850X-28

Managed Switch

User Manual

V1.00

Table of Contents

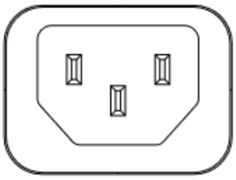
1 Introductions

1.1 System Description

Proscend 28-Port GbE Managed Switch 850X-28 enables full wire-speed with 40G SFP+ Uplinks and can handle extremely large amounts of data between network edge switches and servers at core network. The 850X-28 features Link Aggregation to accommodate all traffic for different kind of requirement of bandwidth, the Spanning Tree Protocol (STP/RSTP/MSTP) to maintain the quality of network and the QoS enablement for performance improvement of critical network traffic.

1.2 Hardware Installation

1.2.1 Connecting Power



The 850X-28 can automatically adjust the AC power setting to adapt to any voltage supply in the range 100~240 VAC 50/60Hz. Connect the one end of the supplied AC power cord to the AC power connector on the rear panel and the other end into a properly grounded power outlet.

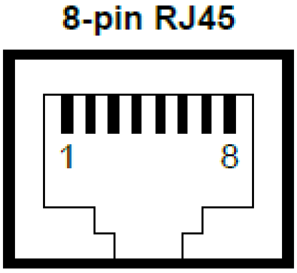
1.2.2 LED Indicators

LED	Color	Description
PWR	On: Green	Power on.
	Off	Power off.
SYS	On: Green	System is ready.
	Blinking	System is booting up.
	Off	No power or system boot up failed.
ALM	On: Red	Alarm for system failure because of overheat or wrong voltage.
	Off	Switch is in operation with normal condition.
1~24 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.

25~28 SFP+ Port Link/Act	On: Blue	LINK UP at 10Gbps.
	On: Green	LINK UP at 1000Mbps.
	Blinking	Traffic detected.
	Off	LINK DOWN.

1.2.3 RJ45 Connector Pinouts

The pin assignment of RJ45 connector is shown in the following table.



Pin	Description	PoE Pinouts
1, 2	T/Rx+, T/Rx-	V+
3, 6	T/Rx+, T/Rx-	V-
4, 5	T/Rx+, T/Rx-	X
7, 8	T/Rx+, T/Rx-	X

1.2.4 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.

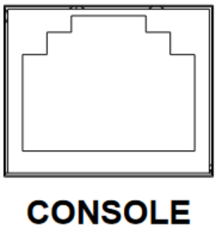
▪DB9 connector connect to computer COM port

▪Baud rate: 115200bps

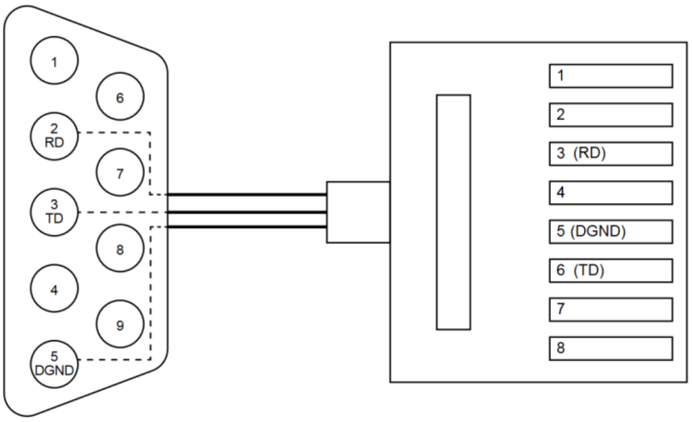
▪8 data bits, 1 stop bit

▪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 (included in package). 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:



