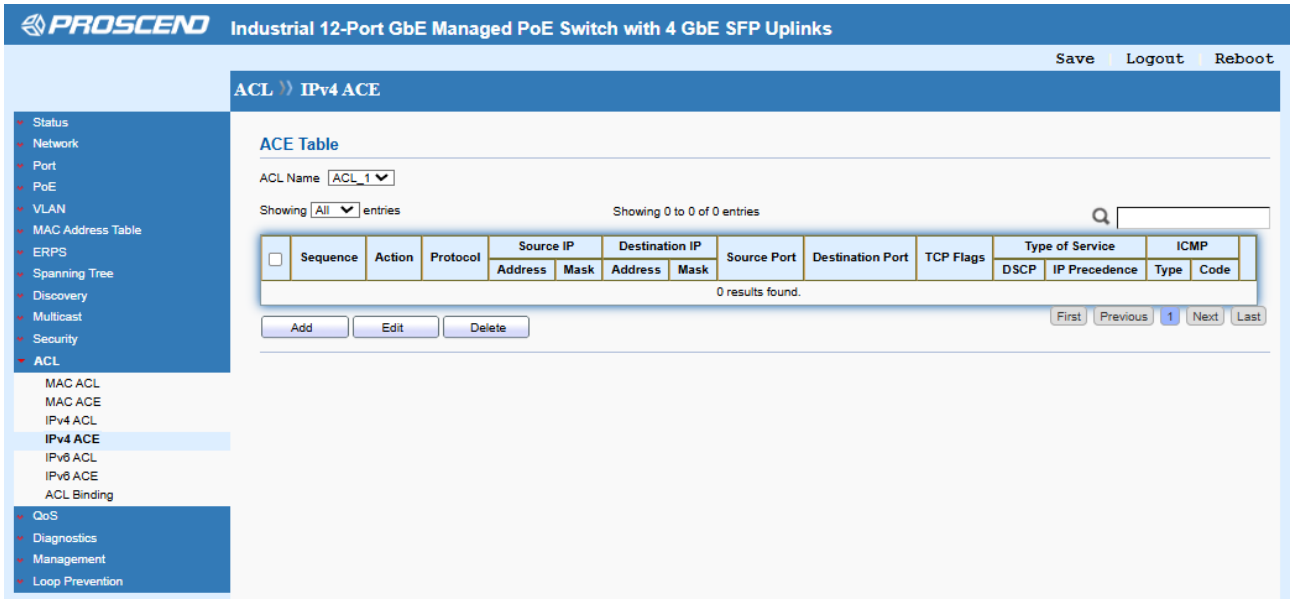
This page shows ACE based on IPv4 address. You may choose ACL, permit, and deny particular packet or frame, even shutdown the port.



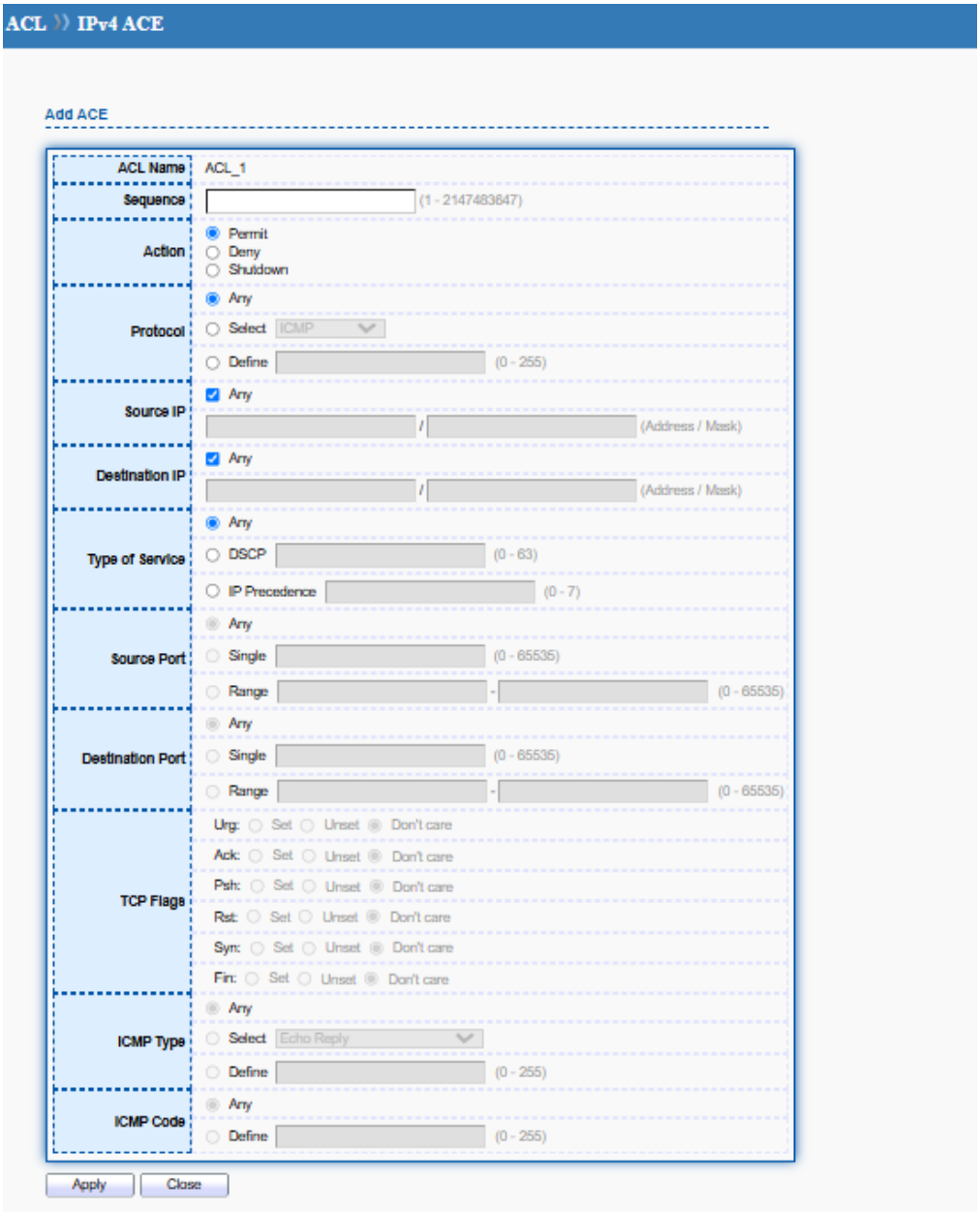
Item	Description
ACL Name	Enter the name for creating ACL profile.
Apply	Apply the settings to the switch.
Delete	Delete the selected entry.

15.4 IPv4 ACE

You may provide filtering/matching criteria for one or more of following packet characteristic (such as Protocol over the IP layer, Source/Destination IPv4 address, Type of Service, Source/Destination port number, TCP flags, ICMP Type, if chosen protocol contains ICMP), for this ACE to identify the packet.



Item	Description
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the selected entry.



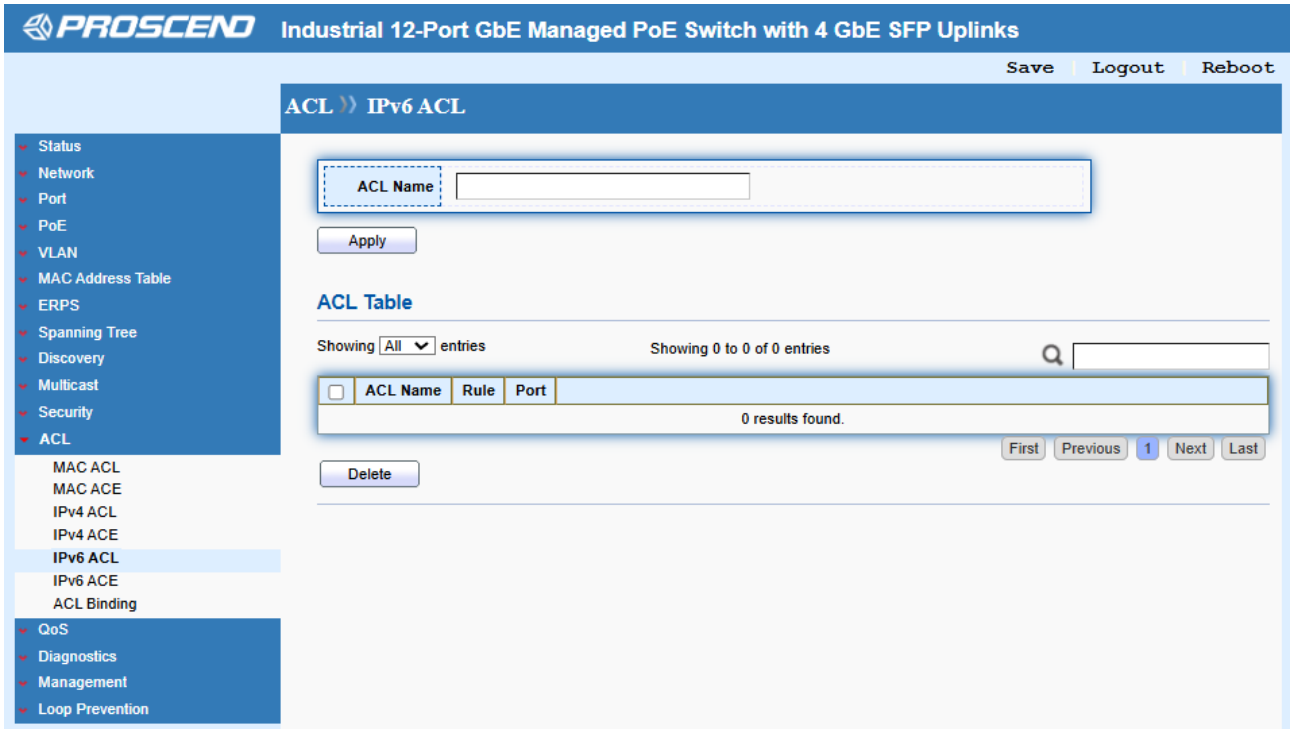
Item	Description
ACL Name	The name of selected ACL profile.
Sequence	Assign a sequence number to this ACE. The sequence is used to identify which one of ACEs in an ACL is firstly used to match ingress packets. The switch port bound with an ACL use the contained ACE rules, start with the one with lower sequence number to match the packet first.
Action	Select the action applied to the packet matched this ACE. Permit or deny the packets into switch core, or shutdown the port for stopping further transmission.

Protocol	Specify the protocol for filtering. **Any**: All packets will be filtered. **Select**: Choose one of the protocol (e.g., ICMP, IP in IP, TCP, EGP, IGP…) from the drop down list. Packets passing through the selected protocol will be filtered. **Define**: Specify a protocol number (0-255). For example, 6 for TCP, 17 for UDP…,etc.
Source IP	Specify the source IPv4 address for filtering. **Any**: All packets will be filtered. Or, enter the IP address to filter the packets coming from that address.
Destination IP	Specify the destination IPv4 address for filtering. **Any**: All packets will be filtered. Or, enter the IP address to filter the packets coming from that address.
Type of Service	**Any**: All packets will be filtered. **DSCP**: All IP traffic is mapped to queues based on the DSCP field in the IP header. If traffic is not IP traffic, it is mapped to the lowest priority queue. **IP Precedence**: All IP traffic is mapped to queues based on the IP Precedence field in the IP header. If traffic is not IP traffic, it is mapped to the lowest priority queue.
Source Port	Specify the source port number for filtering the packets. **Any**: All packets will be filtered. **Single**: Only the packets passing through the number defined here will be filtered. **Range**: Only the packets passing through the port range defined here will be filtered.
Destination Port	Specify the destination port number for filtering the packets. **Any**: All packets will be filtered. **Single**: Only the packets passing through the number defined here will be filtered. **Range**: Only the packets passing through the port range defined here will

	be filtered.
TCP Flags	Specify the TCP Flag (control bit) options.
ICMP Type	**Any**: All packets will be filtered. **Select**: Choose one of the type (e.g., Destination Unreachable Echo Reply, MLD Query….) from the drop down list. **Define**: Specify a type number (0 – 255) for ICMP code. For example, 0 means “Echo Reply”; 254 means “RFC3692-style Experiment 2”.
ICMP Code	Each ICMP type can be defined with different codes. For example, if you define ICMP Type as “3”, then the available codes for Type 3 will be 0-15. **Any**: All packets will be filtered. Or, enter 0 to 255 based on the ICMP type specified.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

15.5 IPv6 ACL

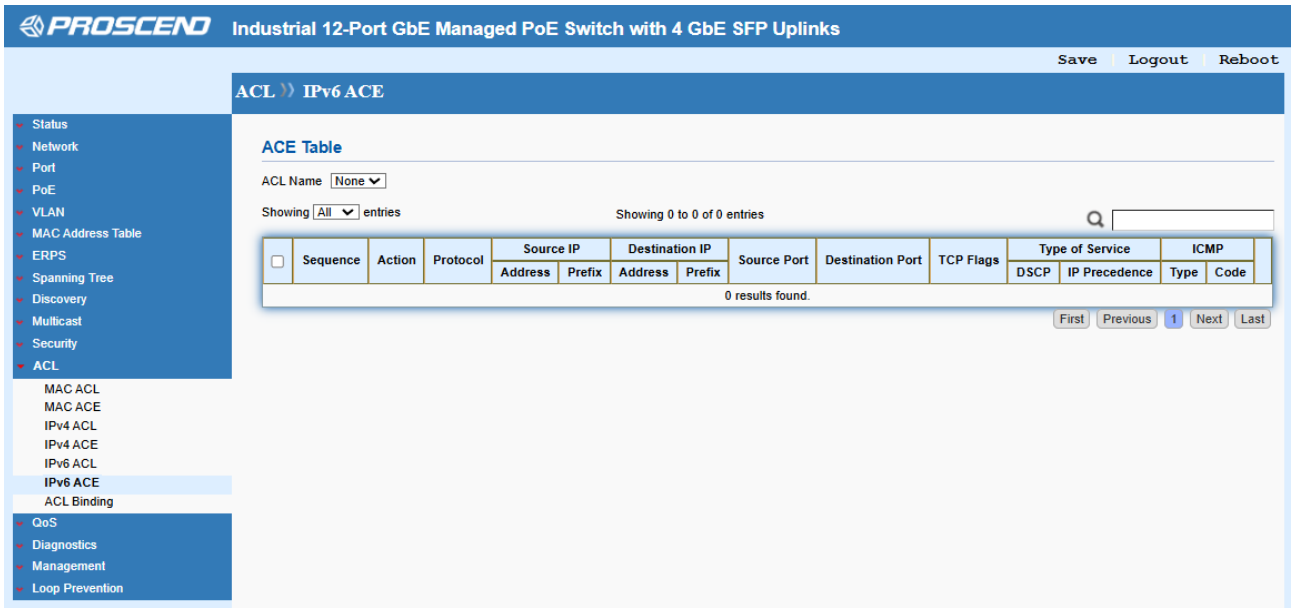
This page shows ACE based on Ipv6 address. You may choose ACL, permit, and deny particular packet or frame, even shutdown the port.



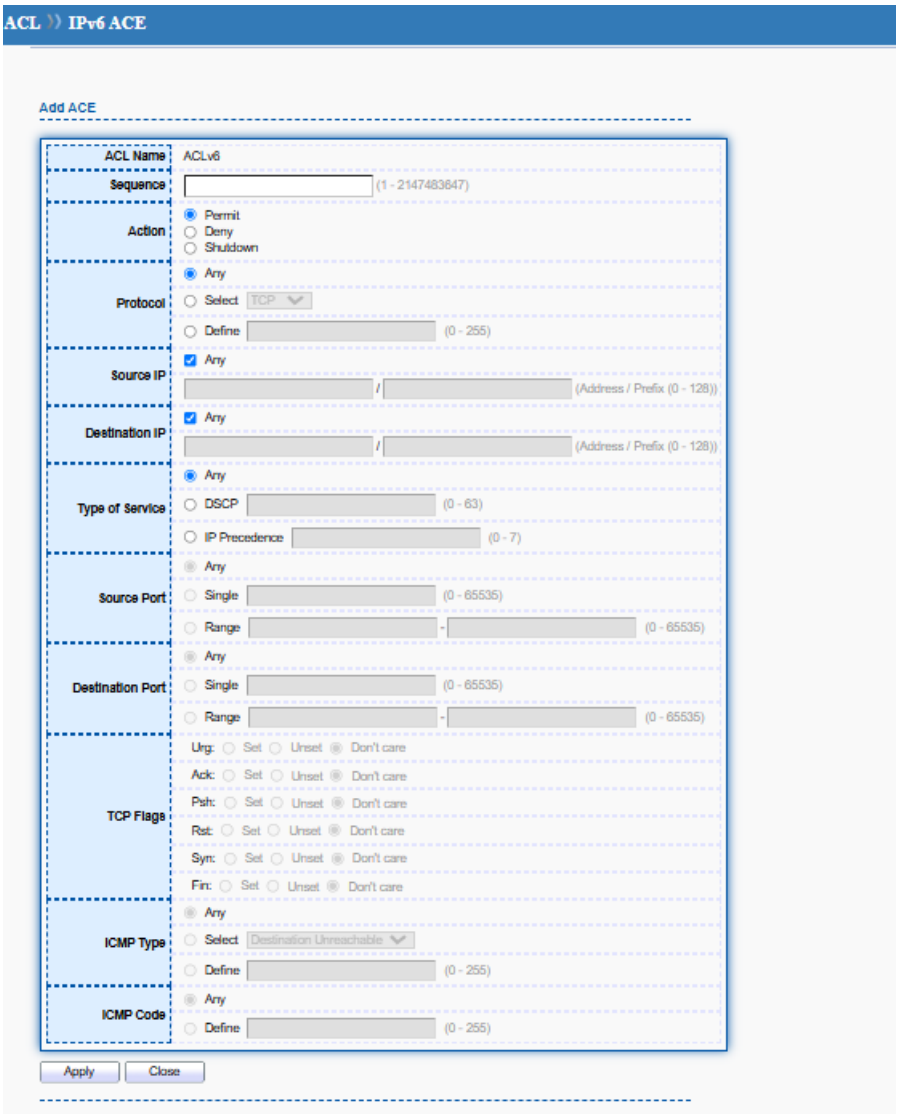
Item	Description
ACL Name	Enter the name for creating ACL profile.
Apply	Apply the settings to the switch.
Delete	Delete the selected entry.

15.6 IPv6 ACE

This page allows to create ACE based on IPv6 address.



Item	Description
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the selected entry.



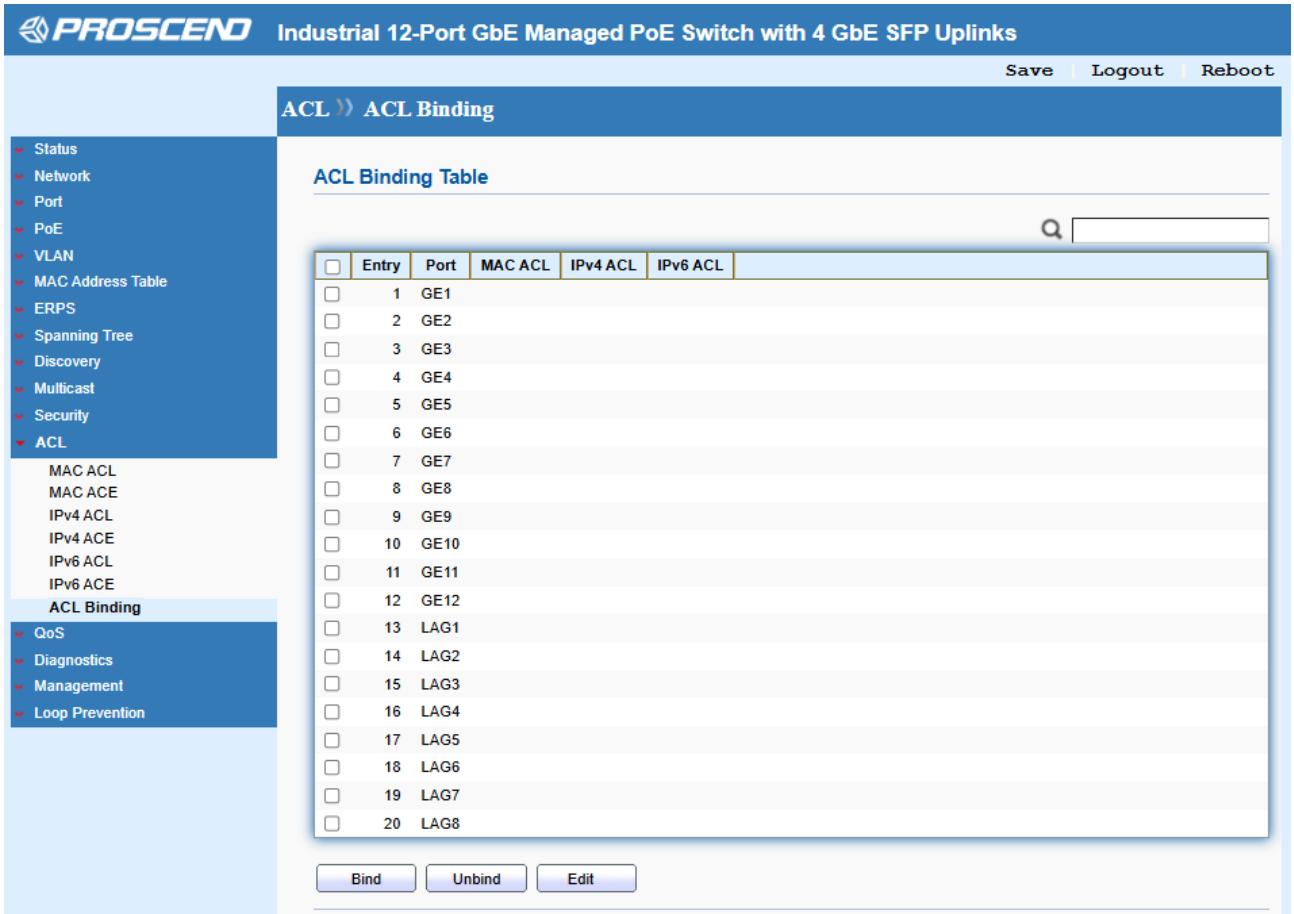
Item	Description
ACL Name	The name of selected ACL profile.
Sequence	Assign a sequence number to this ACE. The sequence is used to identify which one of ACEs in an ACL is firstly used to match ingress packets. The switch port bound with an ACL use the contained ACE rules, start with the one with lower sequence number to match the packet first.
Action	Select the action applied to the packet matched this ACE. Permit or deny the packets into switch core, or shutdown the port for stopping further transmission.
Protocol	Specify the protocol for filtering. **Any**: All packets will be filtered.

	Select: Choose one of the protocol (e.g., TCP/UDP/ICMP) from the drop down list. Packets passing through the selected protocol will be filtered. **Define**: Specify a protocol number (0-255). For example, 6 for TCP, 17 for UDP…,etc.
Source IP	Specify the source IPv4 address for filtering. **Any**: All packets will be filtered. Or, enter the IP address to filter the packets coming from that address.
Destination IP	Specify the destination IPv4 address for filtering. **Any**: All packets will be filtered. Or, enter the IP address to filter the packets coming from that address.
Type of Service	**Any**: All packets will be filtered. **DSCP**: All IP traffic is mapped to queues based on the DSCP field in the IP header. If traffic is not IP traffic, it is mapped to the lowest priority queue. **IP Precedence**: All IP traffic is mapped to queues based on the IP Precedence field in the IP header. If traffic is not IP traffic, it is mapped to the lowest priority queue.
Source Port	Specify the source port number for filtering the packets. **Any**: All packets will be filtered. **Single**: Only the packets passing through the number defined here will be filtered. **Range**: Only the packets passing through the port range defined here will be filtered.
Destination Port	Specify the destination port number for filtering the packets. **Any**: All packets will be filtered. **Single**: Only the packets passing through the number defined here will be filtered. **Range**: Only the packets passing through the port range defined here will be filtered.
TCP Flags	Specify the TCP Flag (control bit) options.

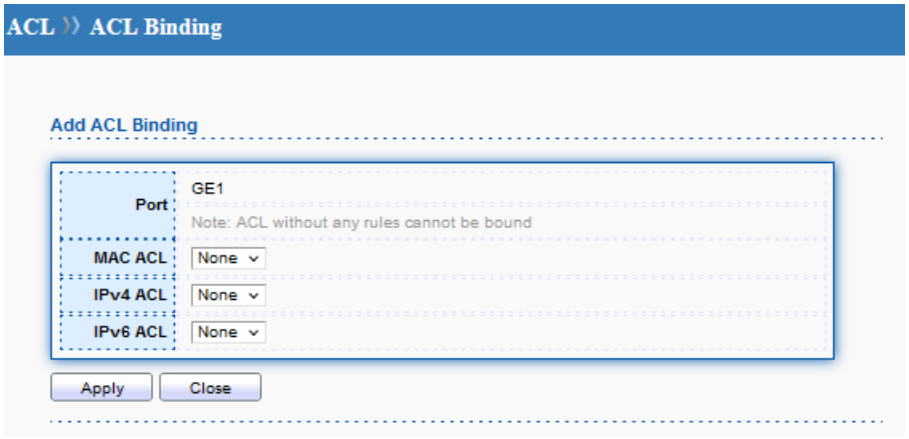
ICMP Type	**Any**: All packets will be filtered. **Select**: Choose one of the type (e.g., Destination Unreachable Echo Reply, MLD Query….) from the drop down list. **Define**: Specify a type number (0 – 255) for ICMP code. For example, 0 means “Echo Reply”; 254 means “RFC3692-style Experiment 2”.
ICMP Code	Each ICMP type can be defined with different codes. For example, if you define ICMP Type as “3”, then the available codes for Type 3 will be 0-15. **Any**: All packets will be filtered. Or, enter 0 to 255 based on the ICMP type specified.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

15.7 ACL Binding

This section allows to bind Access Control Lists created in previous section to an interface (physical port or aggregation). A physical port can only be bound with one of the IPv4 and IPv6 ACL, not both.



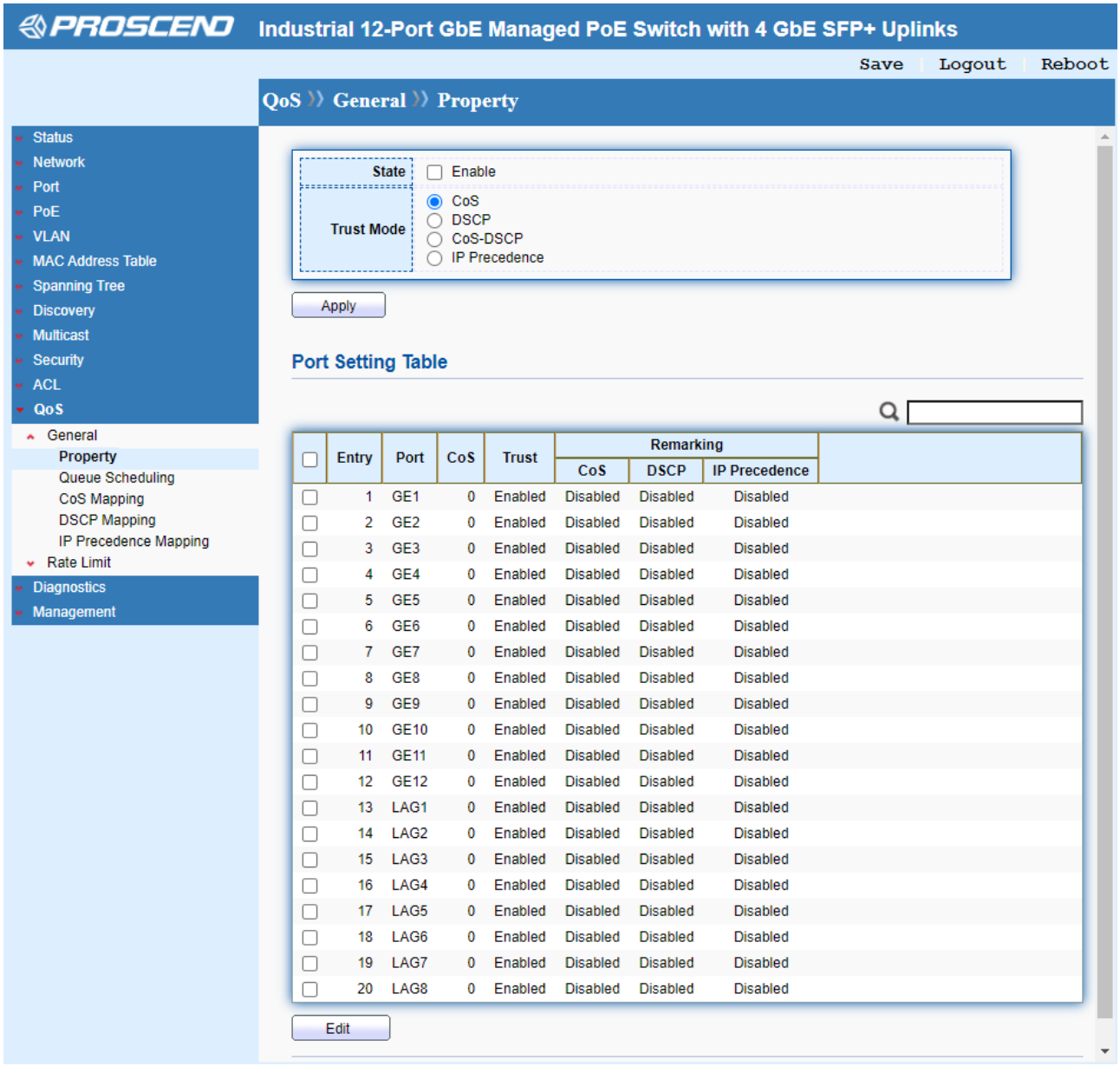
Item	Description
Bind	Edit the settings of specified port(s).
Unbind	Unbind all existing ACL rules on specified port(s).
Edit	Edit the existing entry.



Item	Description
Port	The index number of selected port.
MAC ACL	Select MAC ACLs to be bound on this port, so Switch may filter packets by using it.
IPv4 ACL	Select IPv4 ACLs to be bound on this port, so Switch may filter packets by using it.
IPv6 ACL	Select IPv6 ACLs to be bound on this port, so Switch may filter packets by using it.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

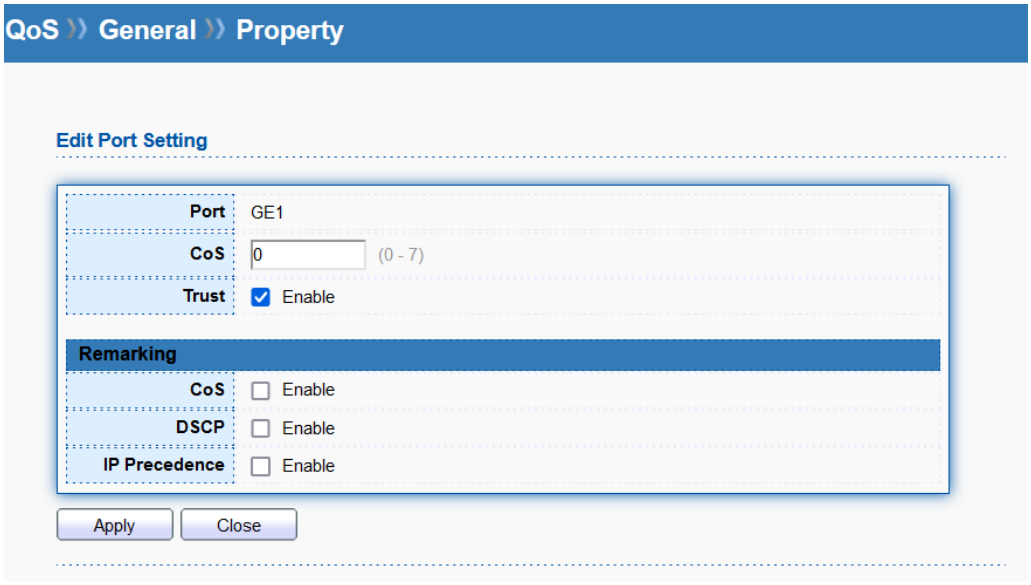
15.7.1 Property

This page allows to specify Ingress Trust Mode for basic QoS mode.



Item	Description
State	Enable or disable the function of QoS mode.
Trust Mode	Select the QoS operation mode. **CoS**: Traffic is mapped to queues based on the CoS field in the VLAN tag, or based on the per-port default CoS value if there is no VLAN tag on the incoming packet. **DSCP**: All IP traffic is mapped to queues based on the DSCP field in

	the IP header. If traffic is not IP traffic, it is mapped to the lowest priority queue. **CoS-DSCP**: All IP traffic is mapped to queues based on the DSCP field in the IP header. If traffic is not IP but has VLAN tag, mapped to queues based on the CoS value in the VLAN tag. **IP Precedence**: All IP traffic is mapped to queues based on the DSCP field in the IP header. If traffic is not IP but has VLAN tag, mapped to queues based on the CoS value in the VLAN
Apply	Apply the settings to the switch.
Edit	Edit the selected port(s).

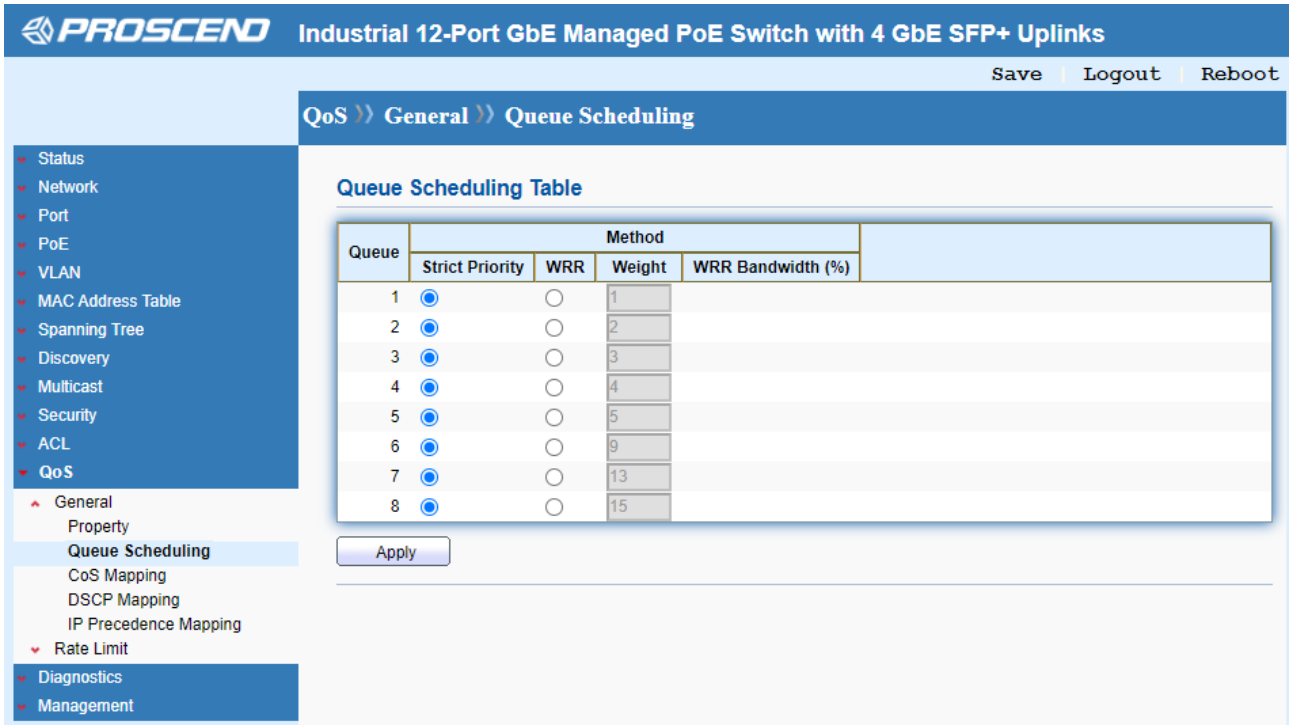


Item	Description
Port	The index number of selected port.
CoS	Specify the default CoS priority value for those ingress frames without given trust QoS tag (802.1q/DSCP/IP Precedence, depending on configuration).
Trust	**Enable**: Traffic will follow trust mode in general setting. **Disable**: No QoS service for this port.
Remarking	
CoS	**Enable**: Egress traffic will be marked with CoS value according to the Queue to CoS mapping table.

	Disable: Disable CoS remarking function for outgoing packets.
DSCP	Egress traffic will be marked with DSCP value according to the Queue to DSCP mapping table once it is enabled.
IP Precedence	Egress traffic will be marked with IP Precedence value according to the Queue to IP Precedence mapping table once it is enabled.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

15.7.2 Queue Scheduling

The Switch supports multiple queues for each interface. The higher numbered queue represents the higher priority.

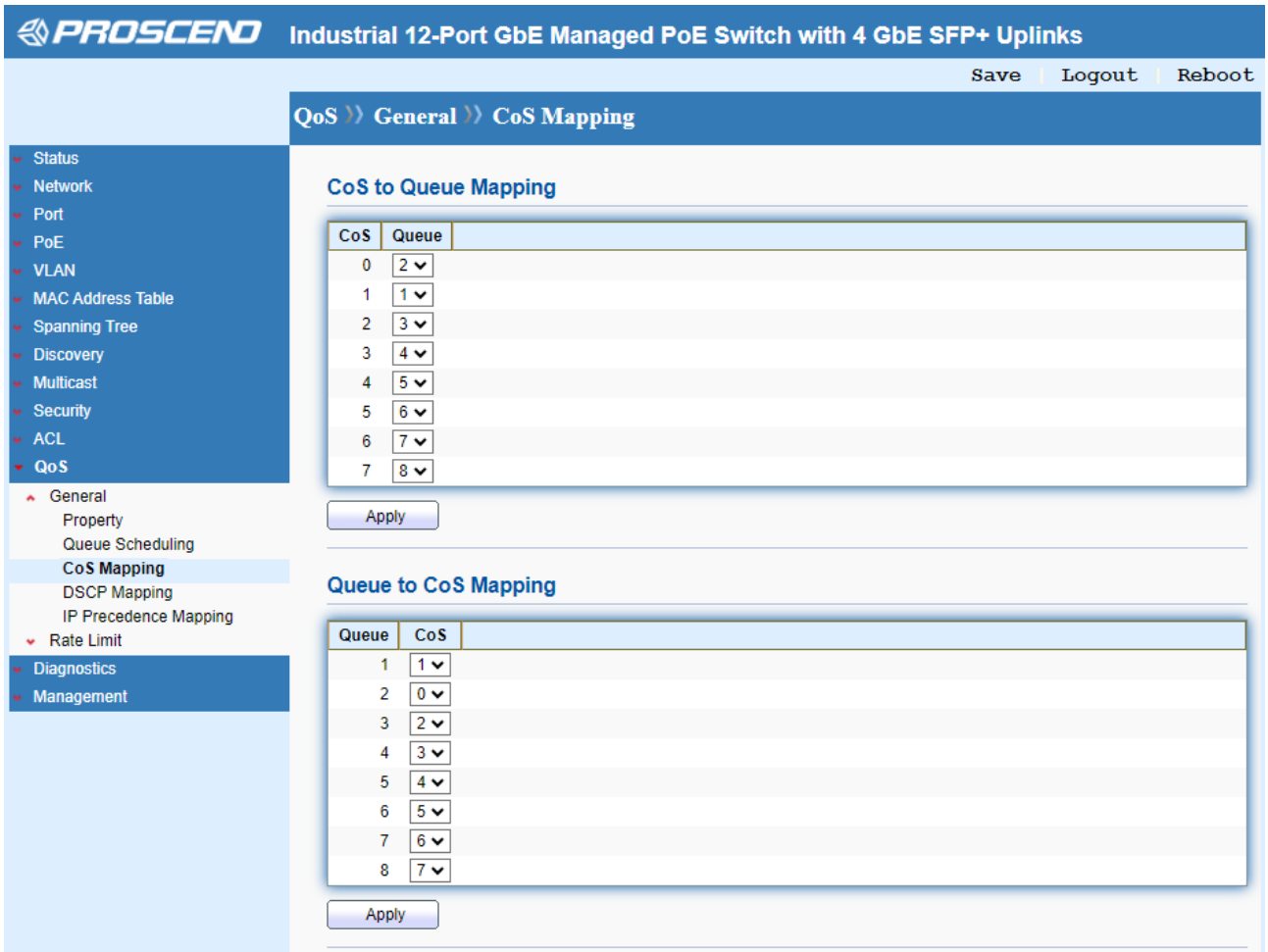


Item	Description
Queue	There are eight queue ID numbers allowed to be configured.
Strict Priority	Egress traffic from the higher priority queue will be transmitted first, lower priority queue shall wait until all traffic in SP queue is transmitted.
WRR	The number of packets sent from the queue is proportional to the weight of the queue.

Weight	If the queue type is WRR, set the queue weight for the queue.
WRR Bandwidth (%)	Display the percentage of traffic which can be sent by current queue compared to total WRR queues.
Apply	Apply the settings to the switch.

15.7.3 CoS Mapping

This section allows to configure how ingress frames with CoS/802.1p tag map to QoS queues, and QoS queues to CoS/802.1p on egress frames. Actual effectiveness is based on how QoS is configured in previous QoS section. This page provides settings for user to configure mapping only.

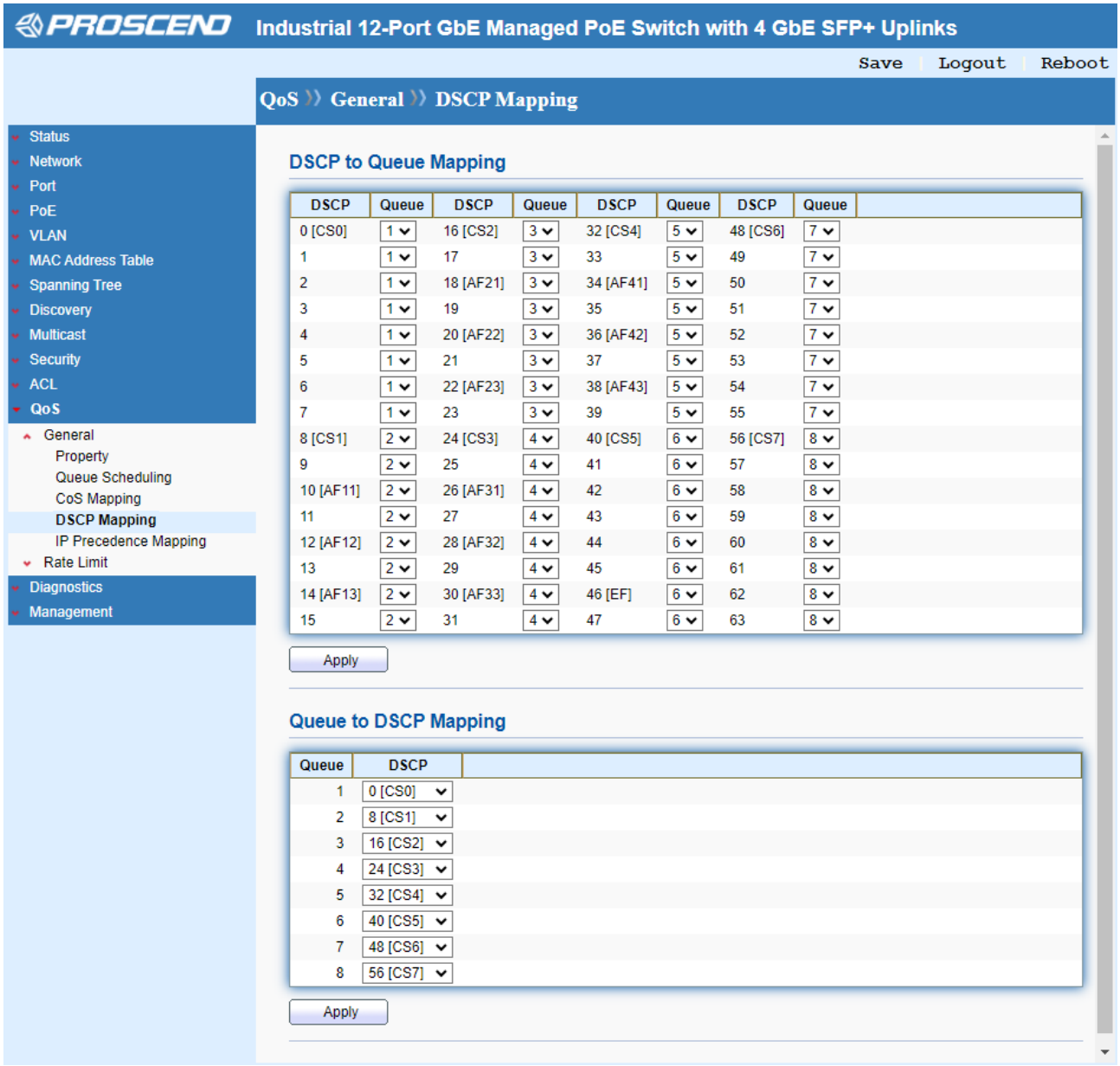


Item	Description
CoS to Queue Mapping	
CoS	Display the class of service value (0 to 7).

Queue	Define the queue ID (level 1 to 8) for different CoS values.
Apply	Apply the settings to the switch.
Queue to CoS Mapping	
Queue	Display the queue ID (level 1 to 8) for different CoS values.
CoS	Display the class of service value (0 to 7).
Apply	Apply the settings to the switch.

15.7.4 DSCP Mapping

This section allows to configure how ingress packets with DSCP tag map to QoS queues, and QoS queues to DSCP on egress packets. Actual effectiveness is based on how QoS is configured in previous QoS section. This page provides settings for user to configure mapping only.

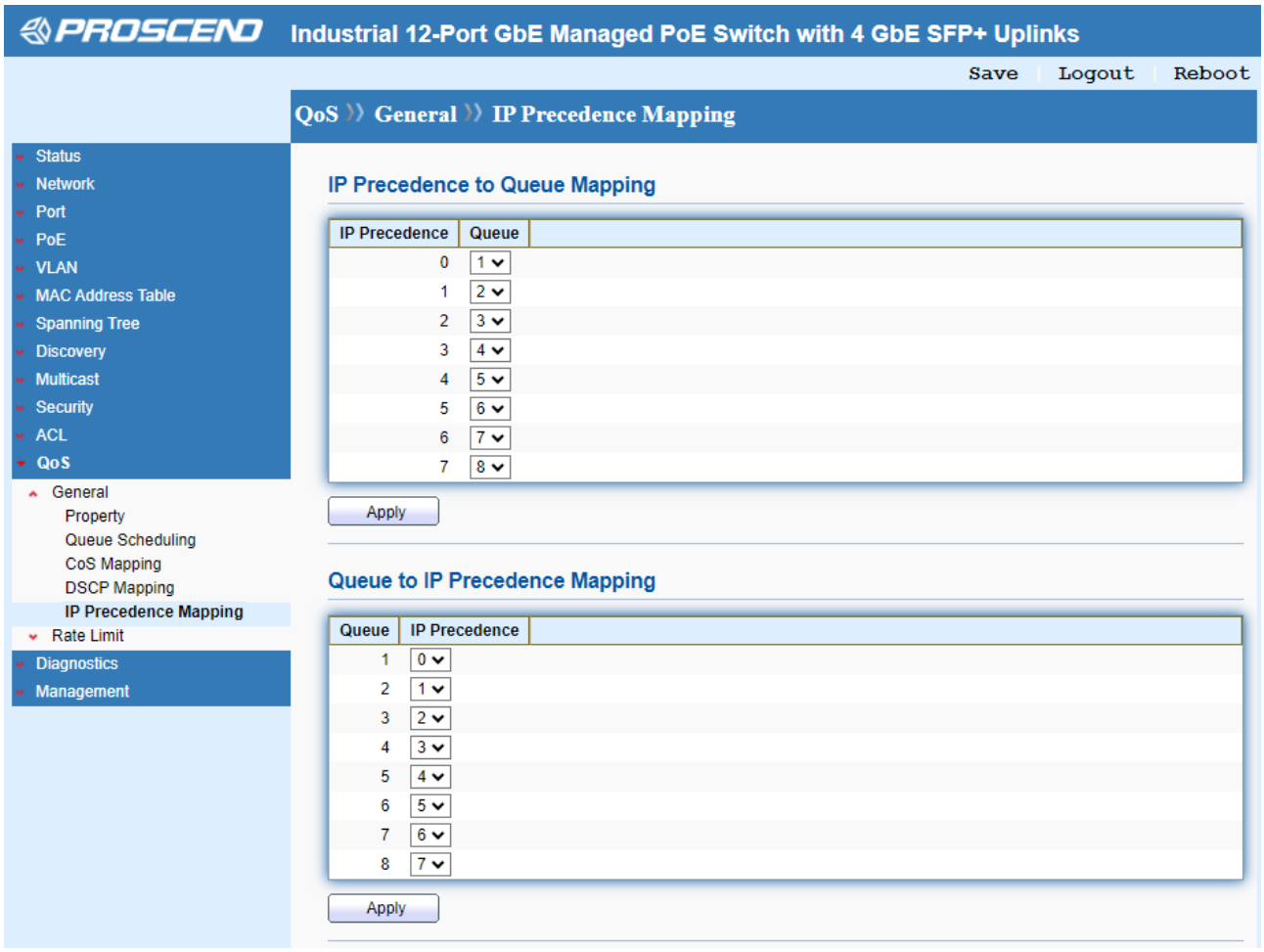


Item	Description
DSCP to Queue Mapping	
DSCP	Display the DSCP value (0 to 63).
Queue	Define the queue ID (level 1 to 8) for different DSCP values.
Apply	Apply the settings to the switch.
Queue to DSCP Mapping	
Queue	Display the queue ID (level 1 to 8) for different DSCP values.
DSCP	Display the DSCP value (0 to 63).
Apply	Apply the settings to the switch.

15.7.5 IP Precedence Mapping

This section allows to configure how ingress packets with IP Precedence tag map to QoS

queues, and QoS queues to IP Precedence on egress packets. Actual effectiveness is based on how QoS is configured in previous QoS section. This page provides settings for user to configure mapping only.

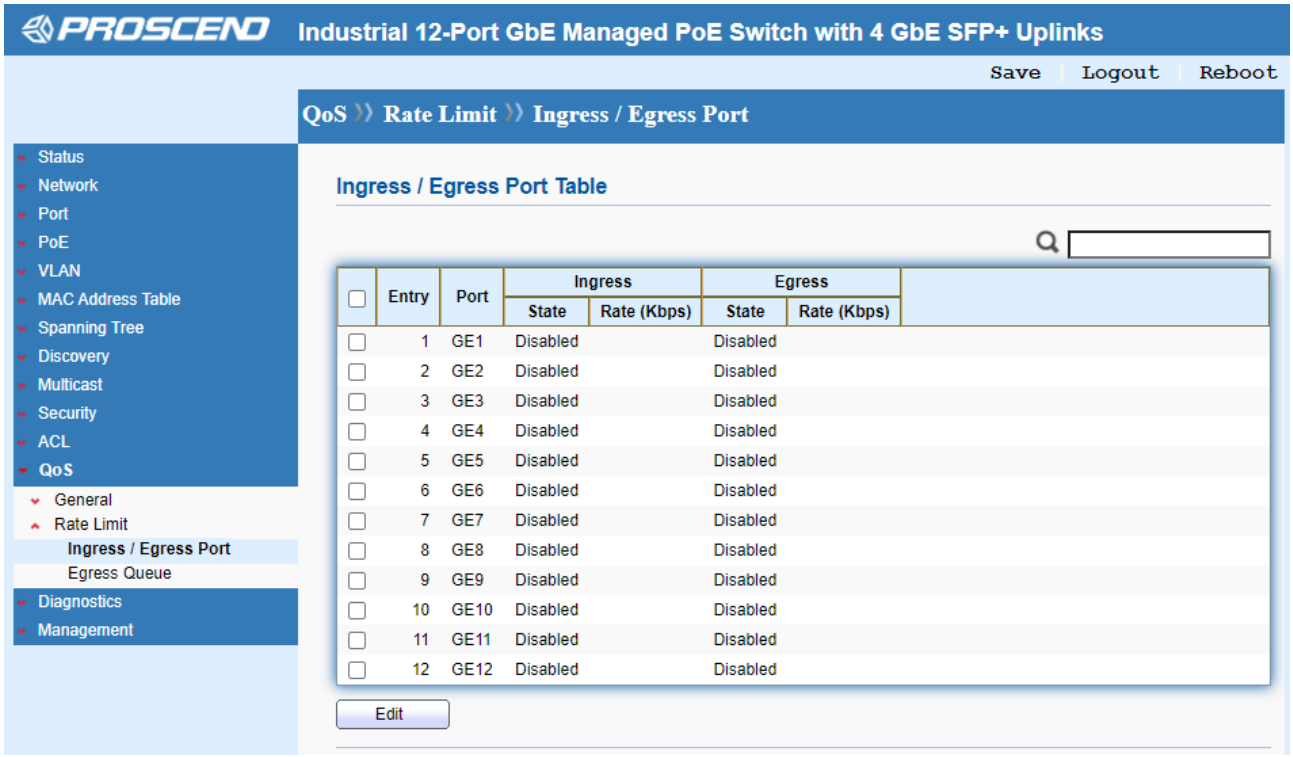


Item	Description
IP Precedence to Queue Mapping	
IP Precedence	Display the IP Precedence value (0 to 7).
Queue	Define the queue ID (level 1 to 8) for different IP Precedence values.
Apply	Apply the settings to the switch.
Queue to IP Precedence Mapping	
Queue	Display the queue ID (level 1 to 8) for different IP Precedence values.
IP Precedence	Display the IP Precedence value (0 to 7).
Apply	Apply the settings to the switch.