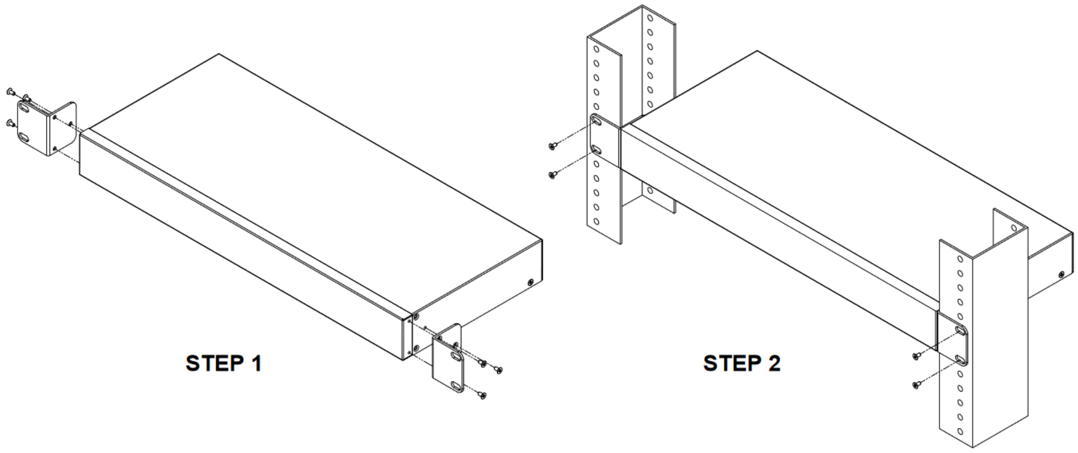
1.2.5 Rack Mounting

STEP 1: Align two brackets with the holes on the sides of the Switch and fasten the mounting kits by using screws.

NOTE: The type of screw is flat head M3 x 5mm.

STEP 2: After attaching two brackets, line up the rack-mounting positions of the holes in the brackets with the appropriate holes on the rack and then fasten the Switch on the rack by using screws.

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



1.2.6 Web Interface: Connect & Login

1. Factory default IP: 192.168.169.1
2. Login with default account and password.

   Username: admin

   Password: admin

1.2.7 CLI Initialization and Configuration

1. Key-in the command under Telnet: telnet 192.168.169.1
2. Login with default account and password.

   Username: admin

   Password: admin
3. Change the IP with commands listed below:

```
config
ip address xxx.xxx.xxx.xxx mask xxx.xxx.xxx.xxx
exit
```

1.3 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.

1.3.1 Web Browser Support

IE 7 (or newer version) with the following default settings is recommended:

Language script	Latin based
Web page font	Times New Roman
Plain text font	Courier New
Encoding	Unicode (UTF-8)
Text size	Medium

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

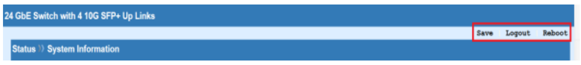
1.3.2 Navigation

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**
- **VLAN**
- **MAC Address Table**
- **Spanning Tree**
- **Discovery**
- **Multicast**
- **Security**
- **ACL**
- **QoS**

- **Diagnostics**
- **Management**

1.3.3 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 un saved change in the configuration will be lost.