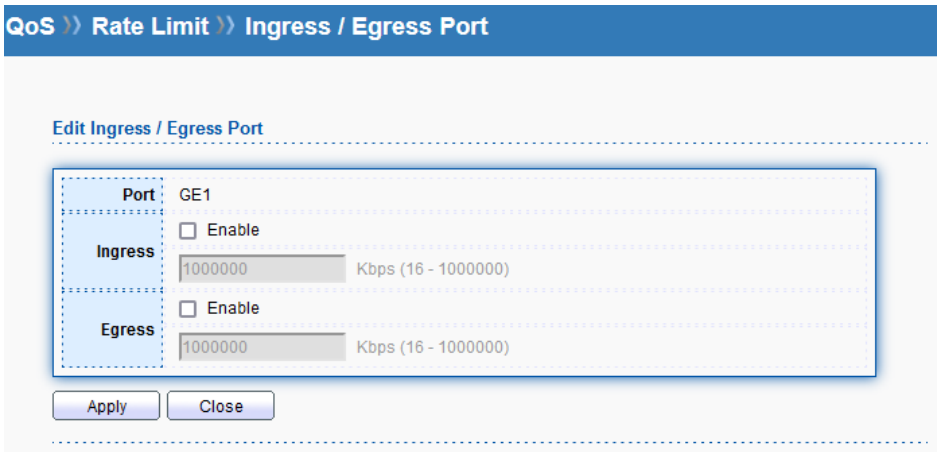
Use the Rate Limit setting pages to define values that determine how much traffic the switch can receive and send on specific port or queue.

15.7.1 Ingress/Egress Port

This page allows to configure ingress/egress port rate limit. The ingress/egress rate limit is the number of bits per second that can be received from the ingress interface. Excess bandwidth above this limit is discarded. The configuration result for each port will be displayed on the table listed on the lower side of this web page.

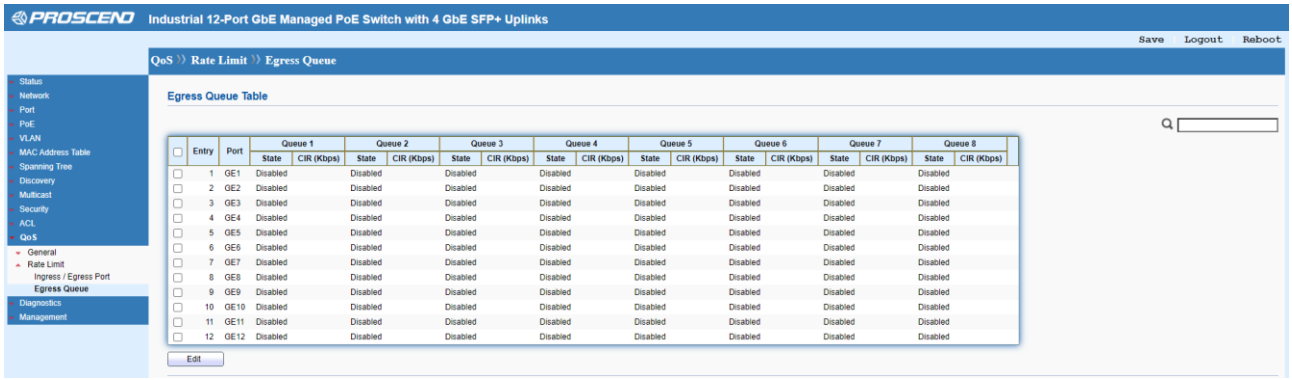


Item	Description
Edit	Edit the selected port(s).

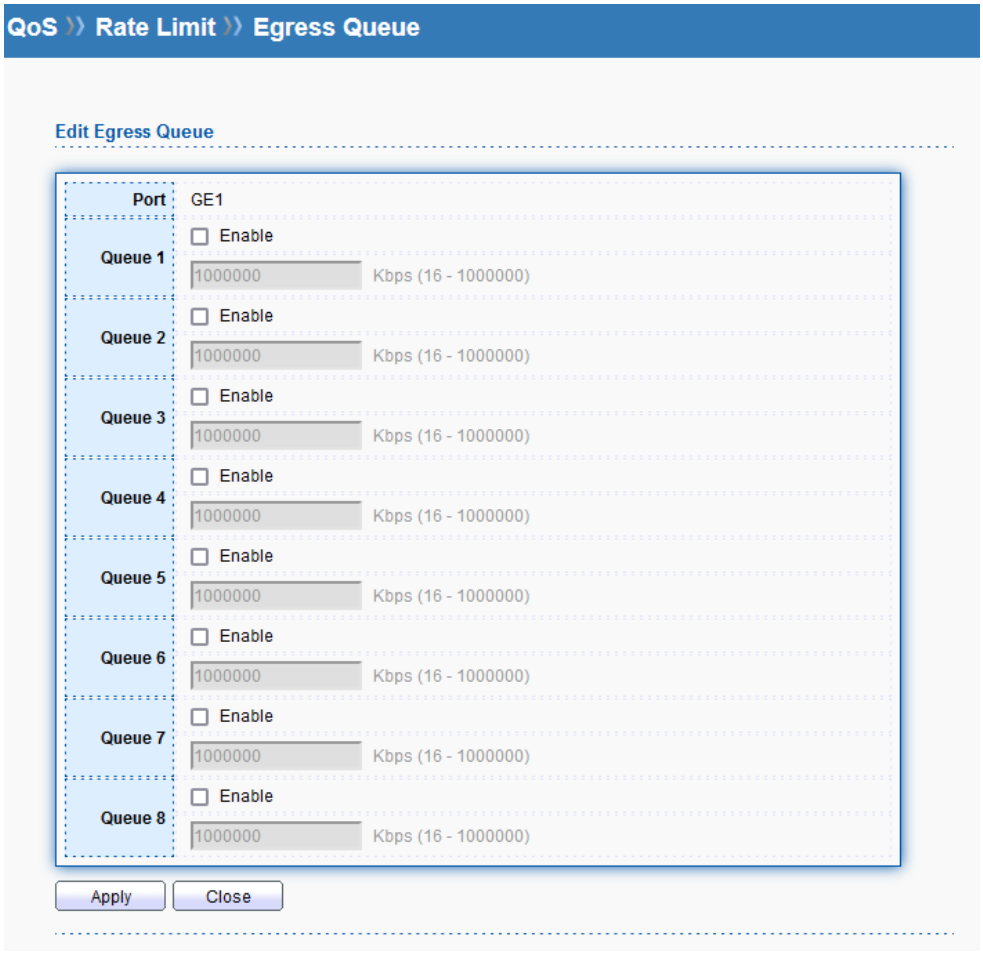


Item	Description
Port	The index number of selected port.
Ingress	Enable or disable ingress bandwidth control. Enter the rate value,<16-1000000>, unit:16 Kbps.
Egress	Enable or disable Egress bandwidth control. Enter the rate value,<16-1000000>, unit:16 Kbps.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

15.7.2 Egress Queue



Item	Description
Edit	Edit the selected port(s).



Item	Description
Port	The index number of selected port.
Queue (1~8)	Total eight queue rules. Enable or disable egress bandwidth control. Enter the rate value,<16-1000000>, unit:16 Kbps.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

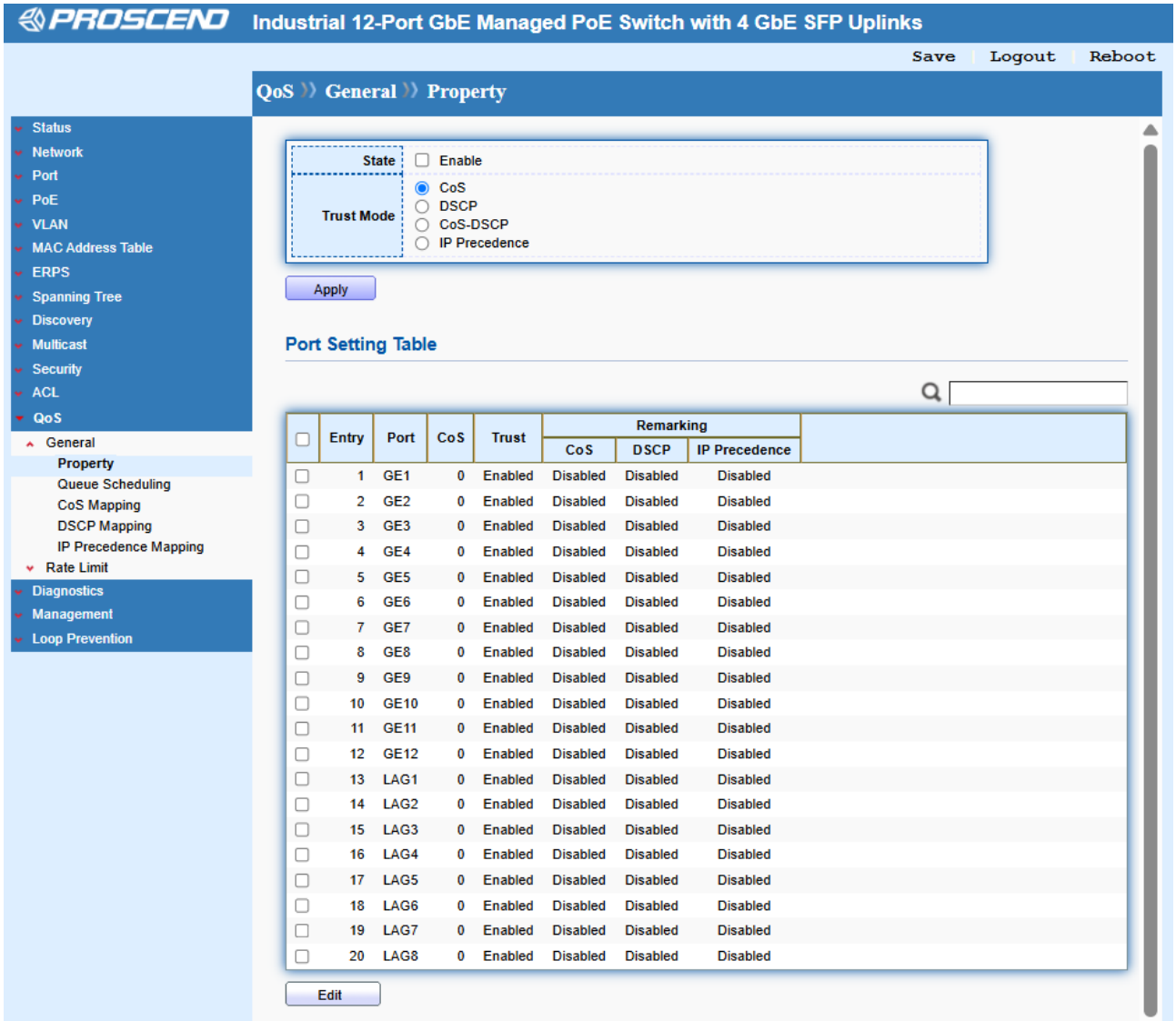
16 QoS

QoS (Quality of Service) functions to provide different quality of service for various network applications and requirements and optimize the bandwidth resource distribution so as to provide a network service experience of a better quality.

16.1 General

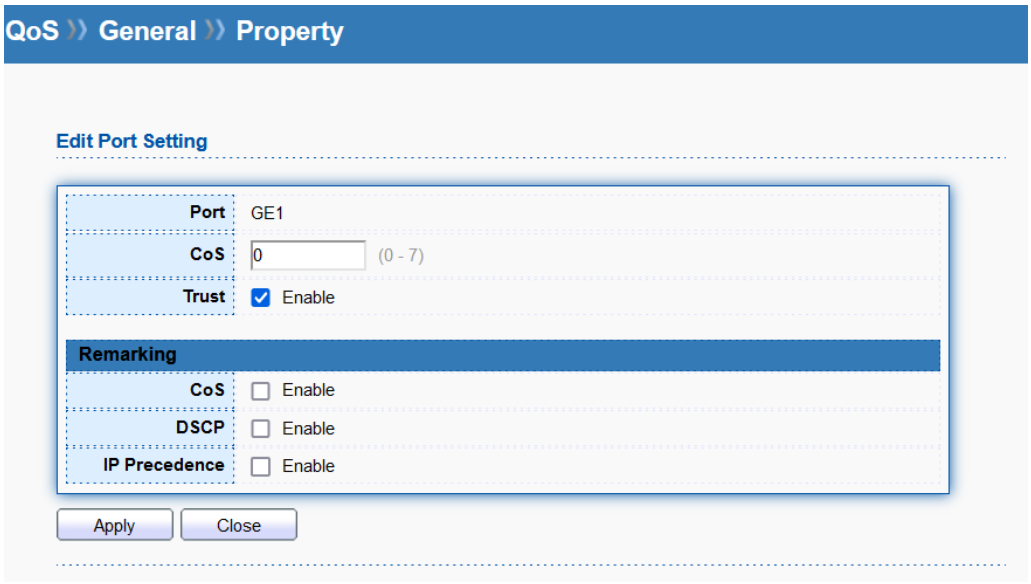
16.1.0 Property

This page allows to specify Ingress Trust Mode for basic QoS mode.



Item	Description
State	Enable or disable the function of QoS mode.

Trust Mode	Select the QoS operation mode. **CoS**: Traffic is mapped to queues based on the CoS field in the VLAN tag, or based on the per-port default CoS value if there is no VLAN tag on the incoming packet. **DSCP**: All IP traffic is mapped to queues based on the DSCP field in the IP header. If traffic is not IP traffic, it is mapped to the lowest priority queue. **CoS-DSCP**: All IP traffic is mapped to queues based on the DSCP field in the IP header. If traffic is not IP but has VLAN tag, mapped to queues based on the CoS value in the VLAN tag. **IP Precedence**: All IP traffic is mapped to queues based on the DSCP field in the IP header. If traffic is not IP but has VLAN tag, mapped to queues based on the CoS value in the VLAN
Apply	Apply the settings to the switch.
Edit	Edit the selected port(s).

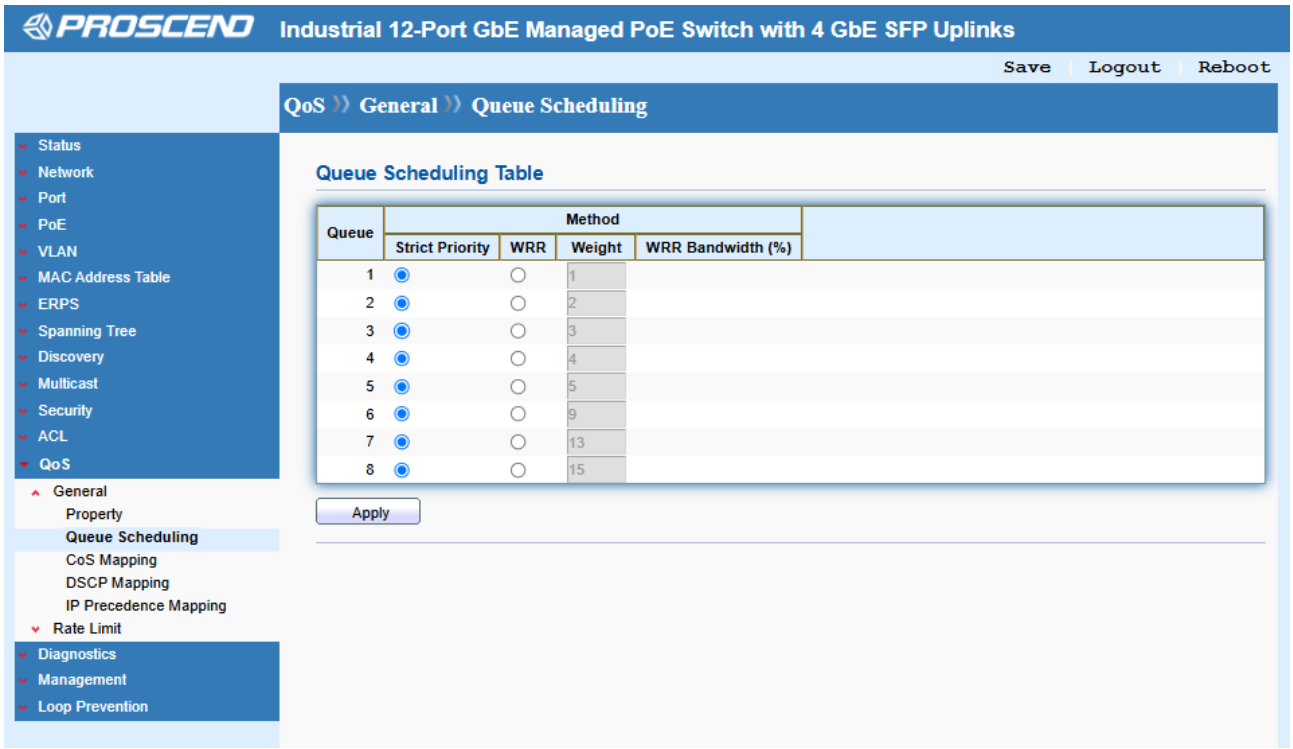


Item	Description
Port	The index number of selected port.
CoS	Specify the default CoS priority value for those ingress frames without given trust QoS tag (802.1q/DSCP/IP Precedence, depending on configuration).
Trust	**Enable**: Traffic will follow trust mode in general setting.

	Disable: No QoS service for this port.
Remarking	
CoS	Egress traffic will be marked with CoS value according to the Queue to CoS mapping table.
DSCP	Egress traffic will be marked with DSCP value according to the Queue to DSCP mapping table once it is enabled.
IP Precedence	Egress traffic will be marked with IP Precedence value according to the Queue to IP Precedence mapping table once it is enabled.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

16.1.1 Queue Scheduling

The Switch supports multiple queues for each interface. The higher numbered queue represents the higher priority.

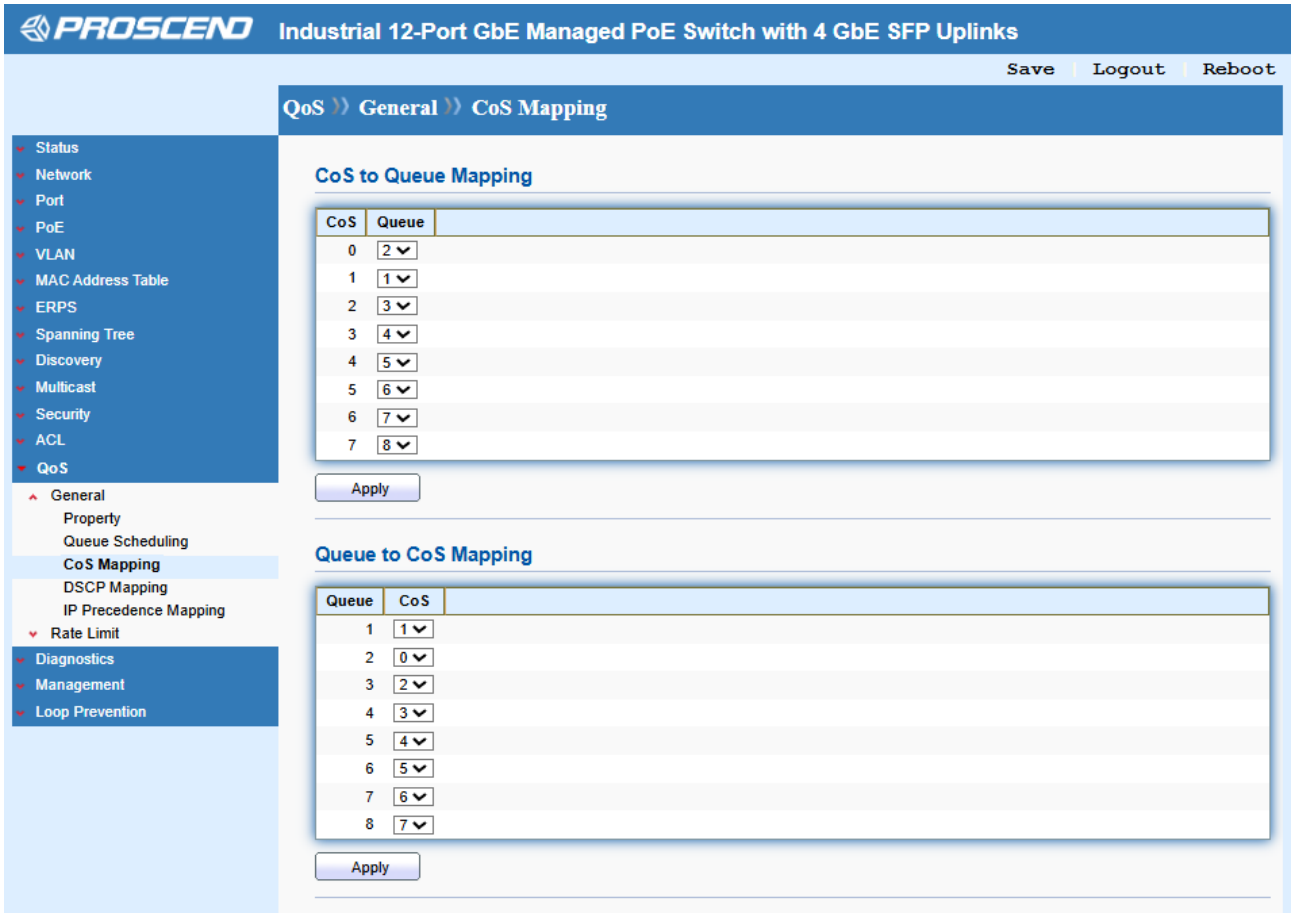


Item	Description
Queue	There are eight queue ID numbers allowed to be configured.
Strict Priority	Egress traffic from the higher priority queue will be transmitted first, lower priority queue shall wait until all traffic in SP queue is

	transmitted.
WRR	The number of packets sent from the queue is proportional to the weight of the queue.
Weight	If the queue type is WRR, set the queue weight for the queue.
WRR Bandwidth (%)	Display the percentage of traffic which can be sent by current queue compared to total WRR queues.
Apply	Apply the settings to the switch.

16.1.2 CoS Mapping

This section allows to configure how ingress frames with CoS/802.1p tag map to QoS queues, and QoS queues to CoS/802.1p on egress frames. Actual effectiveness is based on how QoS is configured in previous QoS section. This page provides settings for user to configure mapping only.

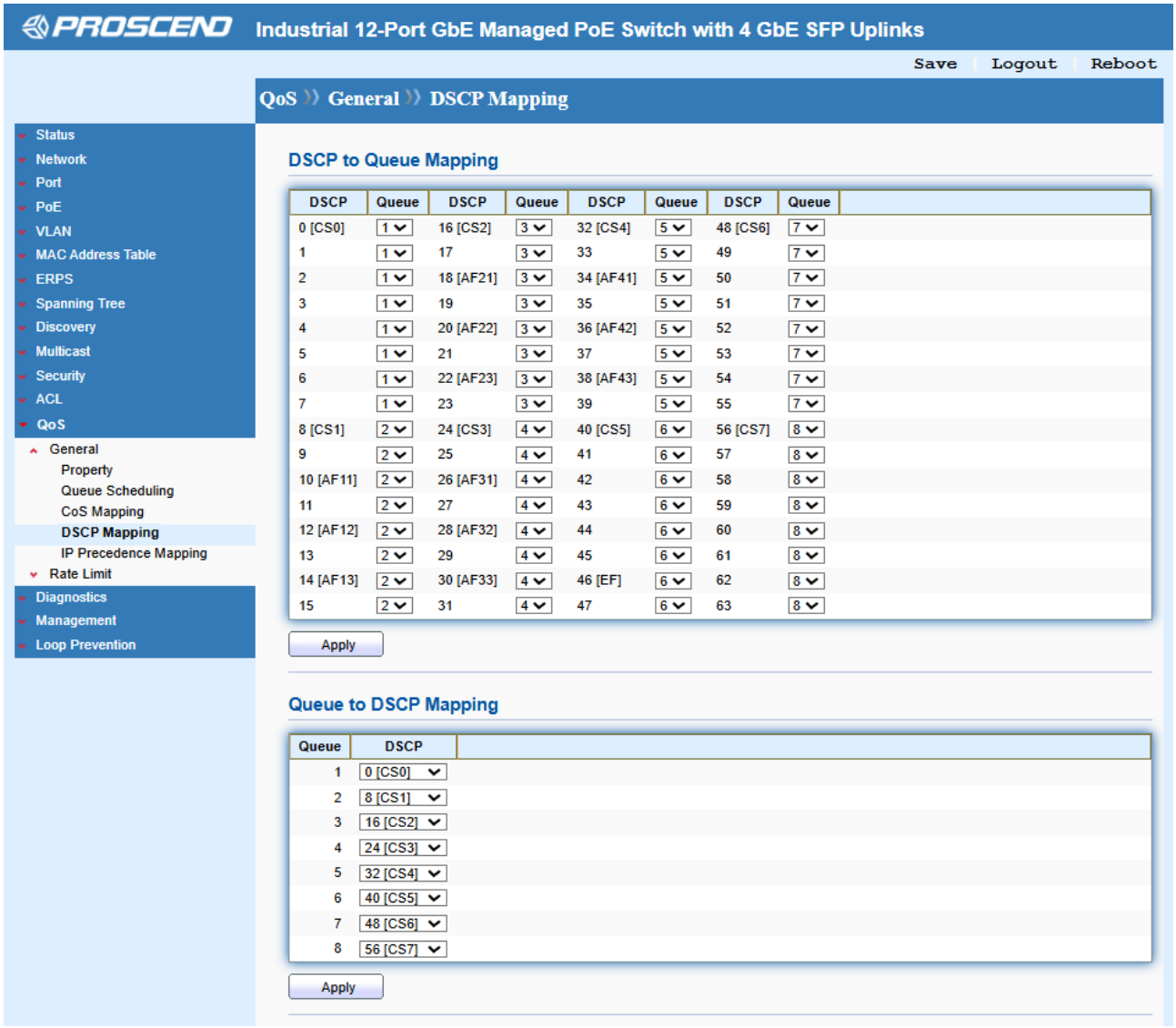


Item	Description
CoS to Queue Mapping	
CoS	Display the class of service value (0 to 7).