2 Using the Web

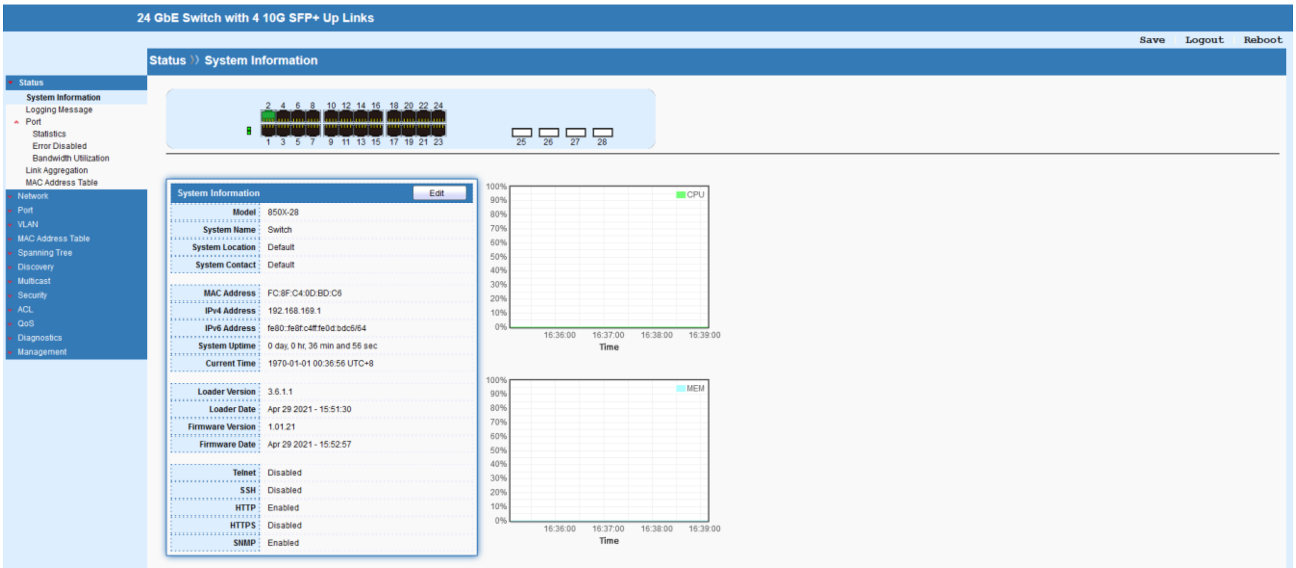
2.1 Login

Operation	1. Open Browser and enter default IP address http://192.168.169.1. 2. Fill Username and Password. 3. Click “LOGIN”
Field	Description
Username	Login user name. The maximum length is 32. Default: admin
Password	Login user password. The maximum length is 32. Default: admin

3 Status

3.1 System Information

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



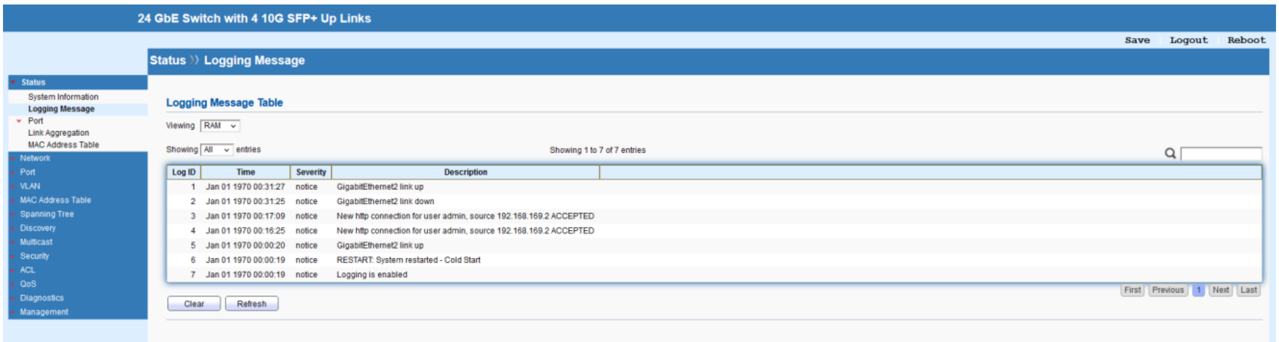
Status » System Information

System Information

Model	850X-28
System Name	Switch
System Location	Default
System Contact	Default
MAC Address	FC:8F:C4:0D:BD:C6
IPv4 Address	192.168.169.1
IPv6 Address	fe80::fe8f:c4ff:fe0d:bdc6/64
System Uptime	0 day, 0 hr, 36 min and 56 sec
Current Time	1970-01-01 00:36:56 UTC+8
Loader Version	3.6.1.1
Loader Date	Apr 29 2021 - 15:51:30
Firmware Version	1.01.21
Firmware Date	Apr 29 2021 - 15:52:57
Telnet	Disabled
SSH	Disabled
HTTP	Enabled
HTTPS	Disabled
SNMP	Enabled

3.2 Logging Message

This page provides the system log for all events.