Queue	Define the queue ID (level 1 to 8) for different CoS values.
Apply	Apply the settings to the switch.
Queue to CoS Mapping	
Queue	Display the queue ID (level 1 to 8) for different CoS values.
CoS	Display the class of service value (0 to 7).
Apply	Apply the settings to the switch.

16.1.3 DSCP Mapping

This section allows to configure how ingress packets with DSCP tag map to QoS queues, and QoS queues to DSCP on egress packets. Actual effectiveness is based on how QoS is configured in previous QoS section. This page provides settings for user to configure mapping only.



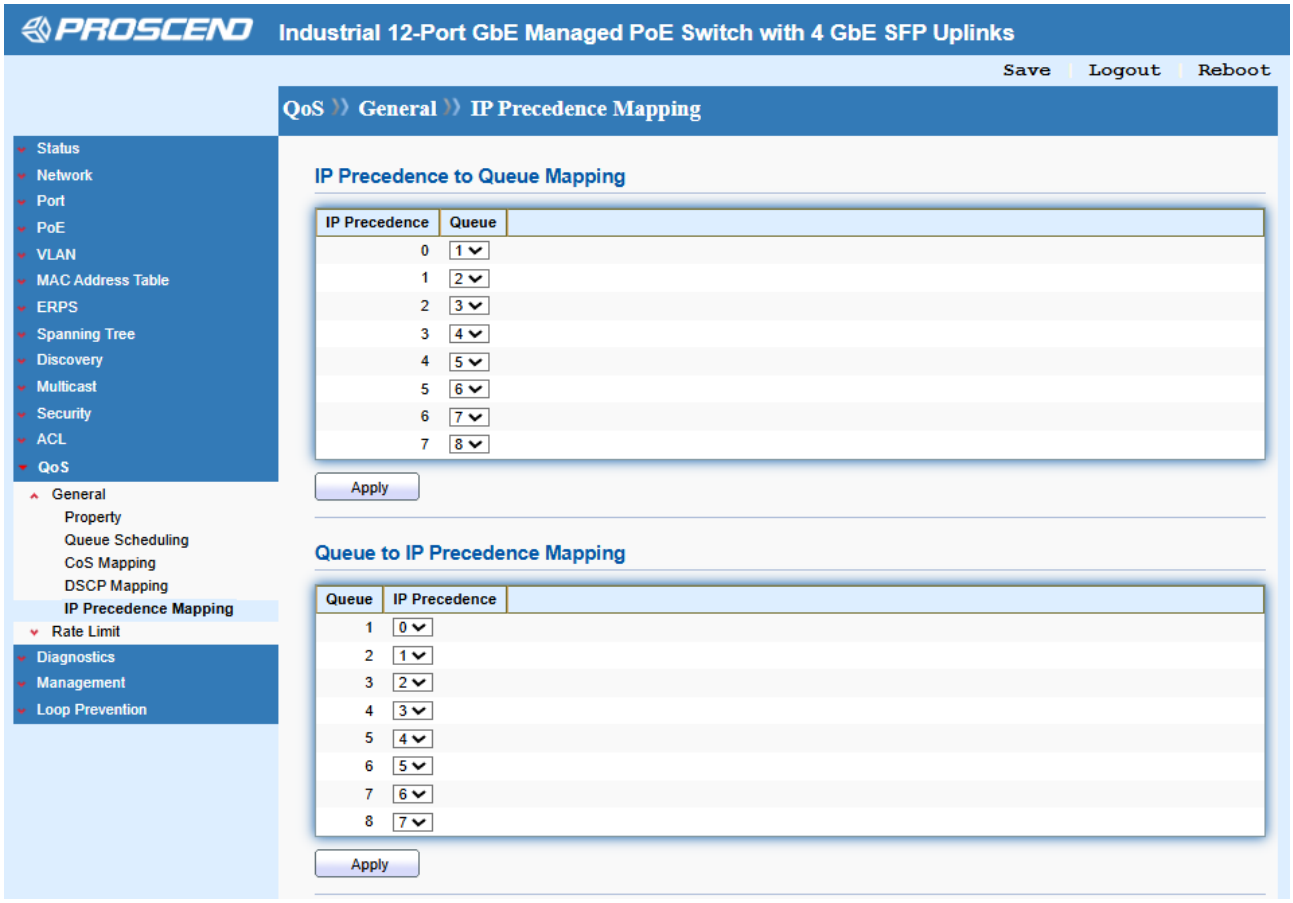
Item	Description
DSCP to Queue Mapping	
DSCP	Display the DSCP value (0 to 63).
Queue	Define the queue ID (level 1 to 8) for different DSCP values.
Apply	Apply the settings to the switch.
Queue to DSCP Mapping	

Queue	Display the queue ID (level 1 to 8) for different DSCP values.
DSCP	Display the DSCP value (0 to 63).
Apply	Apply the settings to the switch.

16.1.4 IP Precedence Mapping

This section allows to configure how ingress packets with IP Precedence tag map to QoS

queues, and QoS queues to IP Precedence on egress packets. Actual effectiveness is based on how QoS is configured in previous QoS section. This page provides settings for user to configure mapping only.



Item	Description
IP Precedence to Queue Mapping	
IP Precedence	Display the IP Precedence value (0 to 7).
Queue	Define the queue ID (level 1 to 8) for different IP Precedence values.
Apply	Apply the settings to the switch.
Queue to IP Precedence Mapping	
Queue	Display the queue ID (level 1 to 8) for different IP Precedence values.

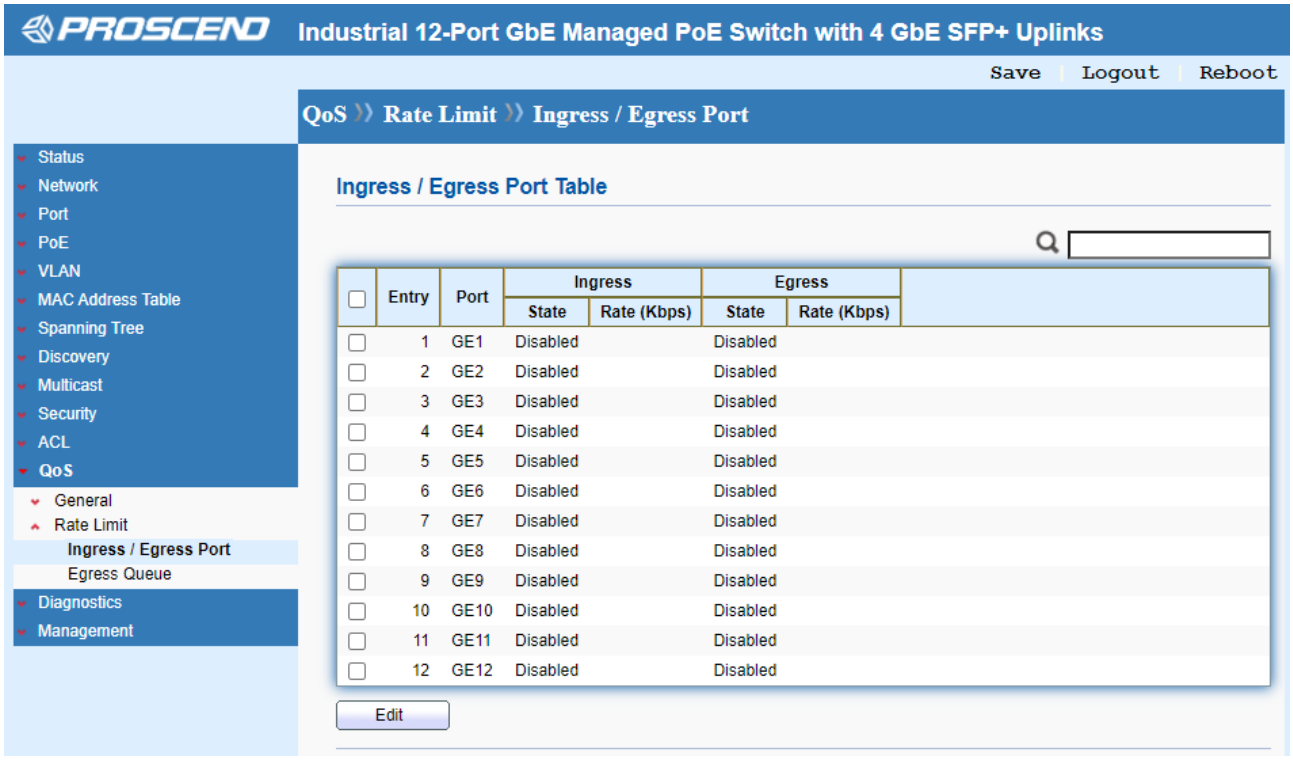
IP Precedence	Display the IP Precedence value (0 to 7).
Apply	Apply the settings to the switch.

16.2 Rate Limit

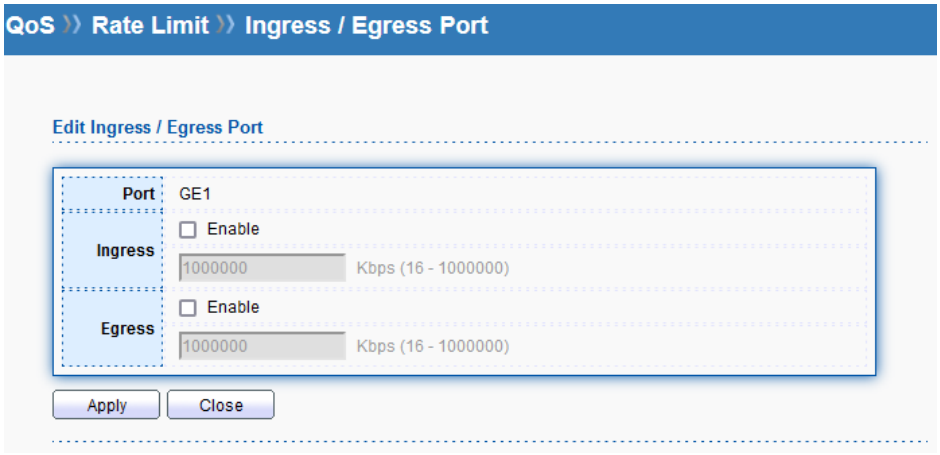
Use the Rate Limit setting pages to define values that determine how much traffic the switch can receive and send on specific port or queue.

16.2.0 Ingress/Egress Port

This page allows to configure ingress/egress port rate limit. The ingress/egress rate limit is the number of bits per second that can be received from the ingress interface. Excess bandwidth above this limit is discarded. The configuration result for each port will be displayed on the table listed on the lower side of this web page.

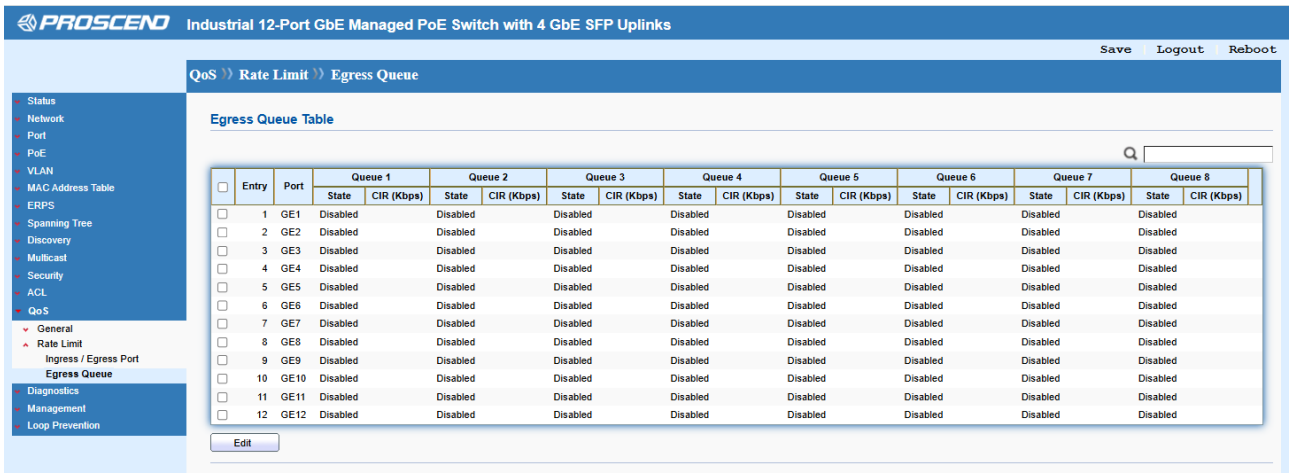


Item	Description
Edit	Edit the selected port(s).

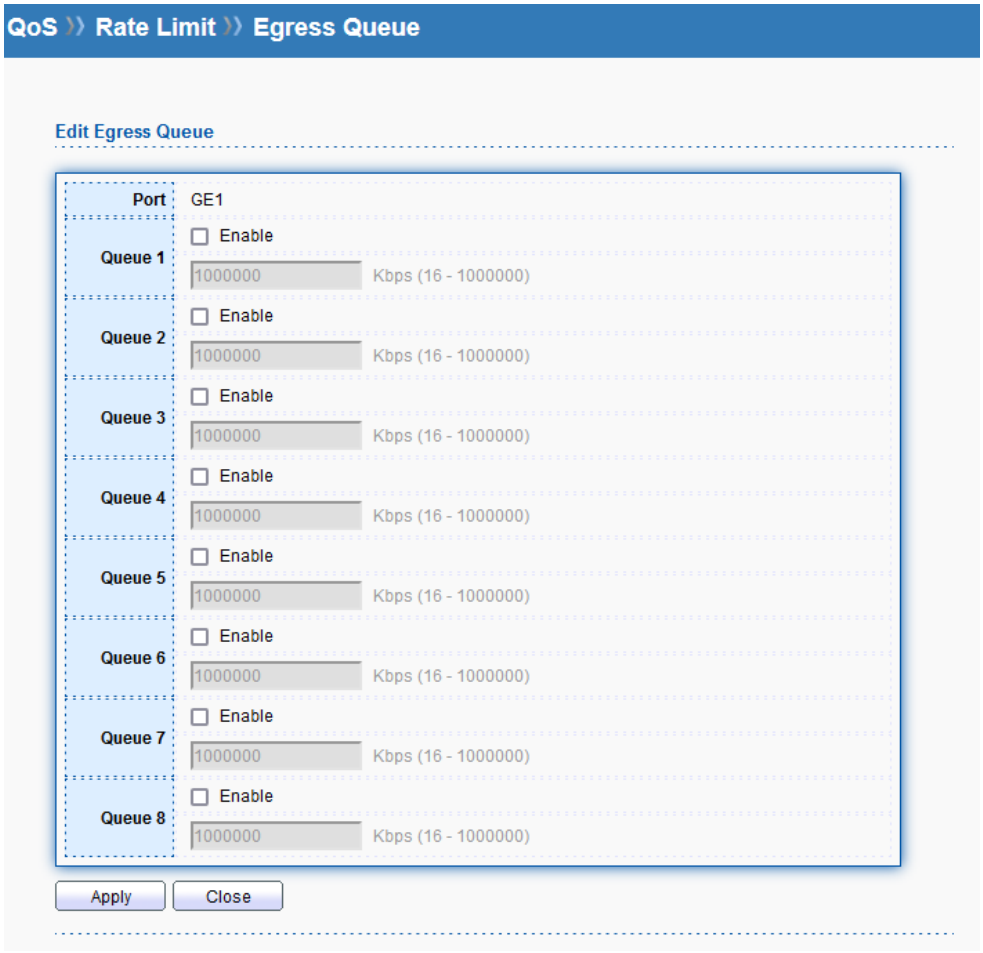


Item	Description
Port	The index number of selected port.
Ingress	Enable or disable ingress bandwidth control. Enter the rate value,<16-1000000>, unit:16 Kbps.
Egress	Enable or disable Egress bandwidth control. Enter the rate value,<16-1000000>, unit:16 Kbps.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

16.2.1 Egress Queue



Item	Description
Edit	Edit the selected port(s).



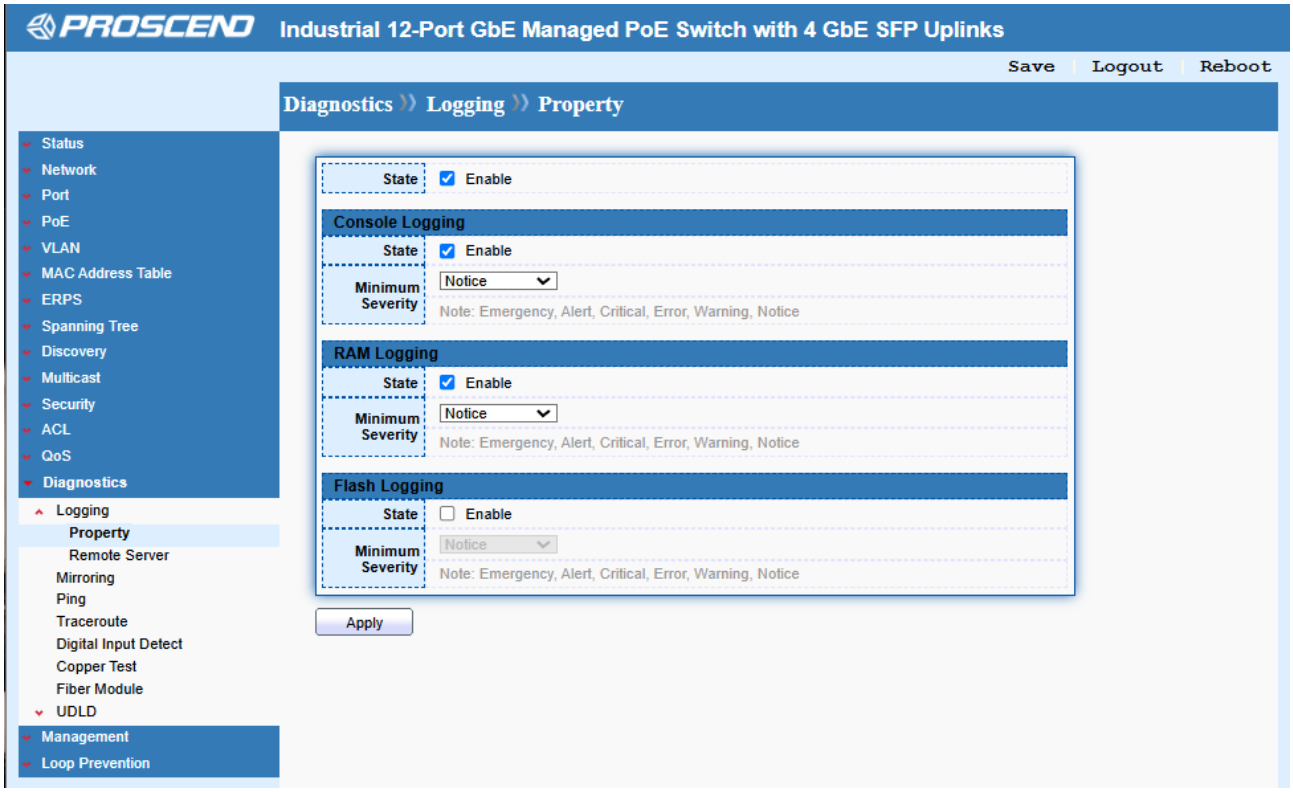
Item	Description
Port	The index number of selected port.
Queue (1~8)	Total eight queue rules. Enable or disable egress bandwidth control. Enter the rate value,<16-1000000>, unit:16 Kbps.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

17 Diagnostics

17.1 Logging

This section allows enable system logging into local syslog and specific remote syslog server for storage.

17.1.1 Property

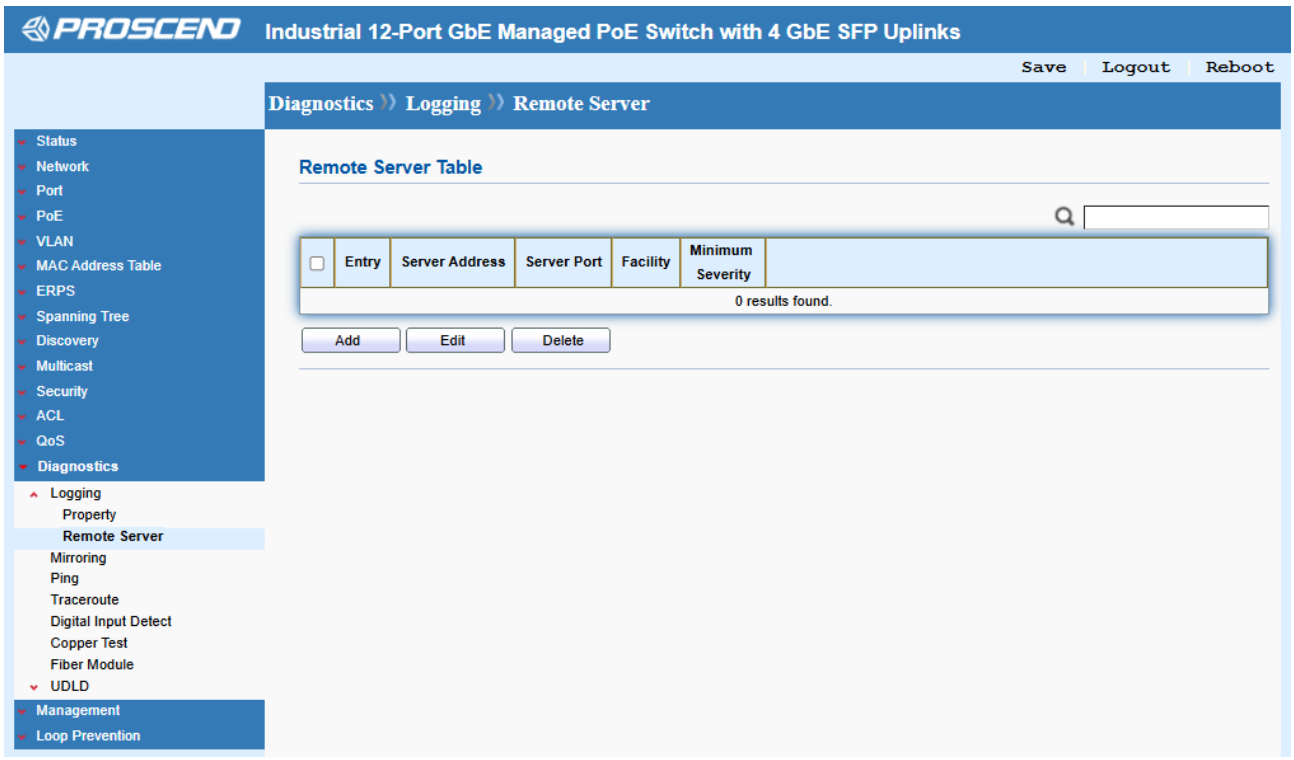


Item	Description
State	Enable or disable the function of syslog.
Console Logging	
State	Enable or disable to write log into console.
Minimum Severity	Select severity (Emergency, Alert, Critical, Error, Warning, Notice, informational and debug) of log messages which you wish to filter out for review.
RAM Logging	
State	Enable or disable to write log into RAM.

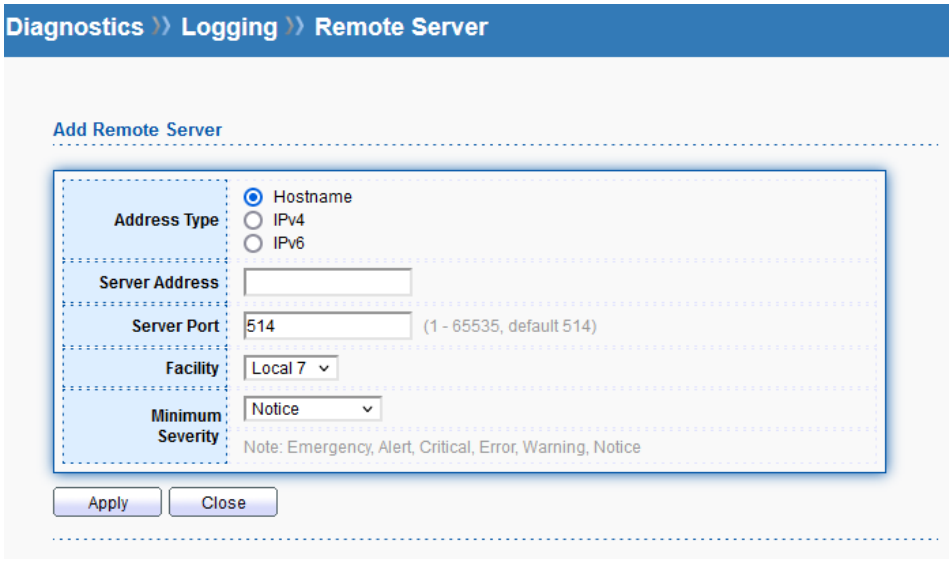
Minimum Severity	Select severity (Emergency, Alert, Critical, Error, Warning, Notice, informational and debug) of log messages which you wish to filter out for review.
Flash Logging	
State	Enable or disable to write log into Flash.
Minimum Severity	Select severity (Emergency, Alert, Critical, Error, Warning, Notice, informational and debug) of log messages which you wish to filter out for review.
Apply	Apply the settings to the switch.