Status » Logging Message

Logging Message Table

Viewing RAM

Showing All entries

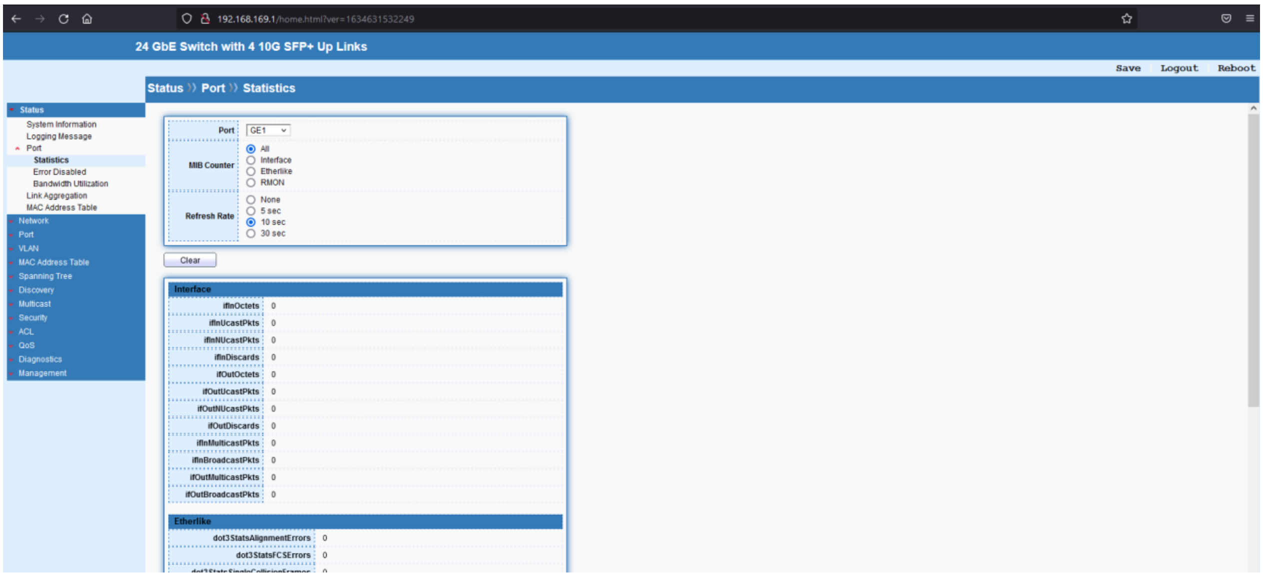
Showing 1 to 7 of 7 entries

Log ID	Time	Severity	Description
1	Jan 01 1970 00:31:27	notice	GigabitEthernet2 link up
2	Jan 01 1970 00:31:25	notice	GigabitEthernet2 link down
3	Jan 01 1970 00:17:09	notice	New http connection for user admin, source 192.168.169.2 ACCEPTED
4	Jan 01 1970 00:16:25	notice	New http connection for user admin, source 192.168.169.2 ACCEPTED
5	Jan 01 1970 00:00:20	notice	GigabitEthernet2 link up
6	Jan 01 1970 00:00:19	notice	RESTART: System restarted - Cold Start
7	Jan 01 1970 00:00:19	notice	Logging is enabled

3.3 Port

3.3.1 Statistics

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



Status » Port » Statistics

Port: GE1

MIB Counter: ● All ○ Interface ○ Etherlike ○ RMON

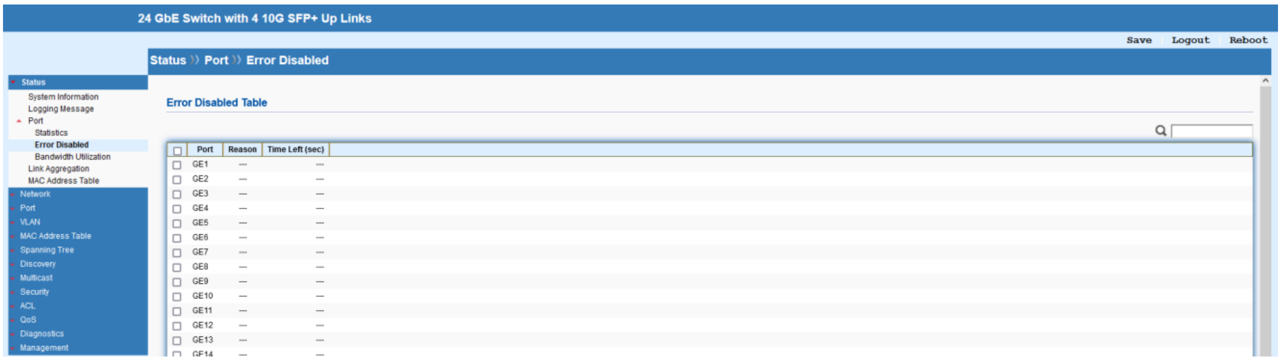
Refresh Rate: ○ None ○ 5 sec ● 10 sec ○ 30 sec