17.1.2 Remote Server

This page allows to enable system logging into specific remote syslog server for storage.



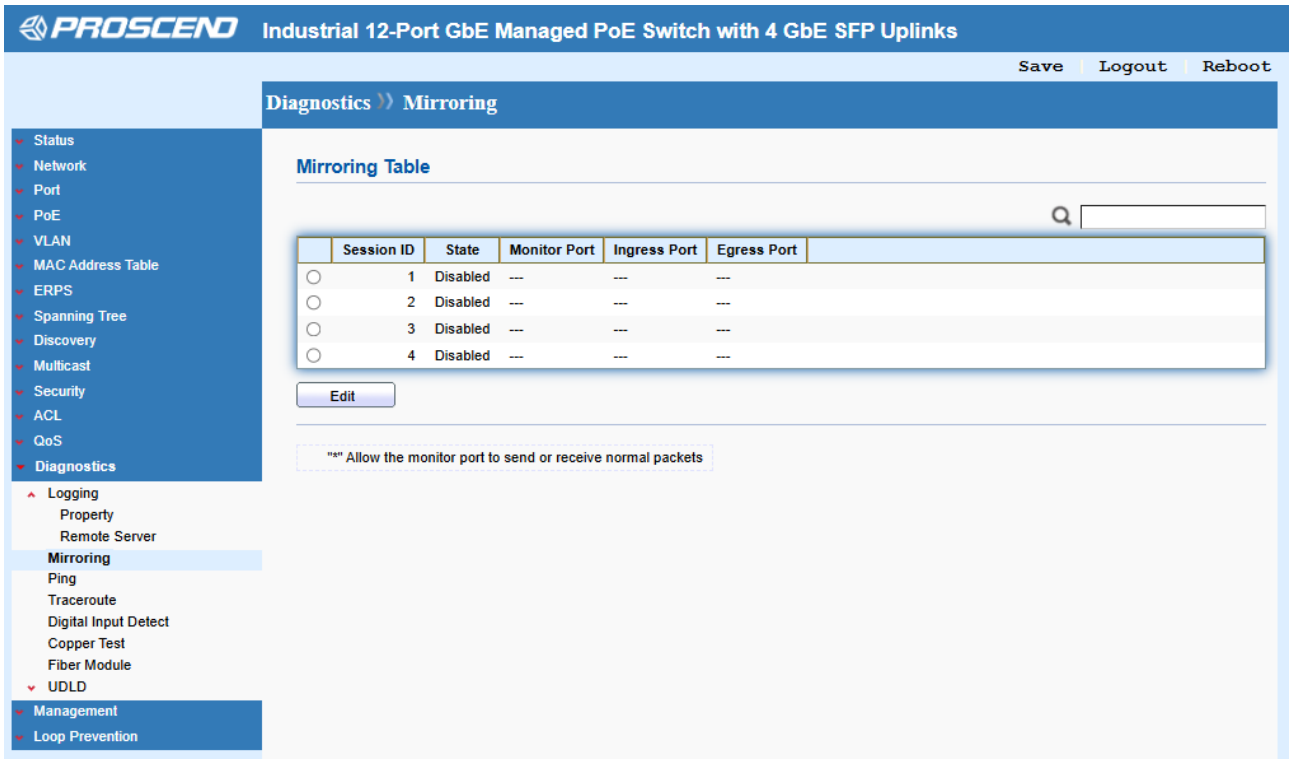
Item	Description
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the selected entry.



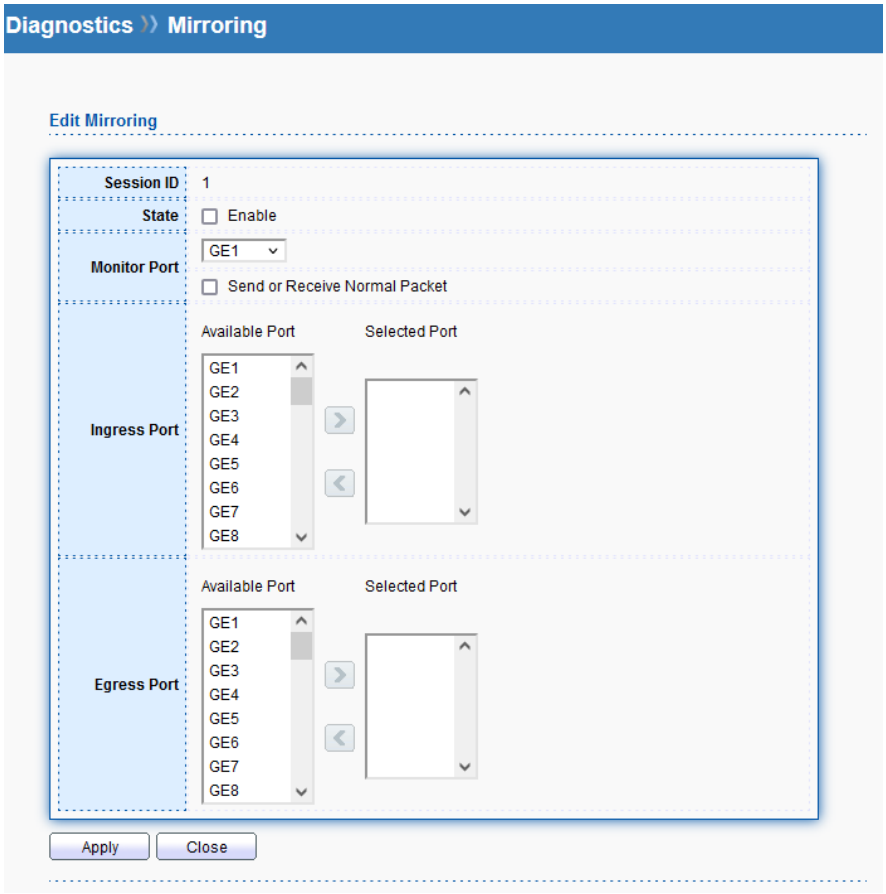
Item	Description
Address Type	Select the address type or remote server.
Server Address	Enter the Hostname/IPv4/IPv6 address of Syslog server.
Server Port	Specify the port that syslog should be sent to.
Facility	One device supports multiple facilities (represented with facility ID, local0 to local7) of remote Syslog server. For each facility ID contains different syslog server configuration, please choose a facility ID for such Syslog server.
Minimum Severity	Select severity (Emergency, Alert, Critical, Error, Warning, Notice, informational and debug) of log messages which you wish to filter out for review.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

17.2 Mirroring

This section provides ability to mirror packets coming in or going out on any port to a destination port. Through the packet duplication in the destination port, this feature is convenient for system administrator to monitor / understand the traffic operation. Session ID 1 to 4 can be enabled simultaneously and operate independently.



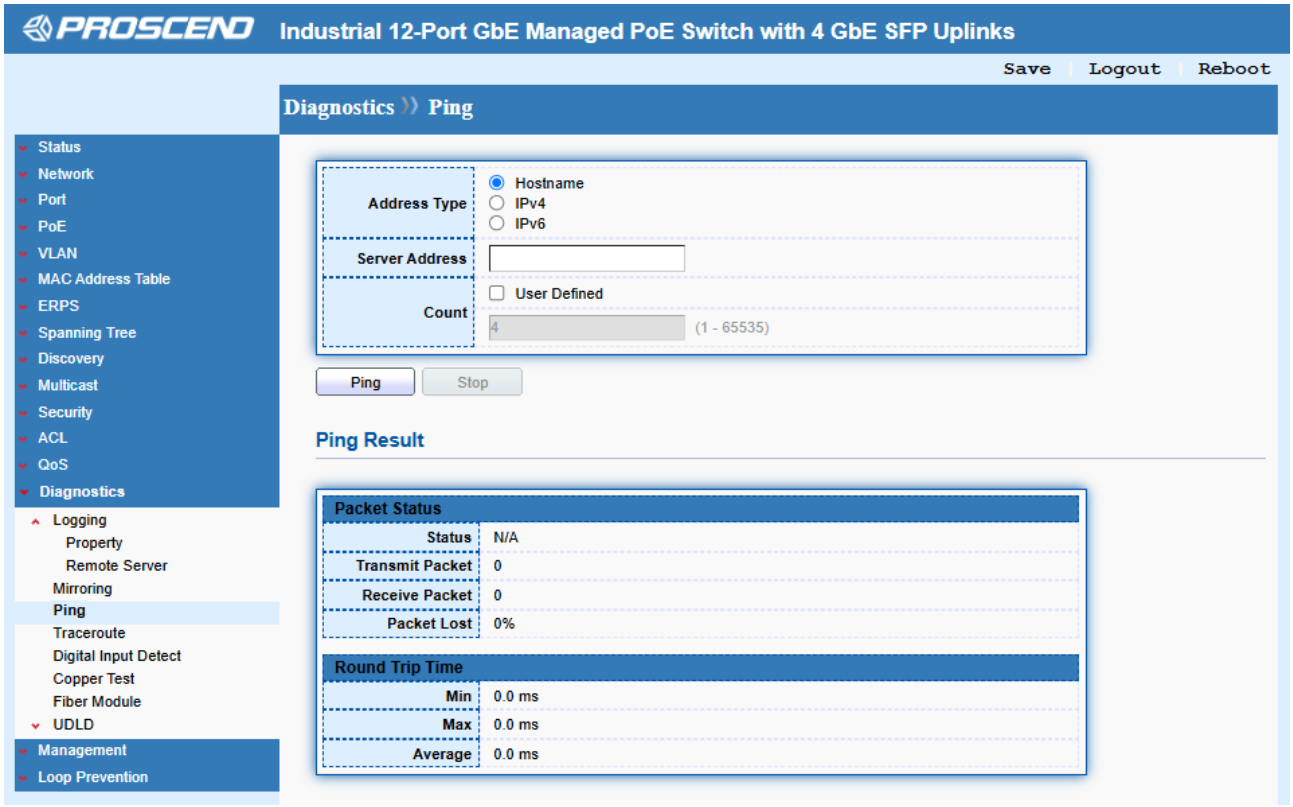
Item	Description
Edit	Edit the selected port(s).



Item	Description
Session ID	The index number of selected session ID.
State	Enable or disable the specified mirror session.
Monitor Port	Specify the port where you wish to observe the mirrored packets. **Enable**: The destination port is able to function as a port connecting to network, communicating with other network devices. **Disable**: Only observe the mirrored packets.
Ingress Port	Select the port(s) which you wish to mirror the traffic, ingress for mirror the packets into the port going out from the port.
Egress Port	Select the port(s) which you wish to mirror the traffic, egress for mirror the packets going out from the port.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

17.3 Ping

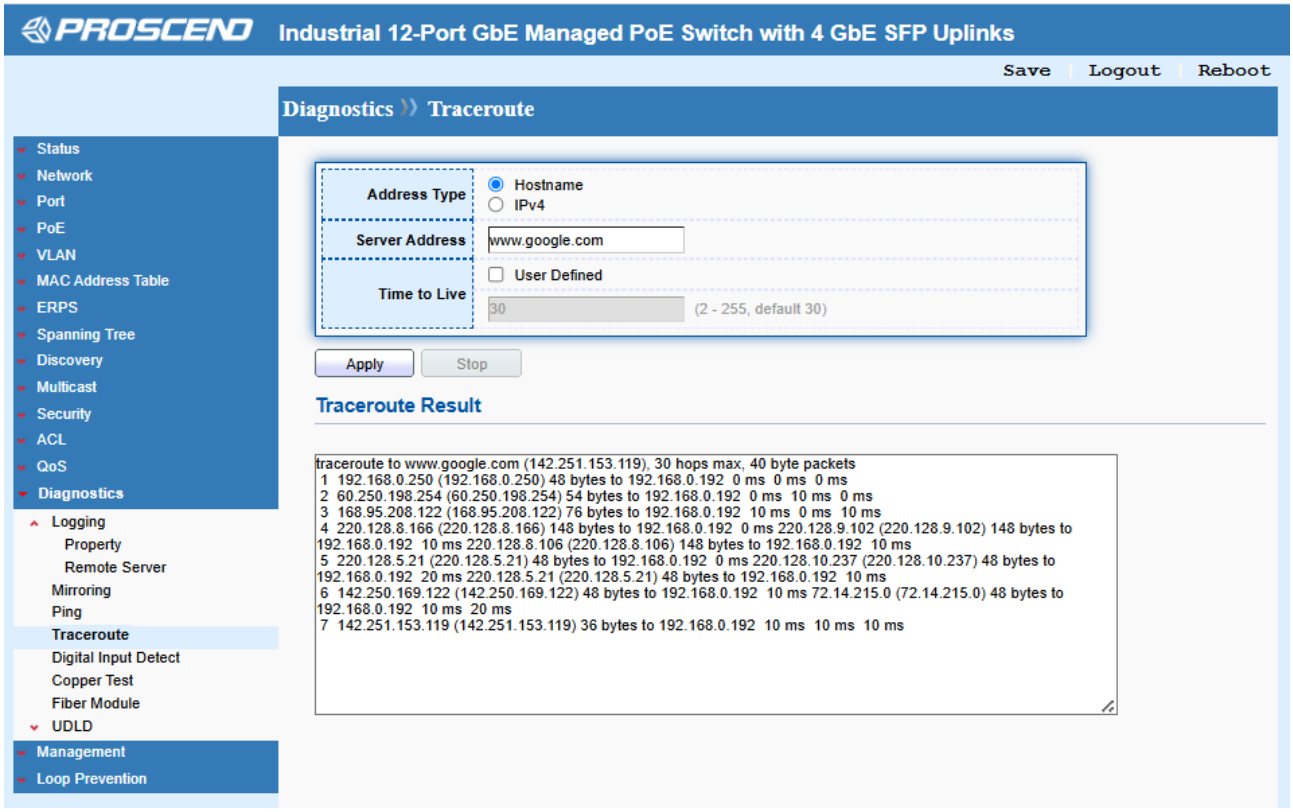
After finished the Ping test, the results will be shown on the lower side of this page.



Item	Description
Address Type	Select the address type or remote server.
Server Address	Enter the Hostname/IPv4/IPv6 address.
Count	It means how many times to send ping request packet. Enter a number between 1 and 65535 as the count and the default configuration is 4.
Ping	Start the Ping process.
Stop	Stop the Ping process.

17.4 Traceroute

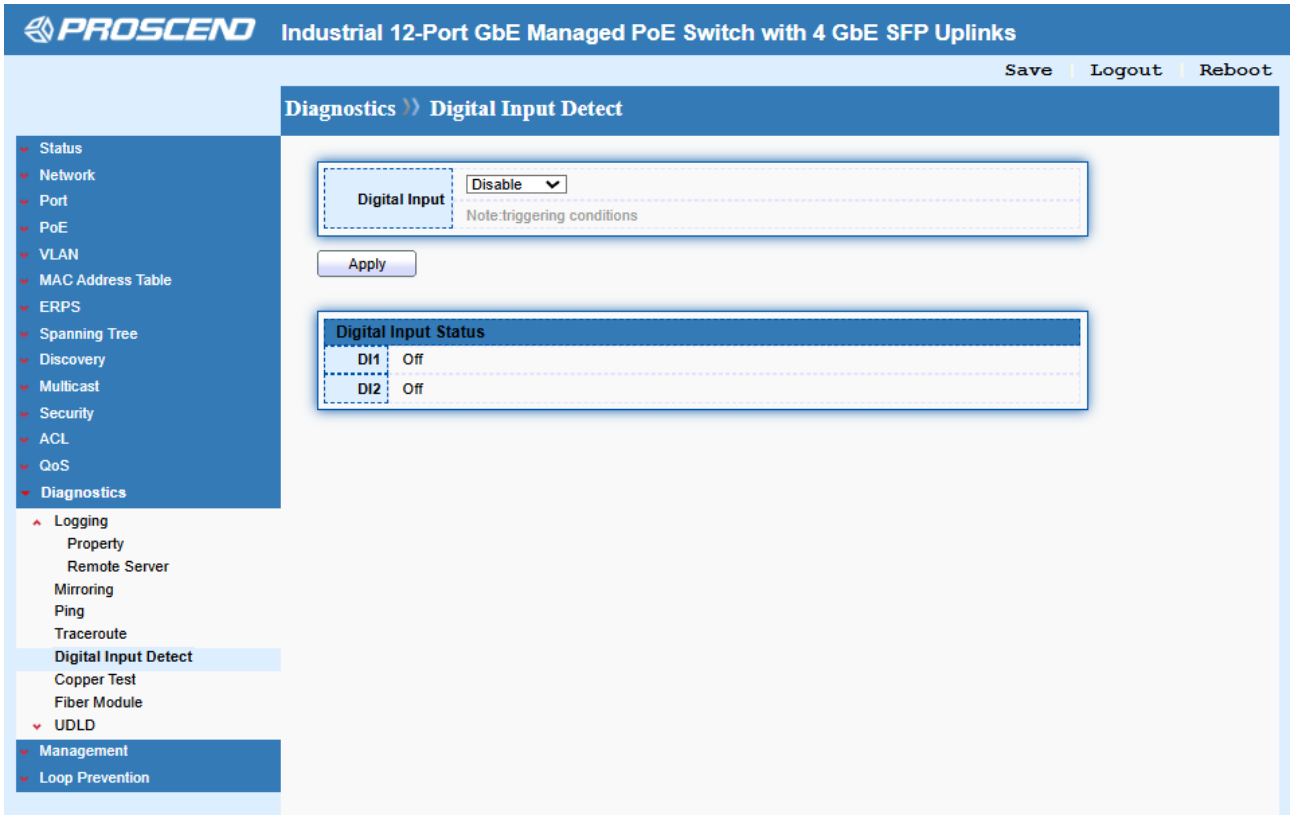
After finished the trace route test, the results will be shown on the lower side of this page.



Item	Description
Address Type	Select the address type or remote Hostname or IPv4.
Server Address	Enter the Hostname/IPv4 address.
Time to Live	Enter the value of “Time to Live” for trace route process. The default configuration is 30.
Apply	Start the trace route process.
Stop	Stop the trace route process.

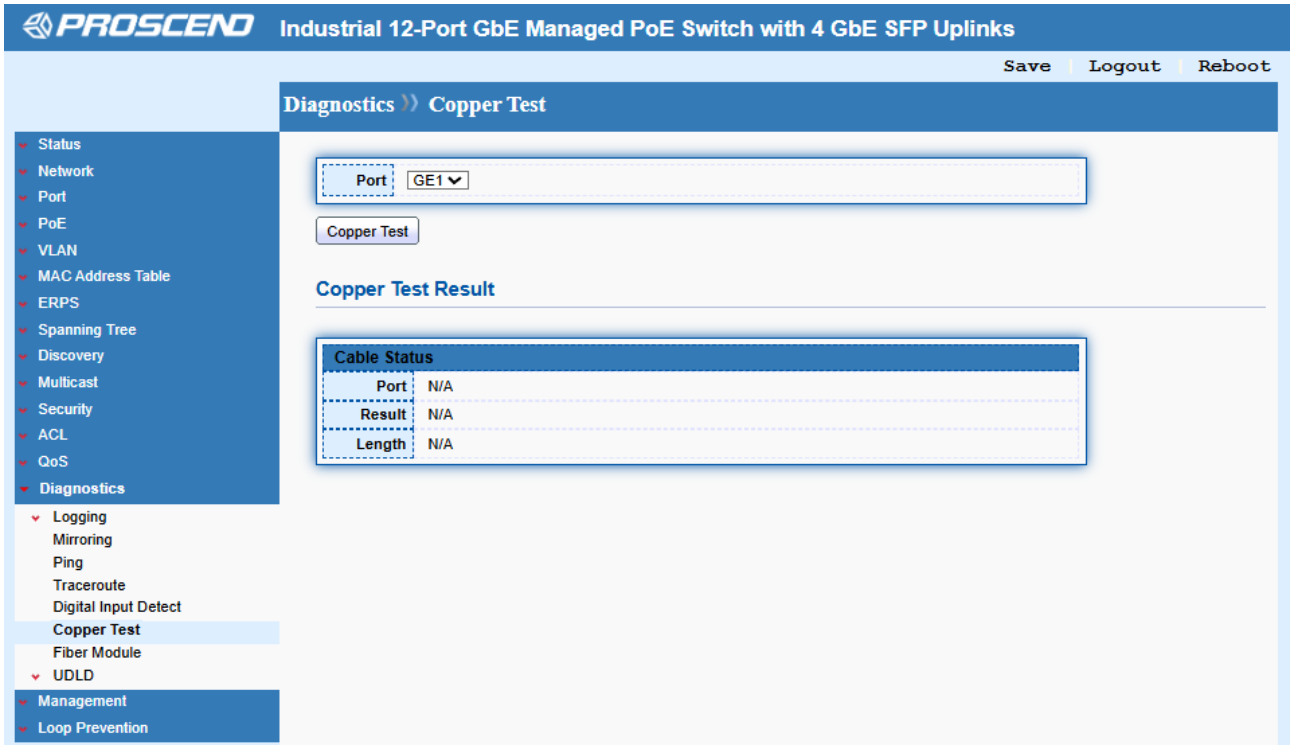
17.5 Digital Input Detect

This page allows to check the status of digital input.



17.6 Copper Test

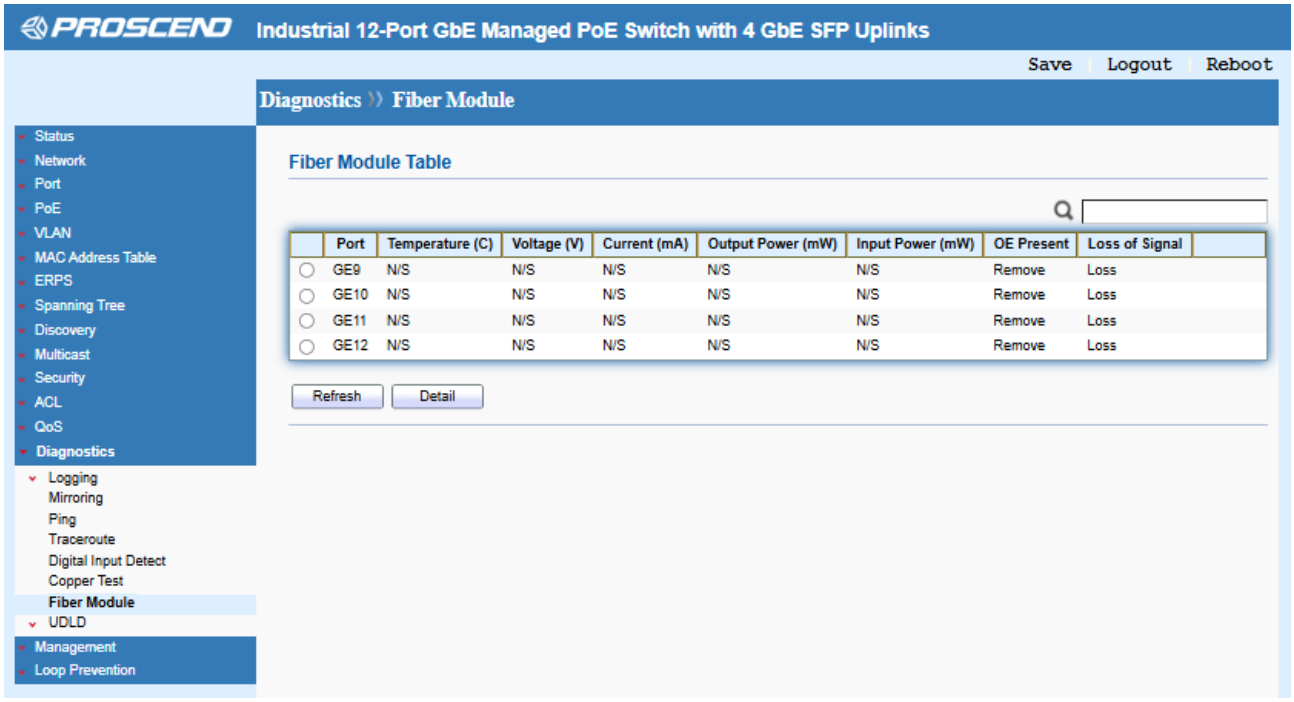
After finished copper test, the results will be shown on the lower side of this page.



Item	Description
Port	Select the port for testing copper.
Copper Test	Start copper test process.

17.7 Fiber Module

This page allows to check the detailed information of SFP module.

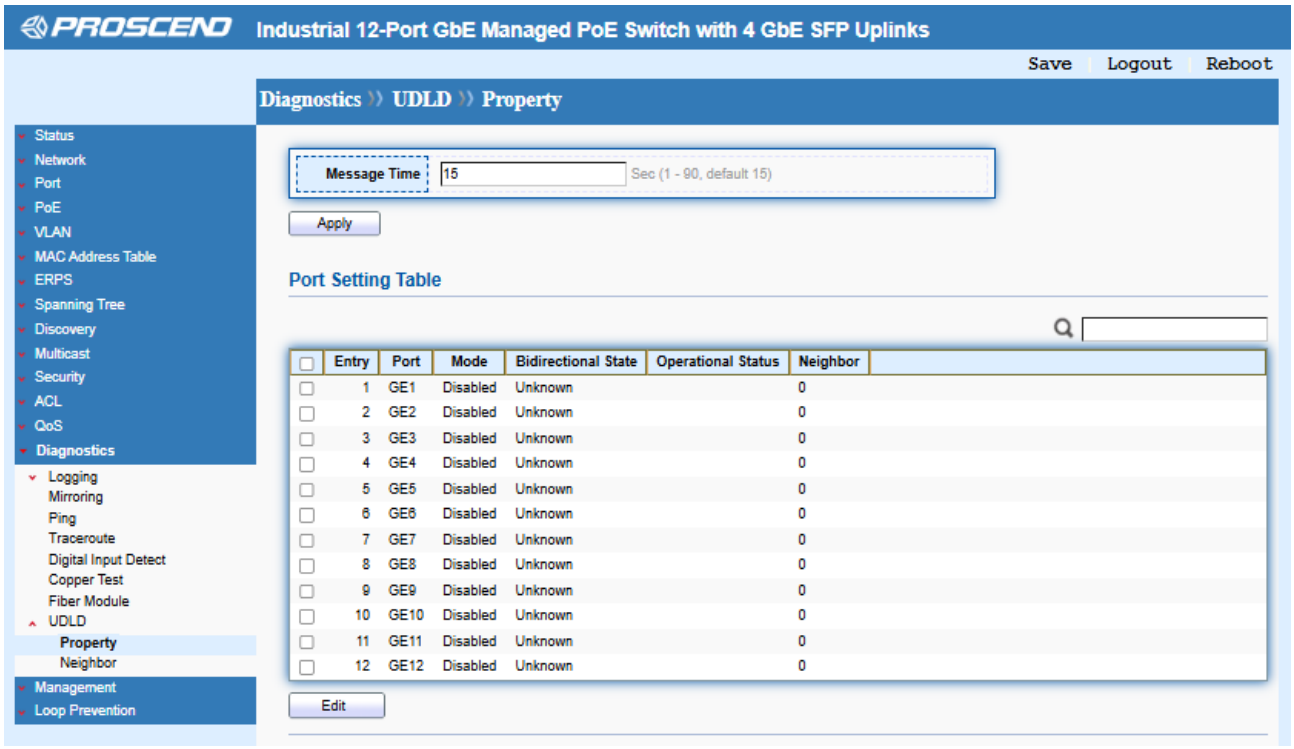


Item	Description
Refresh	Refresh the page to see new status of SFP.
Detail	Get details of SFP module.