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

Etherlike	
dot3StatsAlignmentErrors	0
dot3StatsFCSErrors	0
dot3StatsSingleCollisionFrames	0

3.3.2 Error Disabled

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



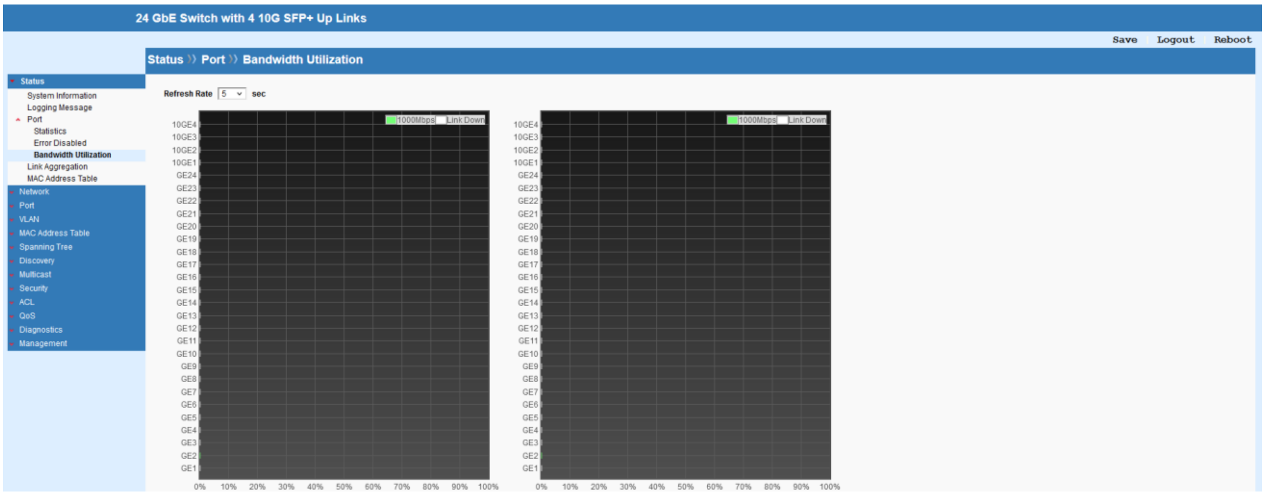
Status » Port » Error Disabled

Error Disabled Table

□	Port	Reason	Time Left (sec)
□	GE1	---	---
□	GE2	---	---
□	GE3	---	---
□	GE4	---	---
□	GE5	---	---
□	GE6	---	---
□	GE7	---	---
□	GE8	---	---
□	GE9	---	---
□	GE10	---	---
□	GE11	---	---
□	GE12	---	---
□	GE13	---	---
□	GE14	---	---

3.3.3 Bandwidth Utilization

This page displays bandwidth utilization for both transmitting and receiving.