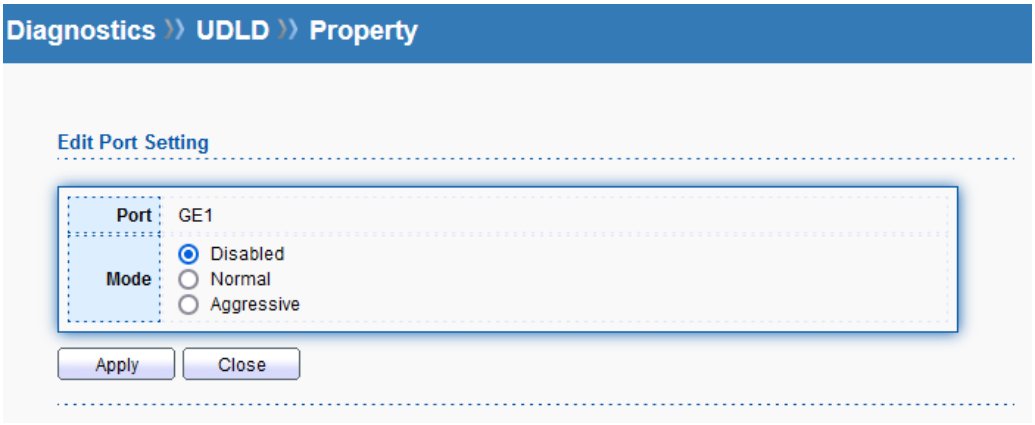
17.8 UDLD

Unidirectional Link Detection (UDLD) is a layer 2 protocol used to determine the physical status of a link. The purpose of Unidirectional Link Detection (UDLD) is to detect and deter issues that arise from Unidirectional Links. UDLD helps to prevent forwarding loops and blackholing of traffic by identifying and acting on logical one-way links that would otherwise go undetected.

17.8.1 Property



Item	Description
Message Time	Enter the message interval in aggressive mode, default is 15.
Apply	Apply the settings to the switch.
Edit	Edit the selected port.



Item	Description
Port	The index number of selected port.
Mode	**Disabled**: Disable the UDLD on selected port. **Normal**: Port state is marked as undetermined and behaves according to STP state. **Aggressive**: UDLD attempts to re-establish the state of the port and put into the error-disable state if unable to re-establish port state.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

17.8.2 Neighbor

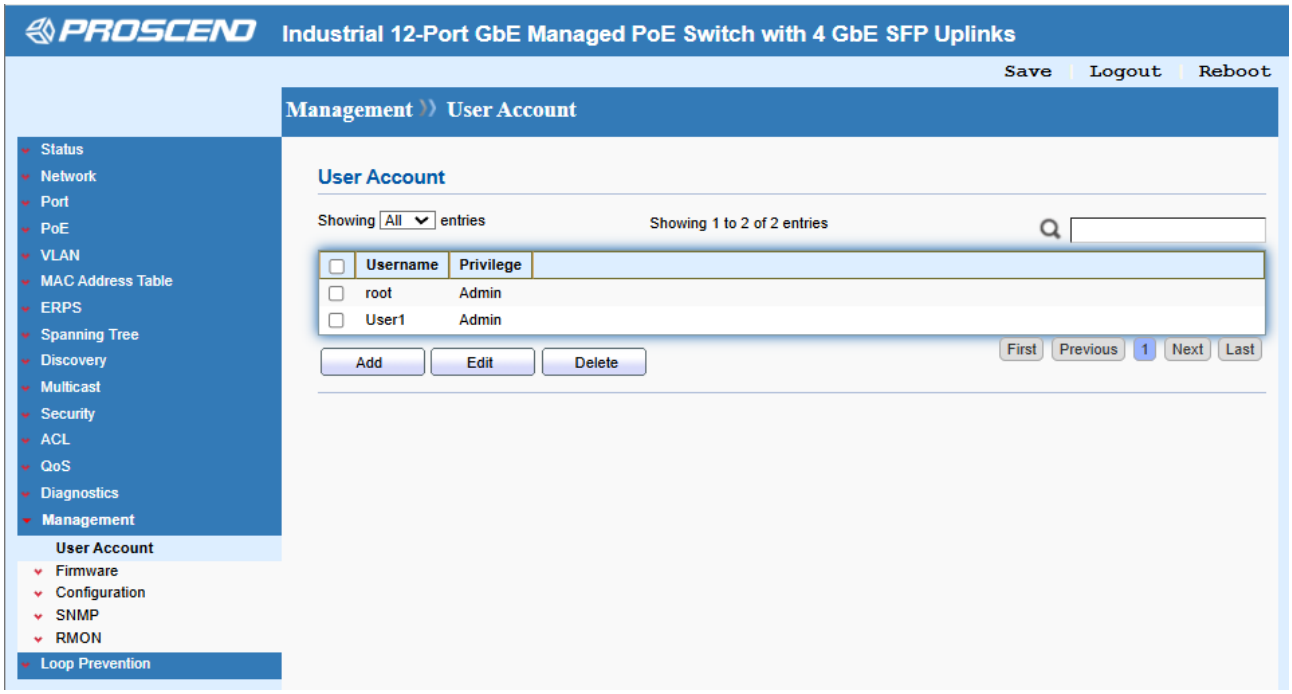
This page displays information of the neighboring devices.



18 Management

18.1 User Account

This page allows to Add/Edit/Delete the user account for device management.



18.2 Firmware

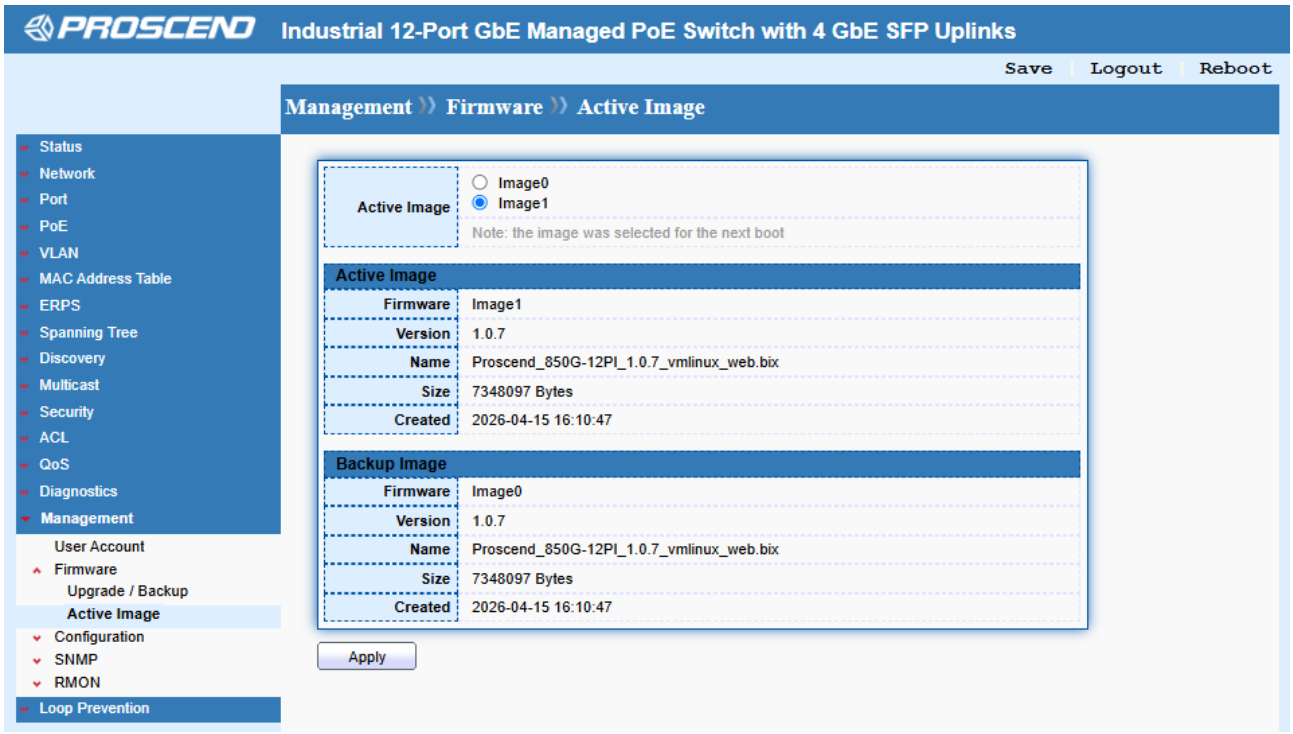
18.2.1 Upgrade / Backup

This page allows to upgrade the current image in the flash partition or backup the firmware from selected flash image partition 0 / 1.



18.2.2 Active Image

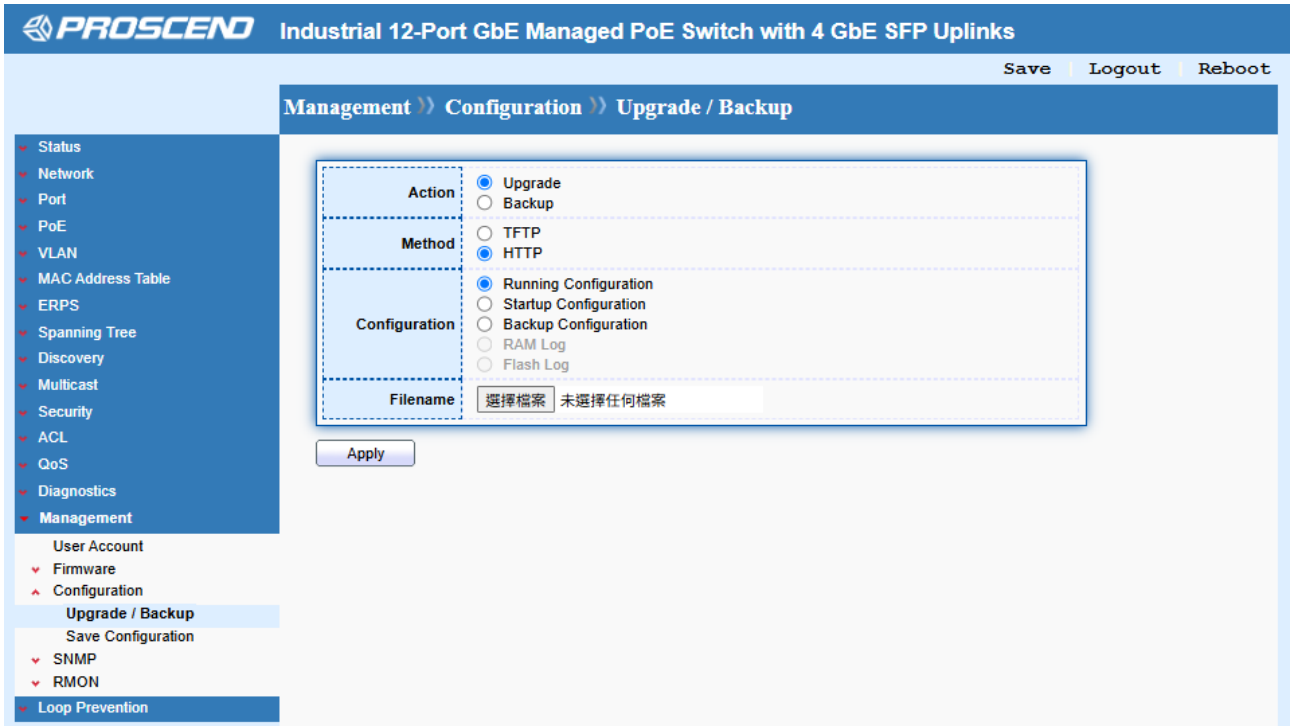
This page allows to boot the system from flash image partition 0 / 1.



18.3 Configuration

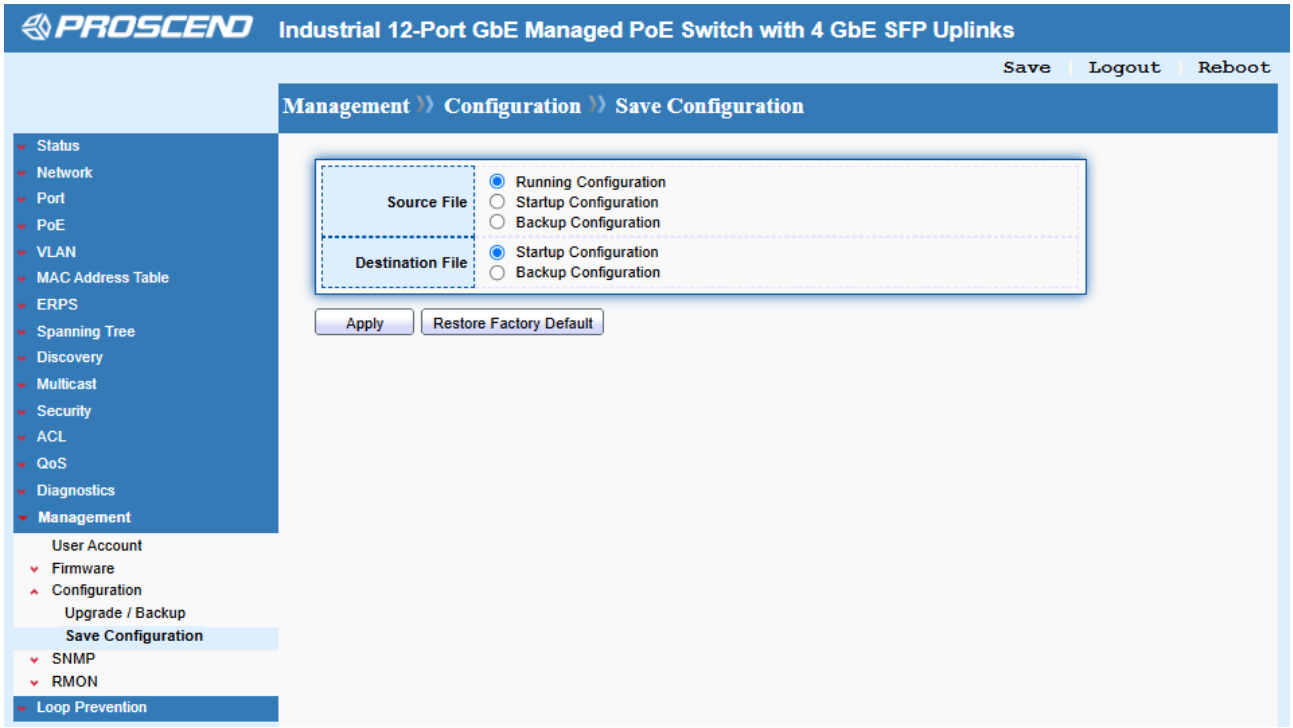
18.3.1 Upgrade / Backup

This page allows to upgrade the Running/Startup/Backup configuration or backup the Running/Startup/Backup configuration and RAM/Flash log via TFTP or HTTP.



18.3.2 Save Configuration

This page allows to save confirmation from different source to specified destination file or reset to factory default.

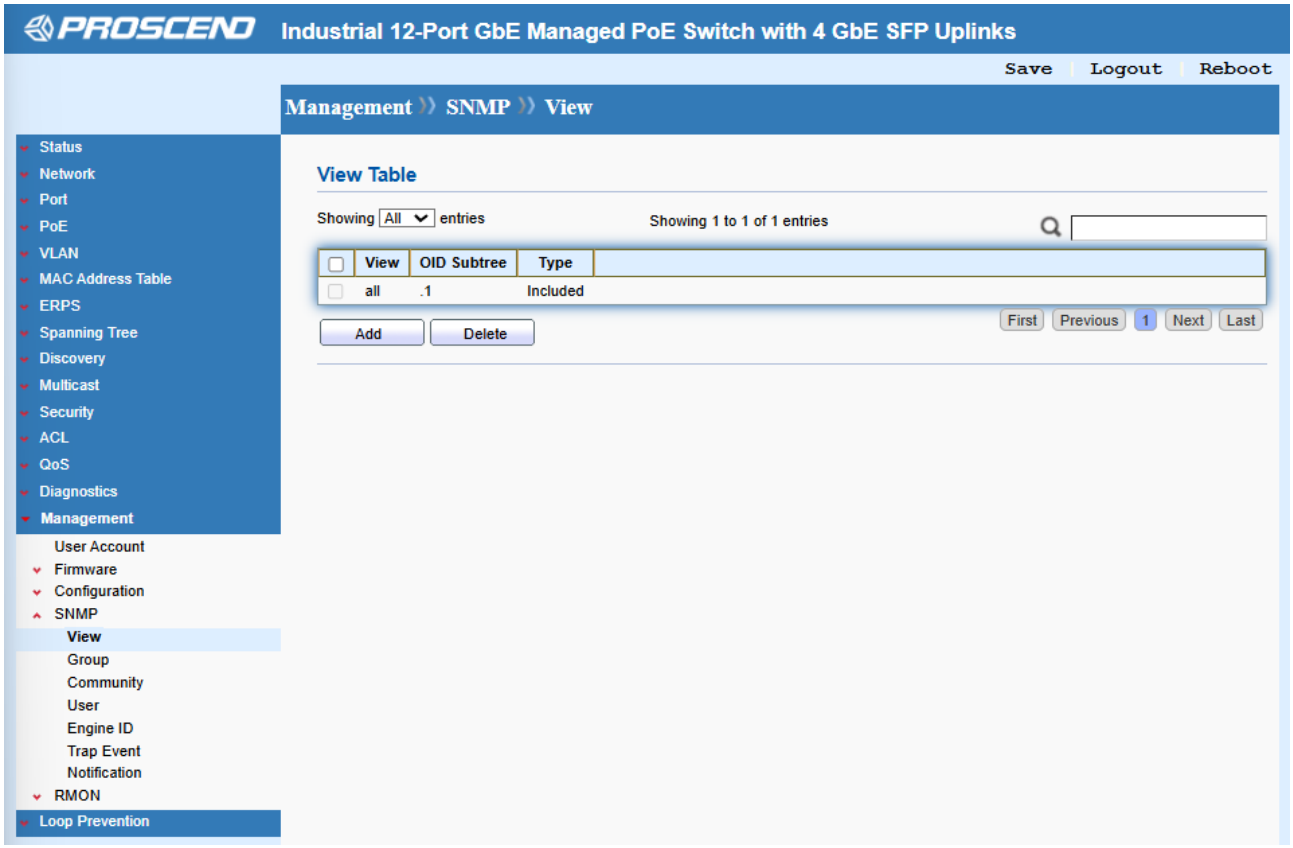


18.4 SNMP

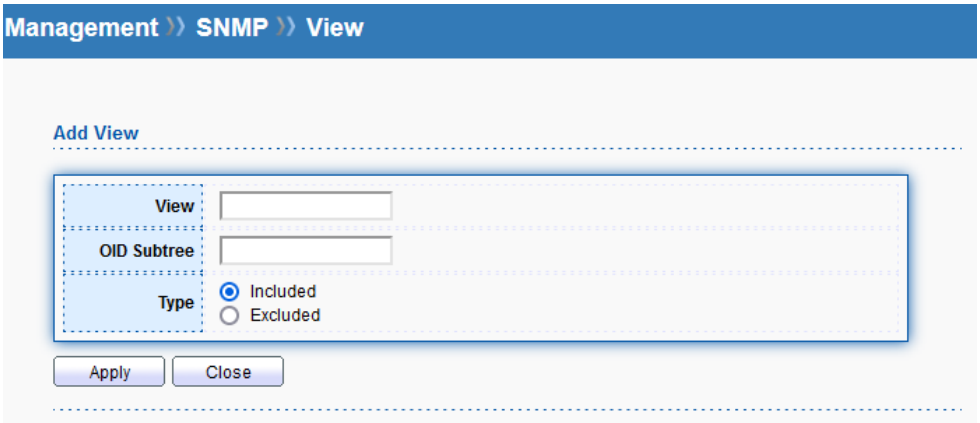
Simple Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks".

18.4.1 View

This page allows to create MIB views (Management information base) and then include or exclude OID (Object Identifier) in a view.



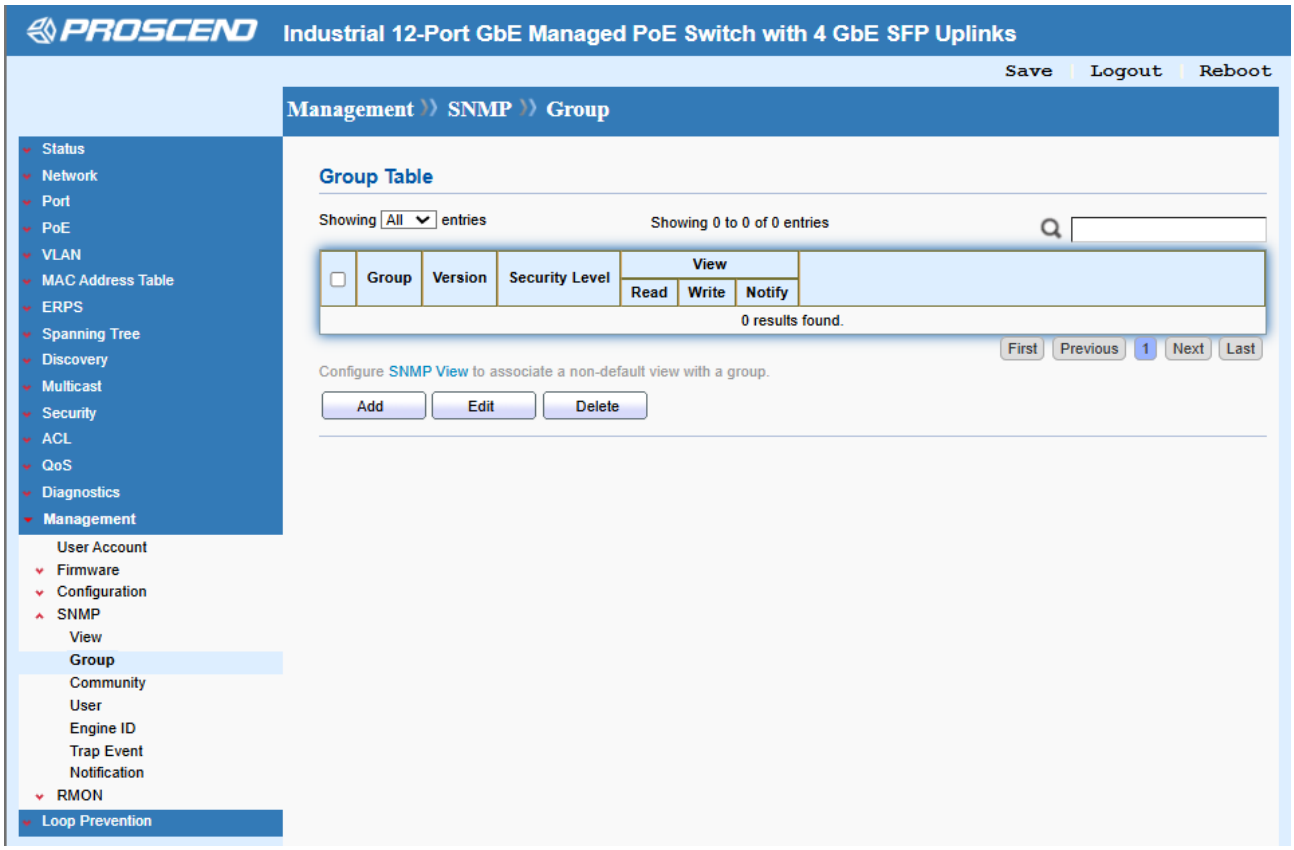
Item	Description
Add	Add a new OID string.
Delete	Delete the existing OID string.