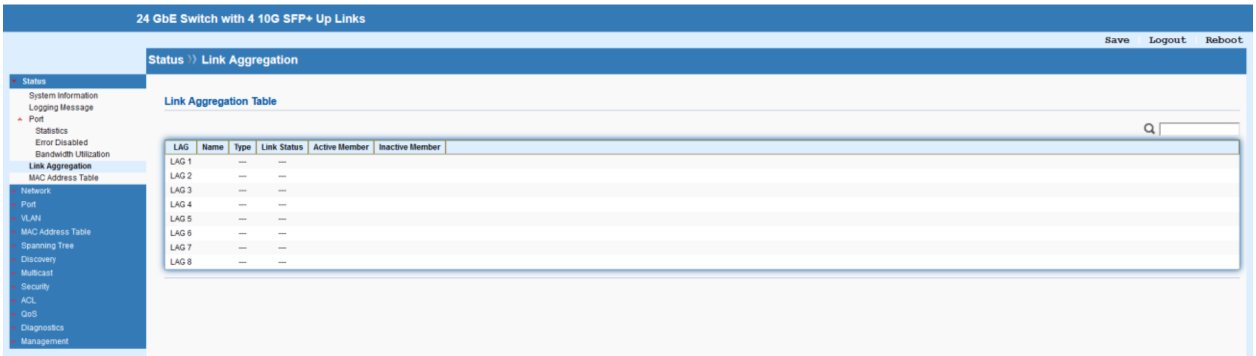


Status » Port » Bandwidth Utilization

Refresh Rate 5 sec

3.4 Link Aggregation

This page displays status of each Link Aggregation port.

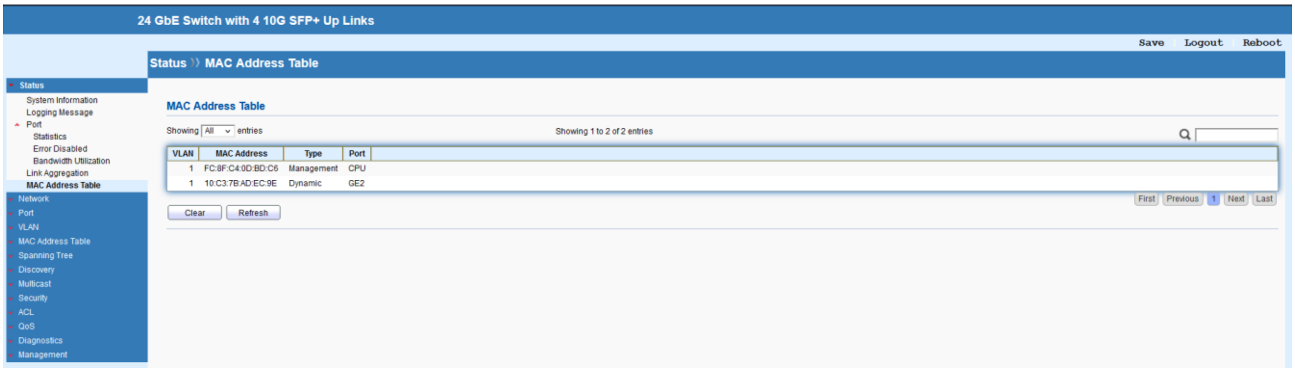


Link Aggregation Table

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

3.5 MAC Address Table

This page displays all MAC addresses that through the 850X-28 Switch.