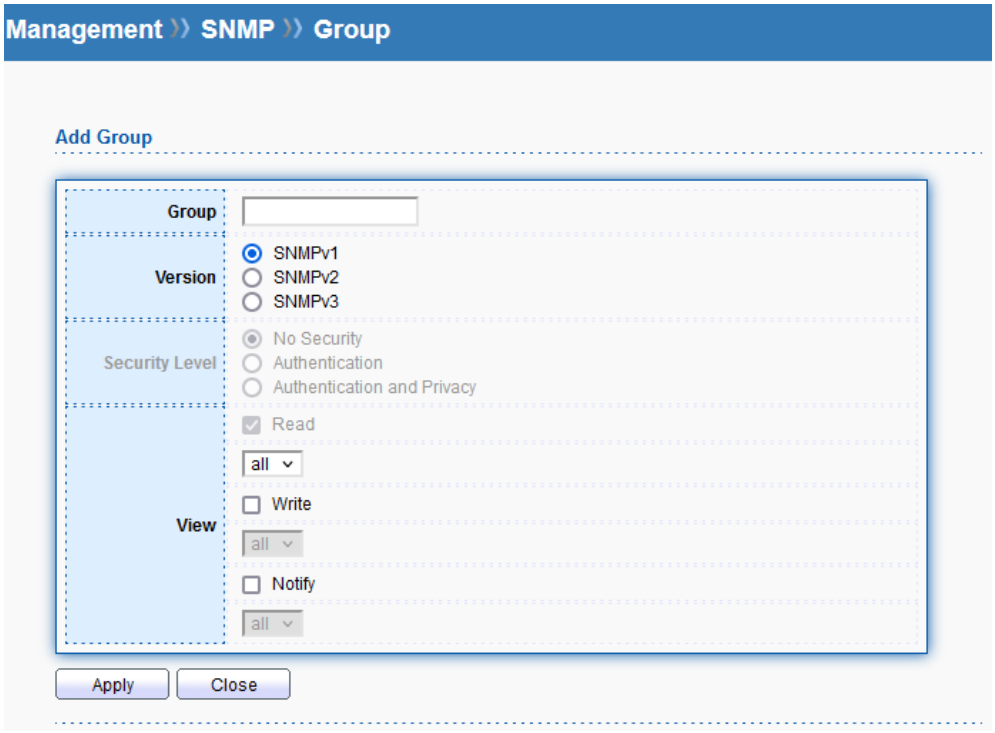
Item	Description
View	Enter a name of the MIB view.
OID Subtree	Enter an OID string to be included or excluded from the MIB view.
Type	Determine to include or exclude the selected MIBs.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

18.4.2 Group

This page allows to group SNMP users and assign different authorization and access privileges.



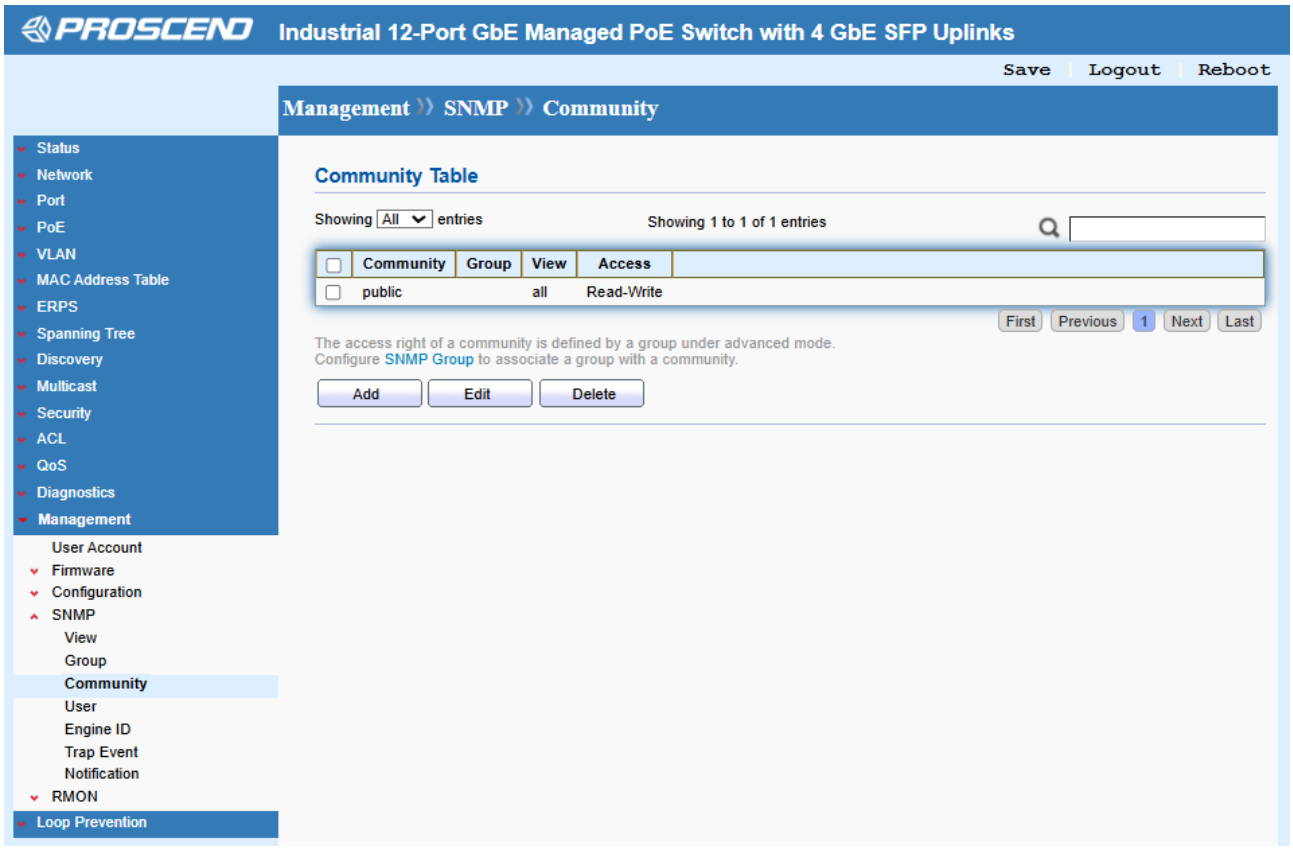
Item	Description
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the selected entry.



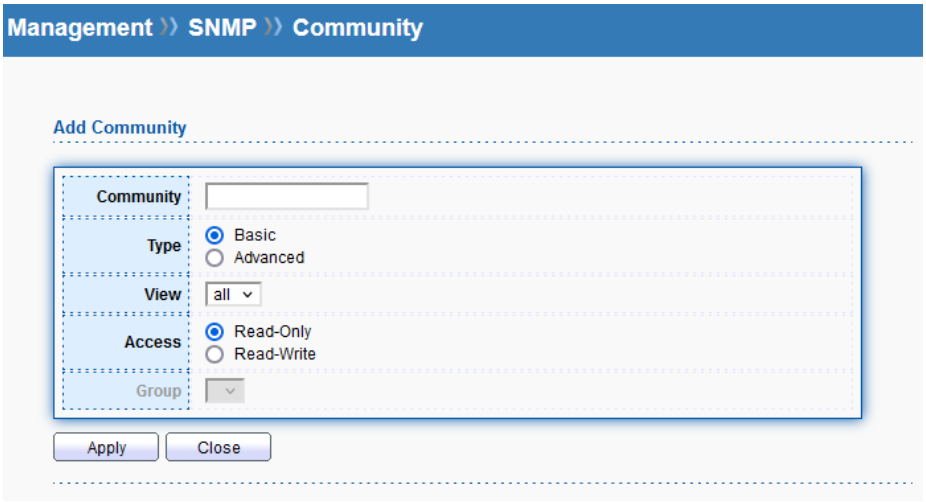
Item	Description
Group	Enter a name for the group.
Version	Specify SNMP version.
Security Level	Specify SNMP security level for the group. It is available when SNMPv3 is selected. **No Security**: No authentication and no encryption. **Authentication**: Requires authentication but no encryption. **Authentication and Privacy**: Requires authentication and encryption.
View	Users of this group have the right to Read/Write/Notify the selected MIB view.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

18.4.3 Community

This page allows to add/remove multiple communities of SNMP.



Item	Description
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the selected entry.

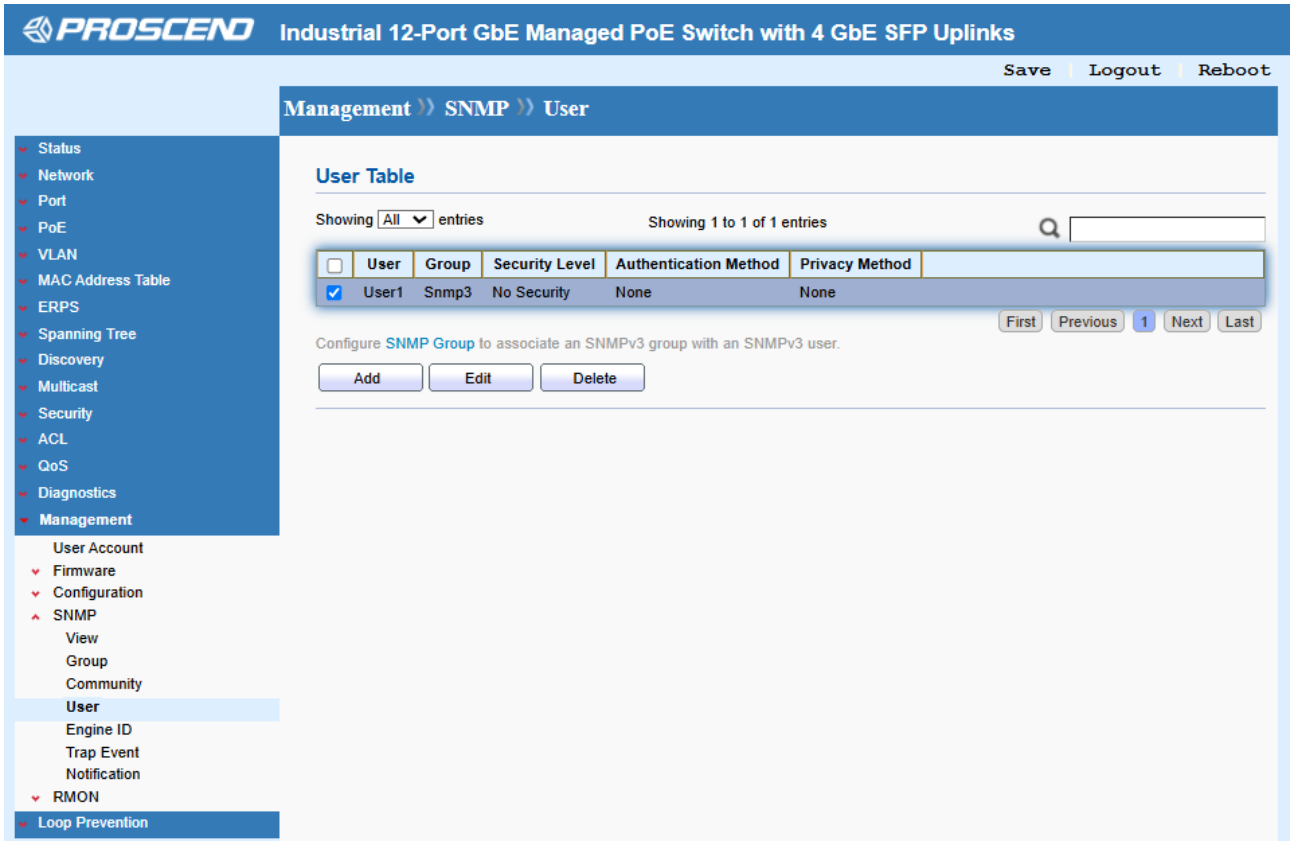


Item	Description
Community	Enter a name as community name.
Type	**Basic**: View and access right can be specified for such SNMP community profile. **Advanced**: Specify one of the SNMP groups for such SNMP community profile.
View	Simply specify one of the view profiles (created in SNMP➔View) from the drop down list.
Access	**Read Only**: It allows unidirectional access to node-specific information. **Read & Write**: It allows bidirectional access to node-specific information.
Group	Specify the SNMP group configured by user (SNMP➔Group) to define the object available to the community.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

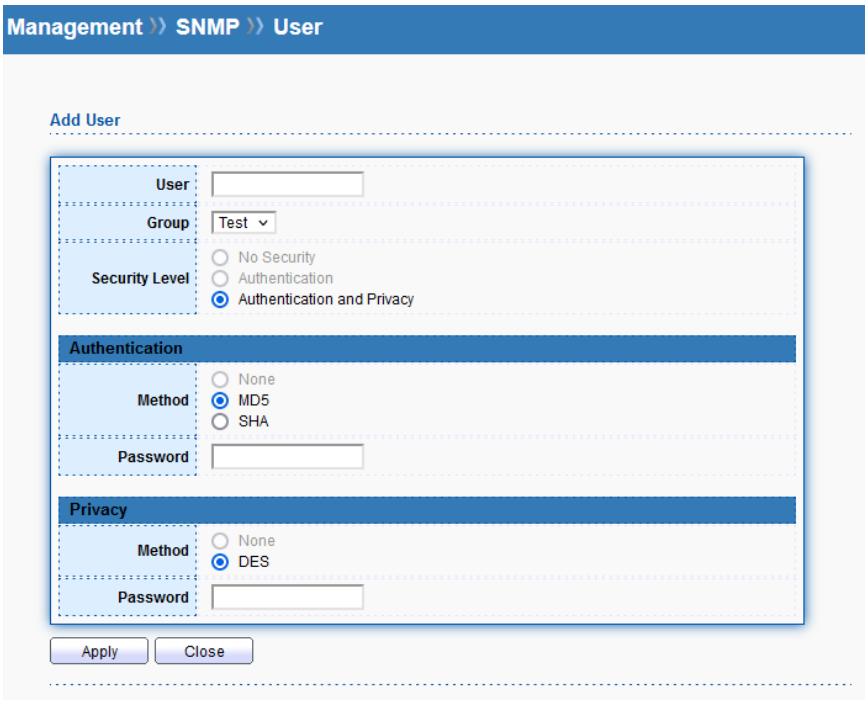
18.4.4 User

This page allows to configure SNMP user profile.

Note : Must create an SNMPv3 Group before it can be created.



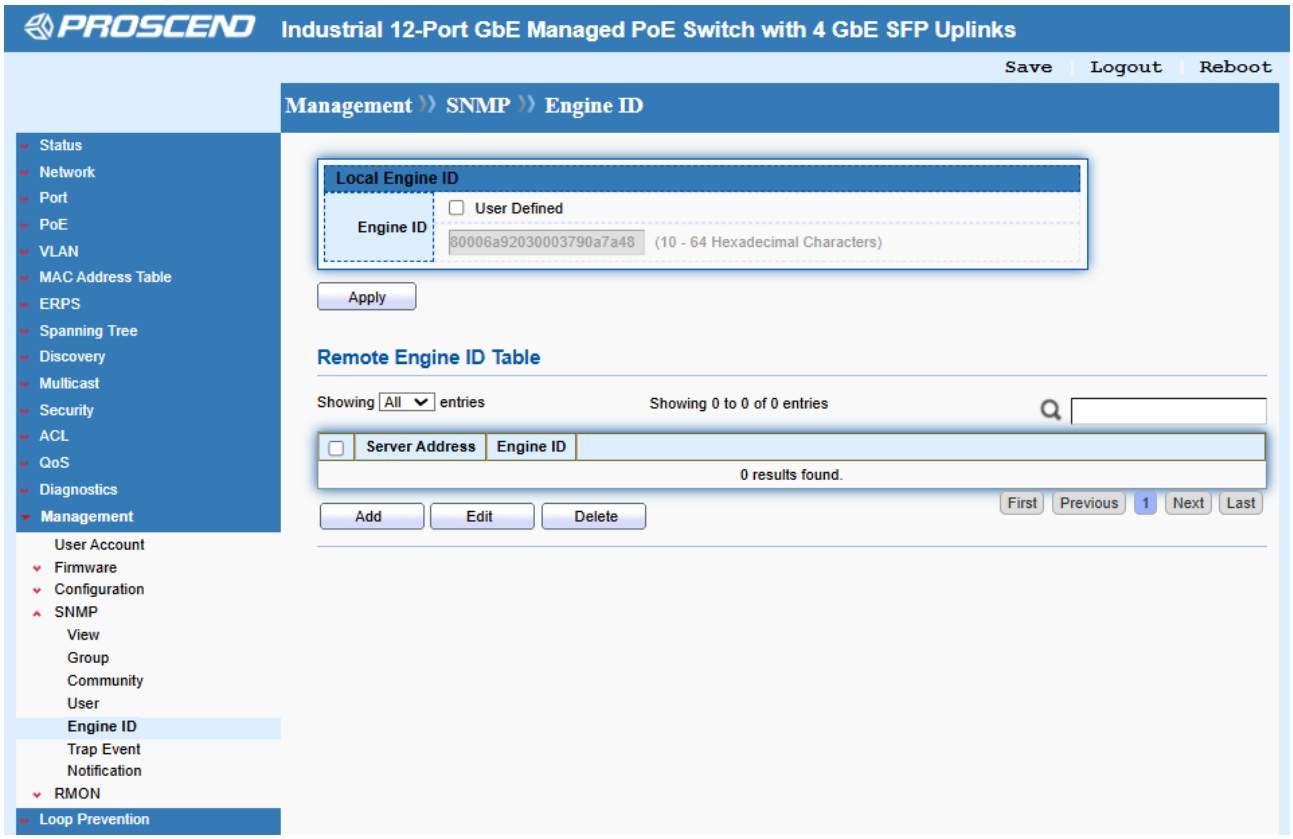
Item	Description
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the selected entry.



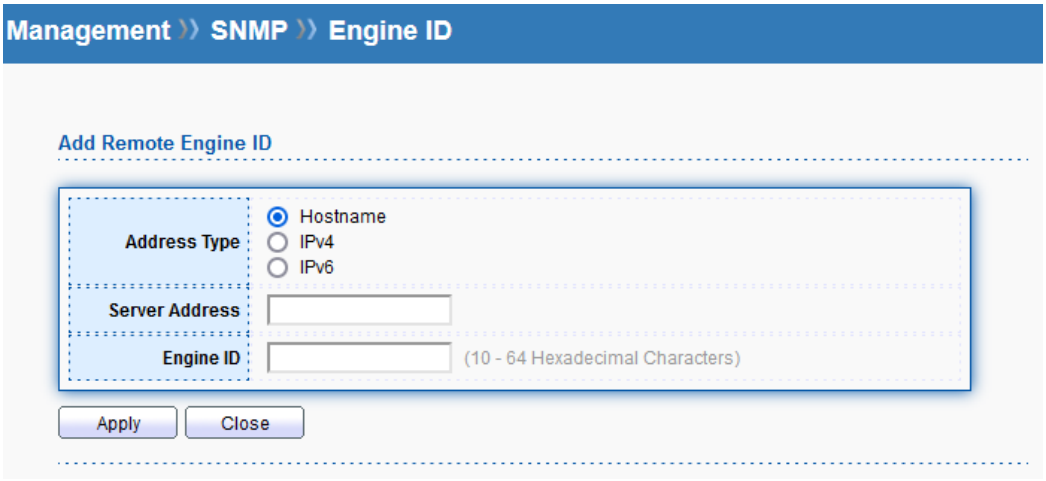
Item	Description
User	Enter a name for creating new SNMP user.
Group	Choose one of the SNMP group from the drop down list. Then, this user profile will be grouped under the selected SNMP group.
Security Level	Specify SNMP security level for the group. It is available when SNMPv3 is selected. **No Security**: No authentication and no encryption. **Authentication**: Requires authentication but no encryption. **Authentication and Privacy**: Requires authentication and encryption.
Authentication	
Method	At present, available methods include None, MD5 and SHA.
Password	Enter a password for the selected method. The password must contain more than 8 characters.
Privacy	
Method	At present, available methods include DES and None.
Password	Enter a password for the selected method. The password must contain more than 8 characters.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

18.4.5 Engine ID

This page allows to configure and display SNMP Local/Remote engine ID.



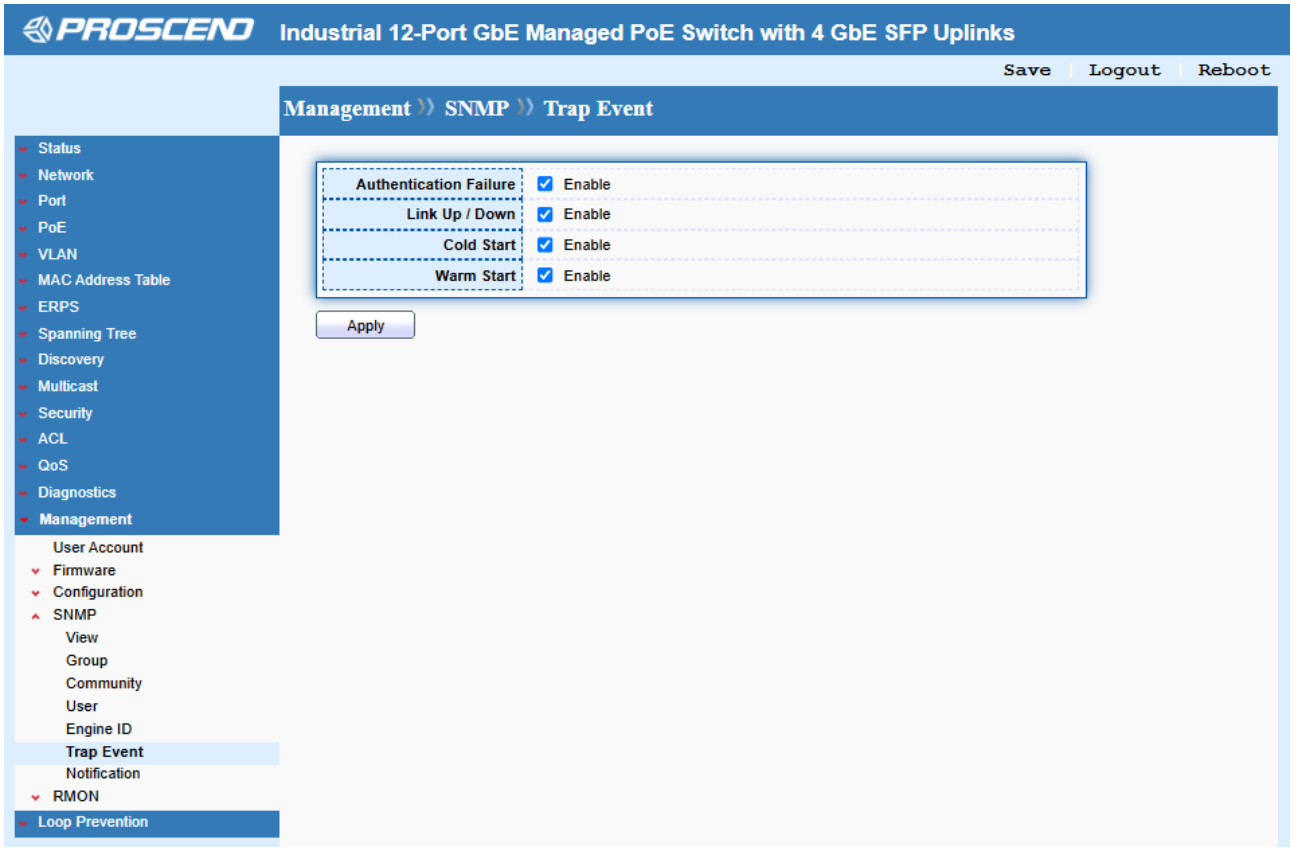
Item	Description
Engine ID	The user defined engine ID is range 10 to 64 hexadecimal characters, and the hexadecimal number must be divided by “2”. **User Defined**: If it is checked, the local engine ID will be configured manually. If not, the default Engine ID which is made up of MAC and Enterprise ID will be used instead.
Apply	Apply the settings to the switch.
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the selected entry.



Item	Description
Address Type	Specify the address type for entering hostname or IPv4/IPv6 address.
Server Address	Enter the IP address or the host name of the SNMP server.
Engine ID	Specify the engine ID for remote SNMP server. The engine ID is range10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

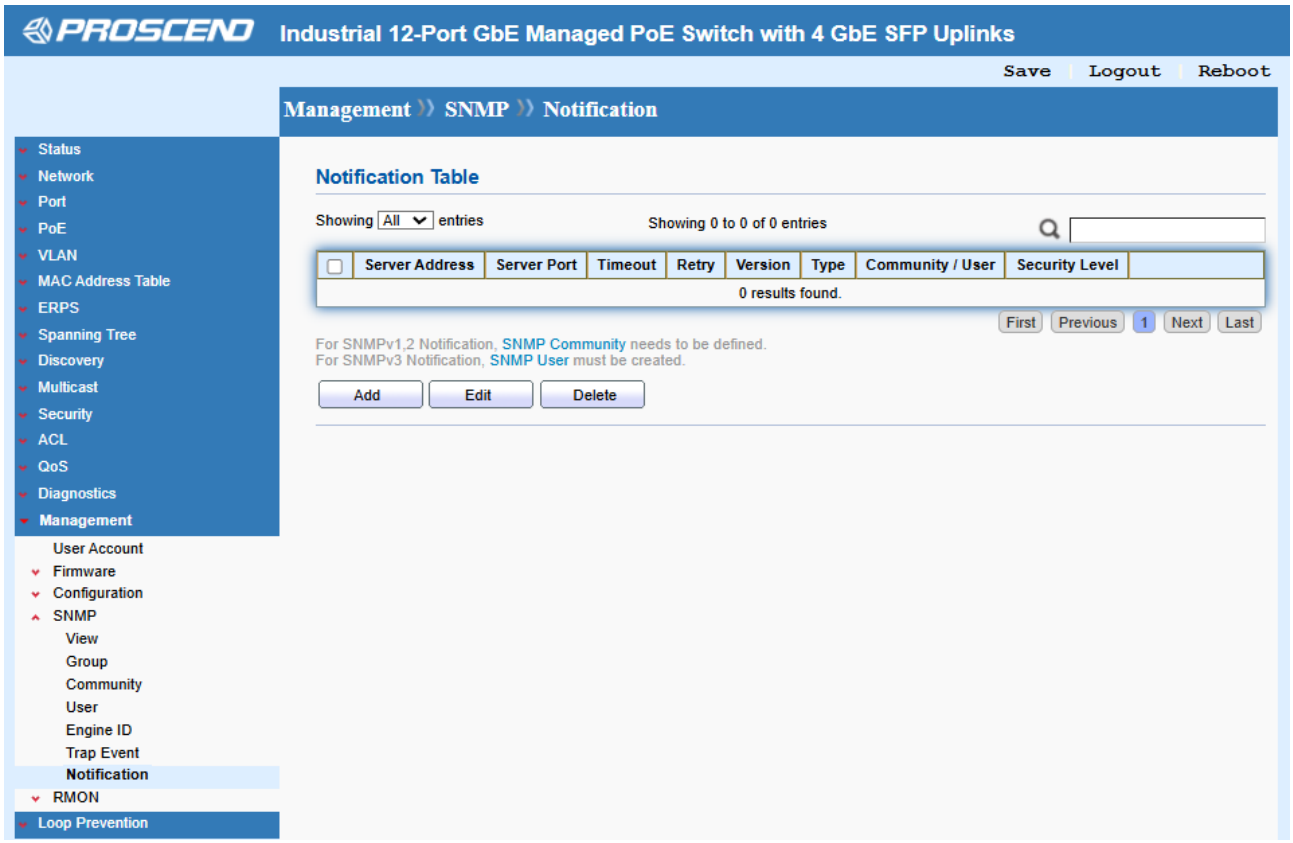
18.4.6 Trap Event

This page allows to add or delete SNMP trap receiver IP address and community name.

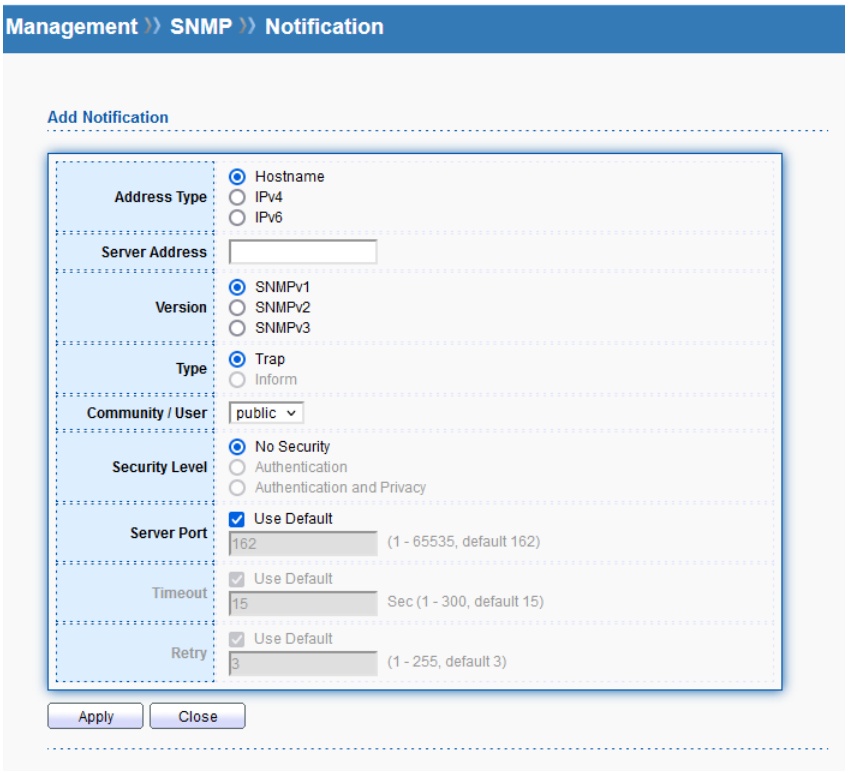


18.4.7 Notification

This page allows to configure a host to receive SNMPv1/v2/v3 notification.



Item	Description
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the selected entry.



Item	Description
Address Type	Specify the address type for entering hostname or IPv4/IPv6 address.
Server Address	Enter the IP address or the host name of the SNMP server.
Version	Specify SNMP version.
Type	Specify Notification Type. **Trap**: Send SNMP traps to the host. **Inform**: Send SNMP informs to the host. If it is used, Timeout and Retry also shall be defined.
Community/User	Use the drop down list to choose one of the community profiles.
Security Level	Specify SNMP security level for the group. It is available when SNMPv3 is selected. **No Security**: No authentication and no encryption. **Authentication**: Requires authentication but no encryption. **Authentication and Privacy**: Requires authentication and encryption.
Server Port	Specify the UDP port number for the recipient's server. **Use Default**: If it is checked, the default number (162) will be used automatically.

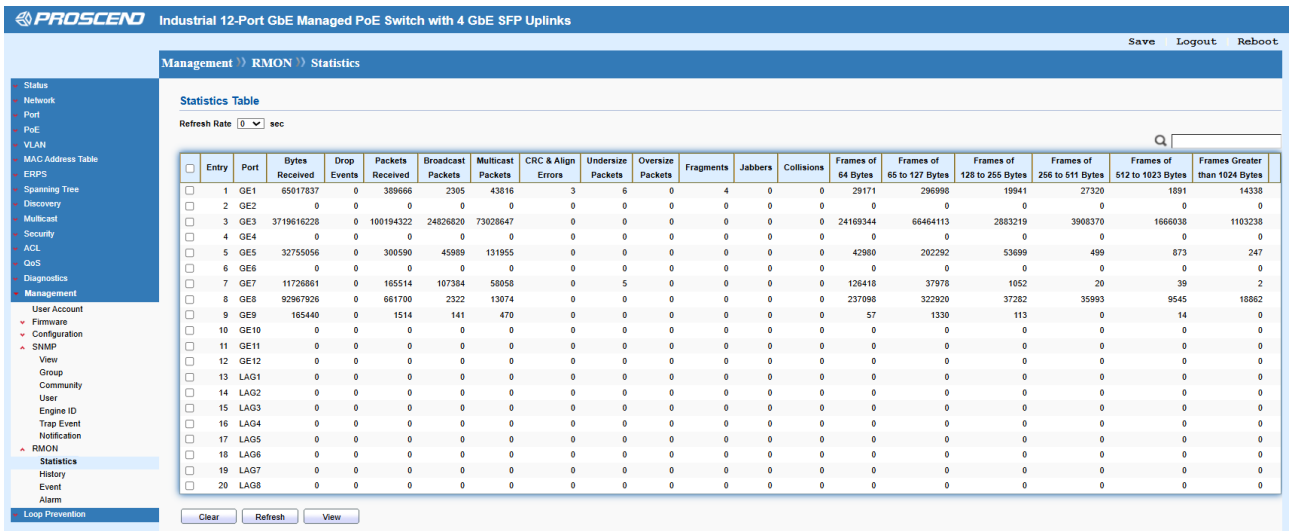
Timeout	Specify the SNMP informs timeout. It is available when Inform is selected as Type. **Use Default**: If it is checked, the default number (15) will be used automatically.
Retry	Specify the SNMP informs retry count. It is available when Inform is selected as Type. **Use Default**: If it is checked, the default number (3) will be used automatically.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

18.5 RMON

Remote Network Monitoring (RMON) was developed by the Internet Engineering Task Force (IETF) to support monitoring and protocol analysis of Local Area Networks (LANs).

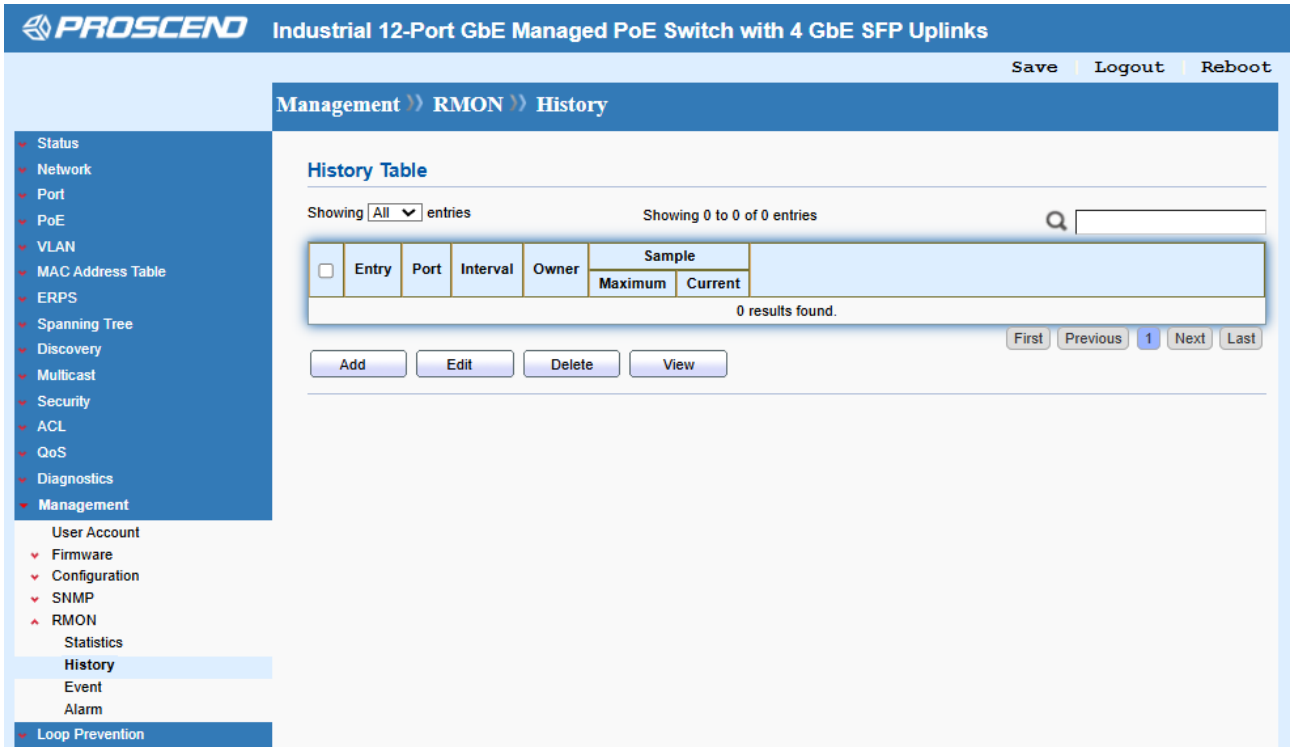
18.5.1 Statistics

This page shows the RMON statistics table.

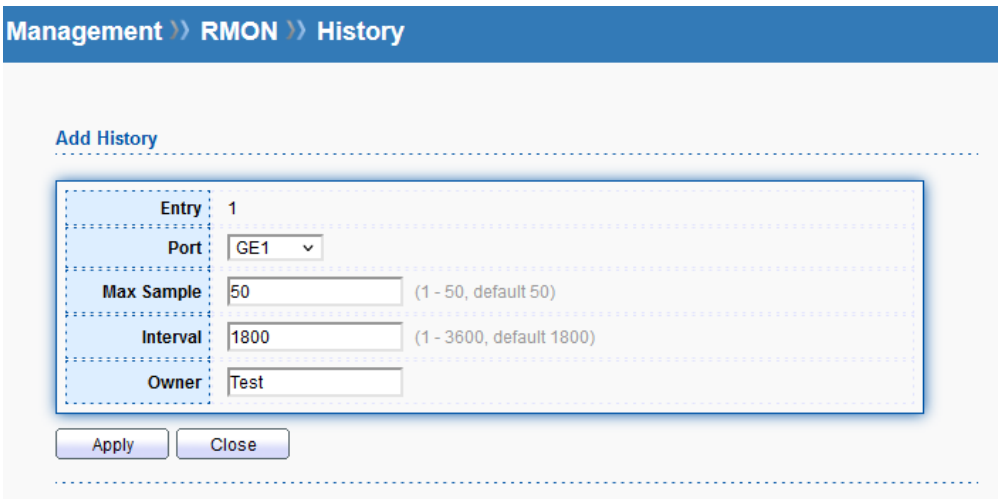


18.5.2 History

This page allows to configure RMON history table.



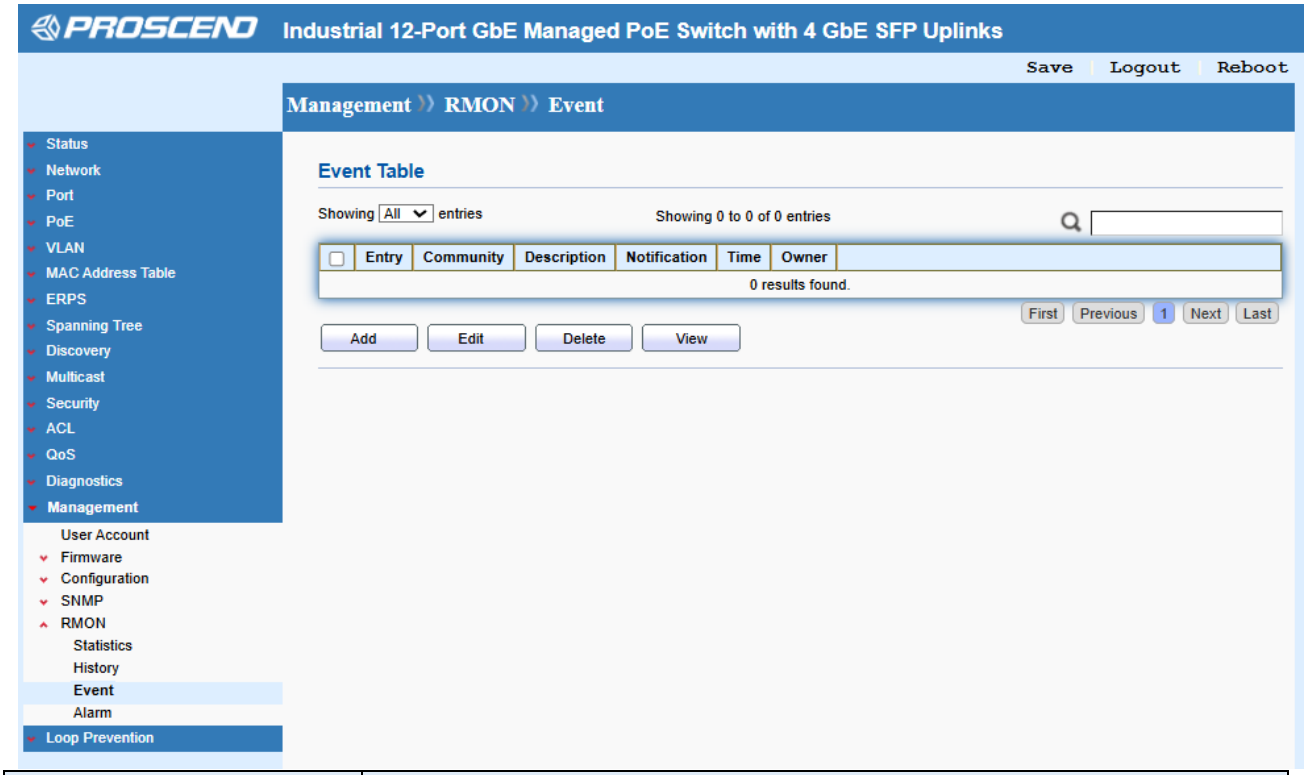
Item	Description
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the selected entry.
View	View the statistics of selected entry.



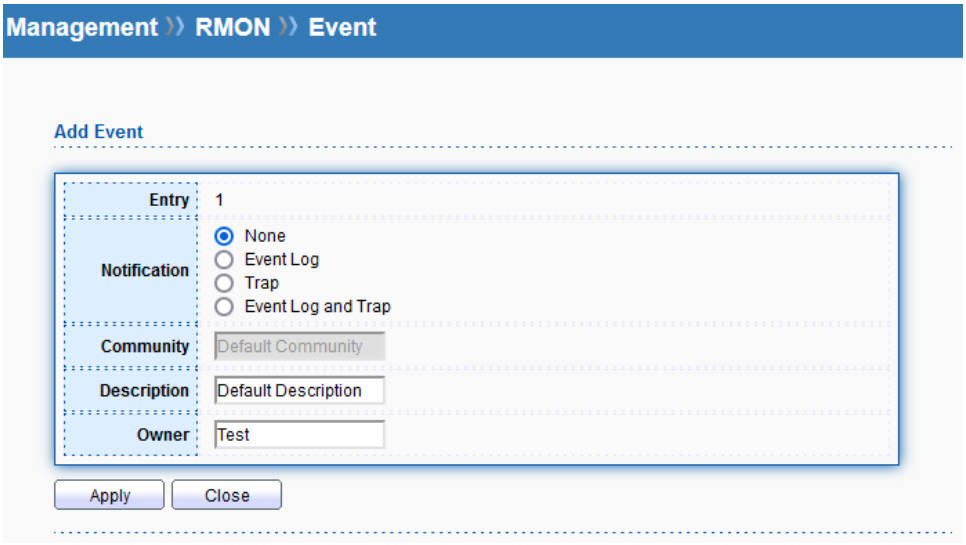
Item	Description
Entry	The index number of entry.
Port	Select the port which wants to be monitored.
Max Sample	Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 50, default value is 50.
Interval	Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.
Owner	Enter the name of owner.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

18.5.3 Event

This page allows to configure RMON Event table.



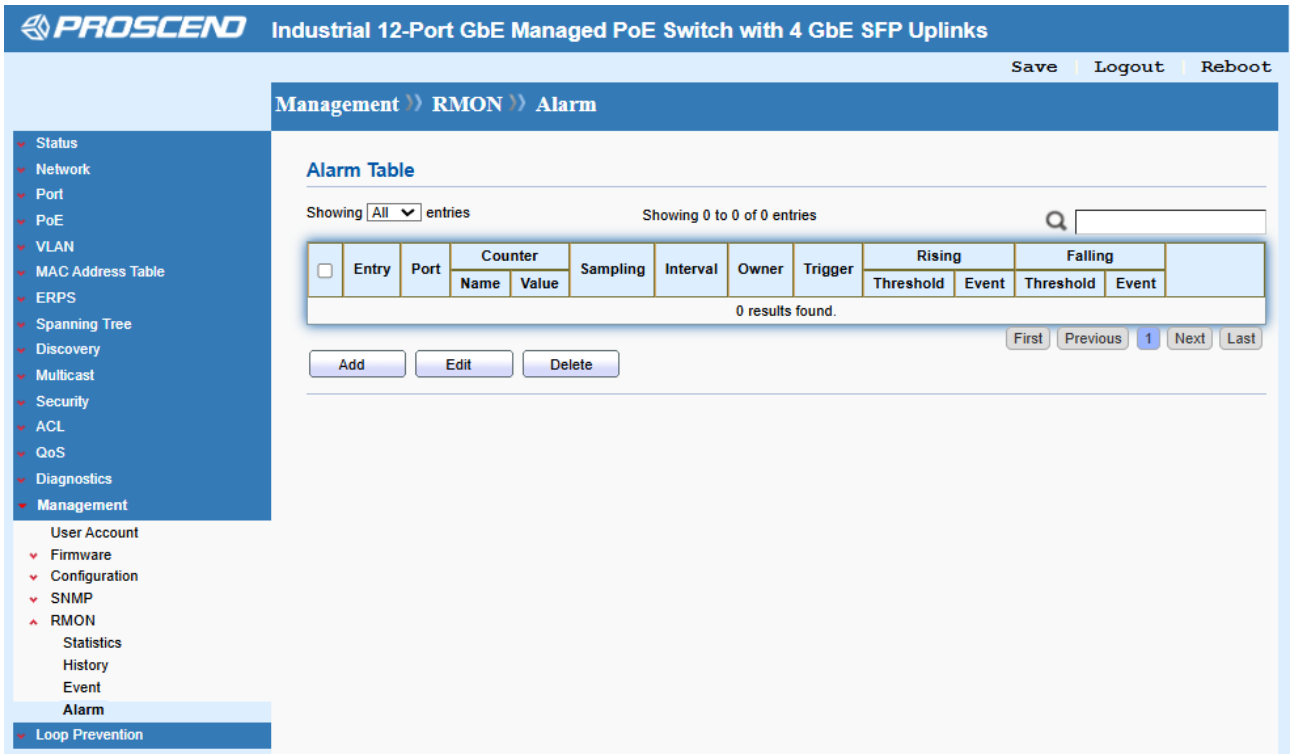
Item	Description
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the selected entry.
View	View the statistics of selected entry.



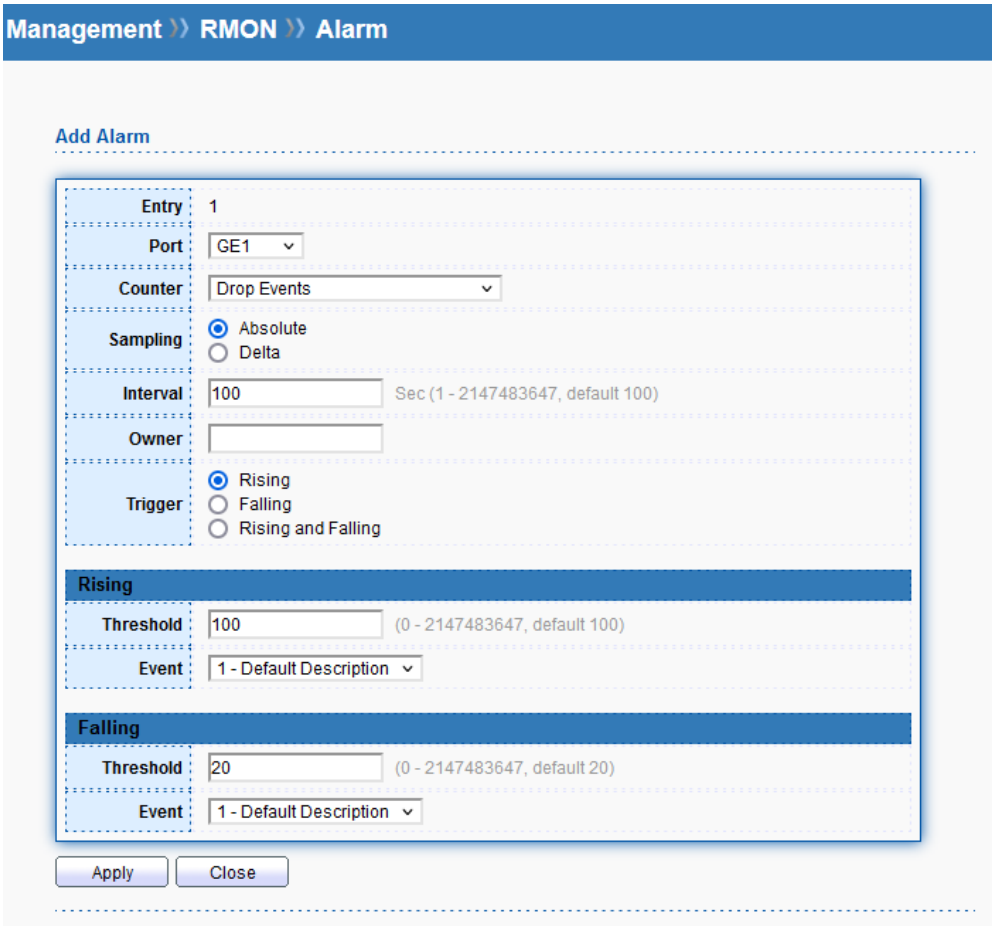
Item	Description
Entry	The index number of entry.
Notification	Indicates the notification of the event, the possible types are: **None**: No SNMP log is created; no SNMP trap is sent. **Event Log**: Create SNMP log entry when the event is triggered. **Trap**: Send SNMP trap when the event is triggered. **Event Log and Trap**: Create SNMP log entry and sent SNMP trap when the event is triggered.
Community	Specify the community when trap is sent.
Description	Indication of this event.
Owner	Enter the name of owner.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

18.5.4 Alarm

This page allows to configure RMON Event table.



Item	Description
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the selected entry.



Item	Description
Entry	The index number of entry.
Port	Select the port which wants to be monitored.
Counter	Indicates the particular variable to be sampled.
Sampling	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: **Absolute**: Get the sample directly. **Delta**: Calculate the difference between samples (default).
Interval	Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^{31}-1. Default is 100.

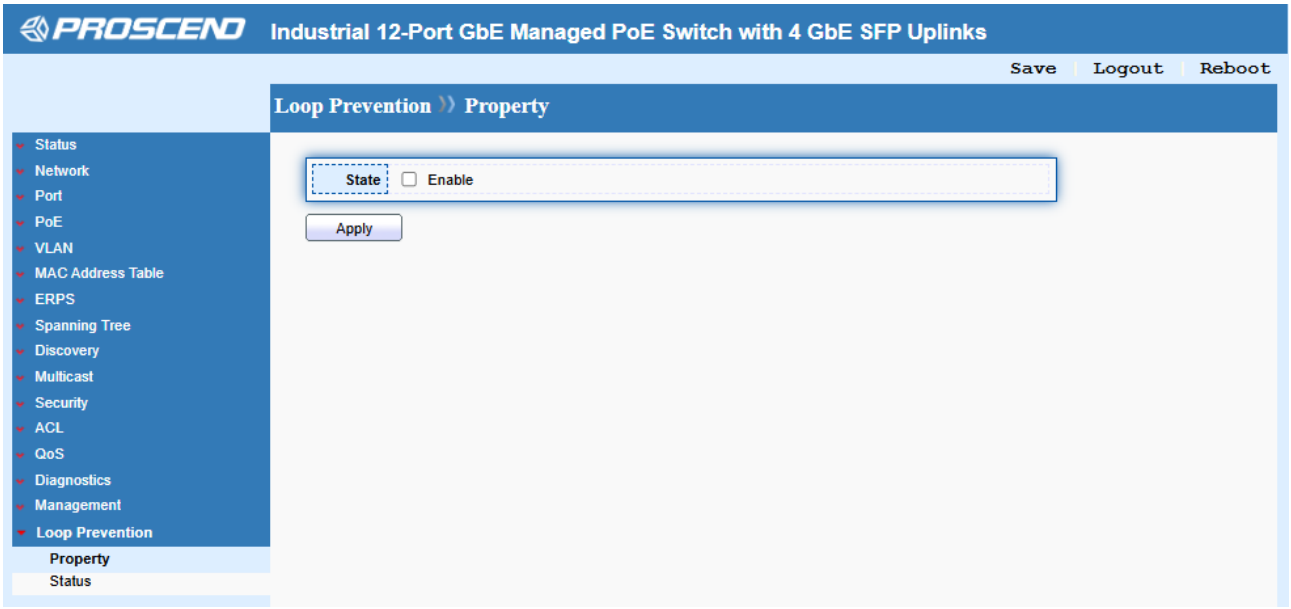
Owner	Enter the name of owner.
Trigger	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: **Rising**: Trigger alarm when the first value is larger than the rising threshold. **Falling**: Trigger alarm when the first value is less than the falling threshold. **Rising and Falling**: Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold.
Rising	
Threshold	Rising threshold value (0-2147483647).
Event	Rising event index.
Falling	
Threshold	Falling threshold value (0-2147483647)
Event	Falling event index.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

19 Loop Prevention

refers to mechanisms that prevent a system from entering an endless loop. The specific implementation depends on the application context.

19.1 Property

The Page enable or disable loop prevention.



19.2 Status

This page displays the Loop Prevention table.