MAC Address Table

Showing All entries

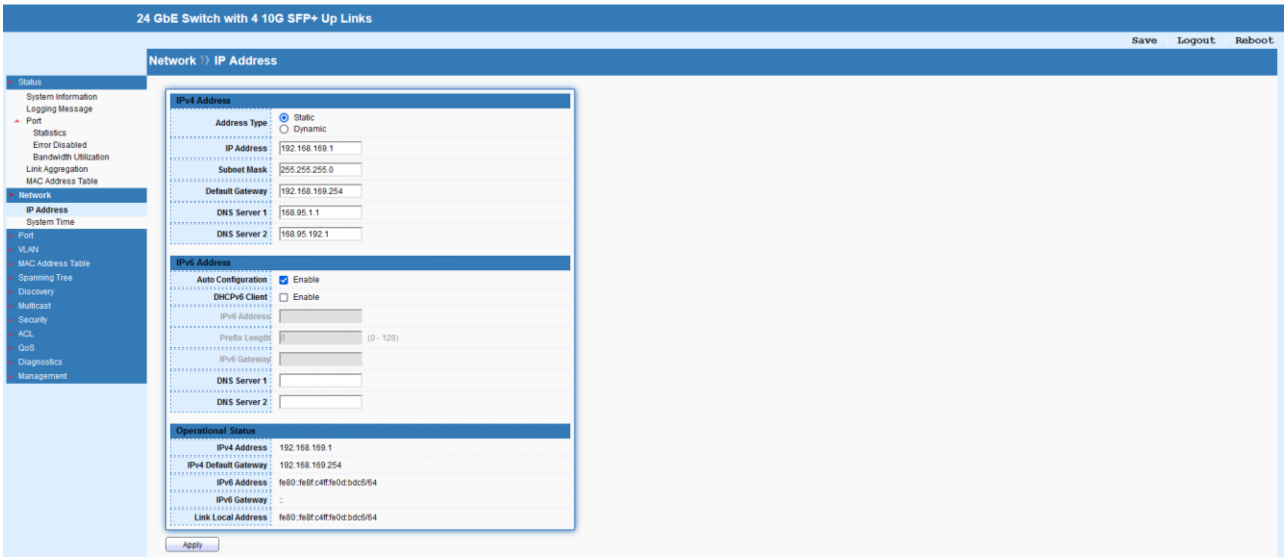
Showing 1 to 2 of 2 entries

VLAN	MAC Address	Type	Port
1	FC:8F:C4:0D:BD:C6	Management	CPU
1	10:C3:7B:AD:EC:9E	Dynamic	GE2

4 Network

4.1 IP Address

The switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.169.1/24. This page allows to configure IP basic settings.



IPv4 Address

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

IPv6 Address

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

Operational Status

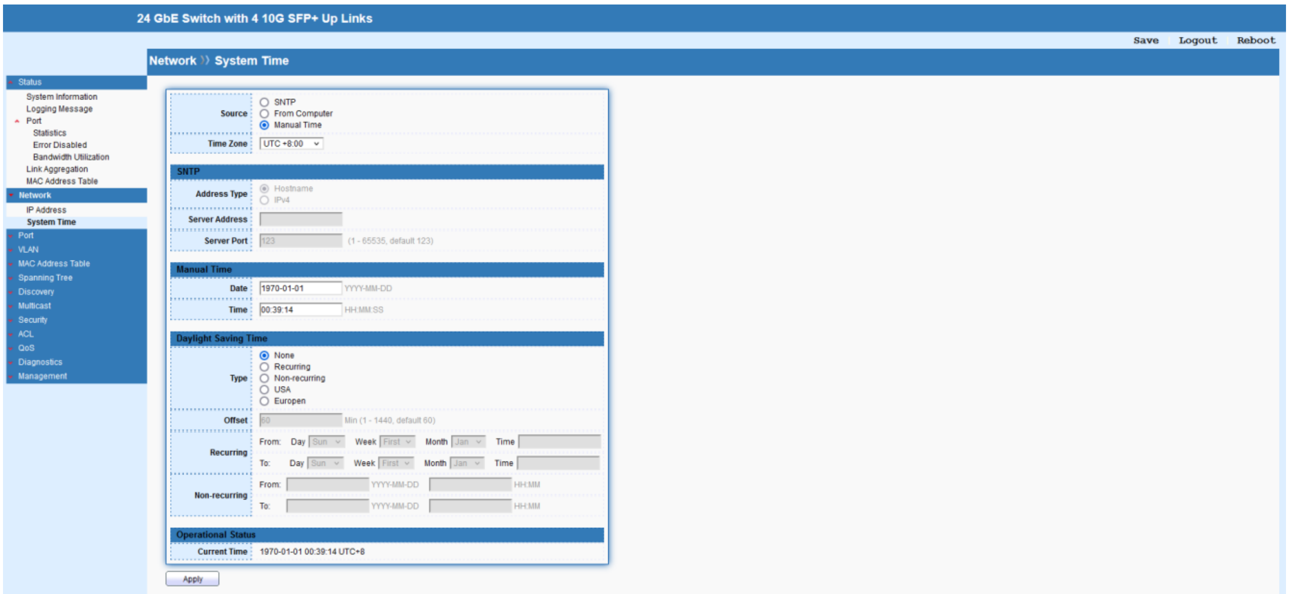
IPv4 Address: 192.168.169.1
IPv4 Default Gateway: 192.168.169.254
IPv6 Address: fe80::fe8f:c4ff:fe0d:bdc6/64
IPv6 Gateway: ::
Link Local Address: fe80::fe8f:c4ff:fe0d:bdc6/64

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.

4.2 System Time

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



Source: ○ SNTP ○ From Computer ● Manual Time

Time Zone: UTC +8:00

SNTP

Address Type: ● Hostname ○ IPv4

Server Address:

Server Port: 123 (1 - 65535, default 123)

Manual Time

Date: 1970-01-01 YYYY-MM-DD

Time: 00:39:14 HH:MM:SS

Daylight Saving Time

Type: ● None ○ Recurring ○ Non-recurring ○ USA ○ Europen

Offset: 60 Min (1 - 1440, default 60)

Recurring: From: Day Sun Week First Month Jan Time / To: Day Sun Week First Month Jan Time

Non-recurring: From: YYYY-MM-DD HH:MM / To: YYYY-MM-DD HH:MM

Operational Status

Current Time: 1970-01-01 00:39:14 UTC+8

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

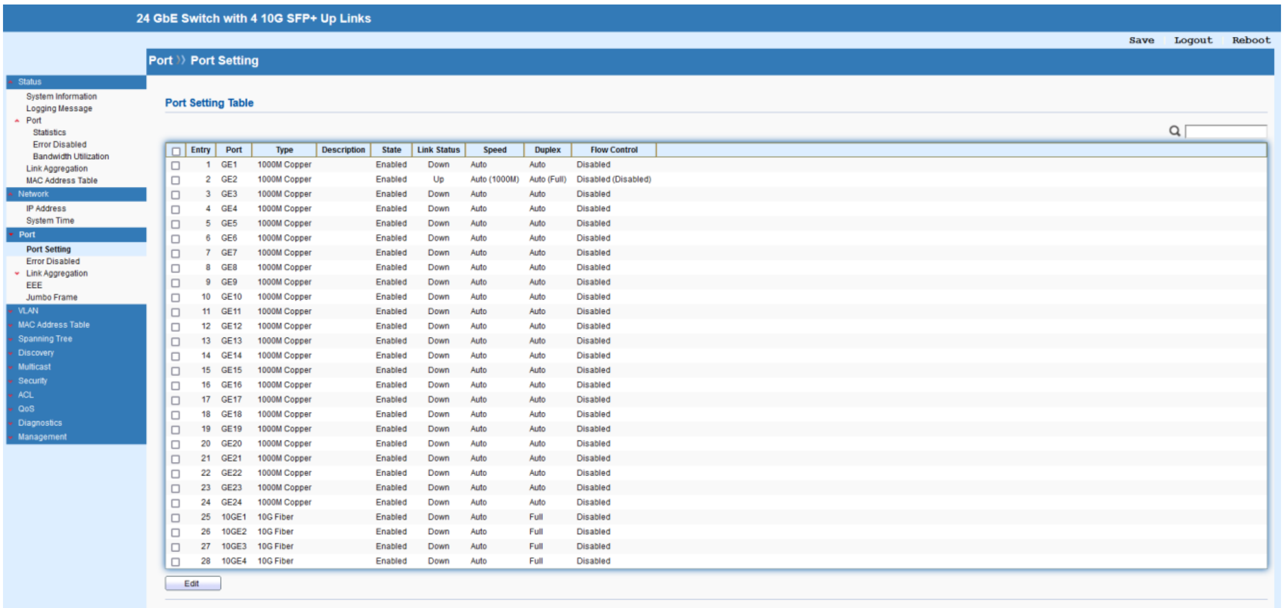
	time. **USA**: Using daylight saving time in the United States that starts on the second Sunday of March and ends on the first Sunday of November. **European**: Using daylight saving time in the Europe that starts on the last Sunday.
Offset	Specify the adjust offset of daylight saving time.
Recurring	**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 Port

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

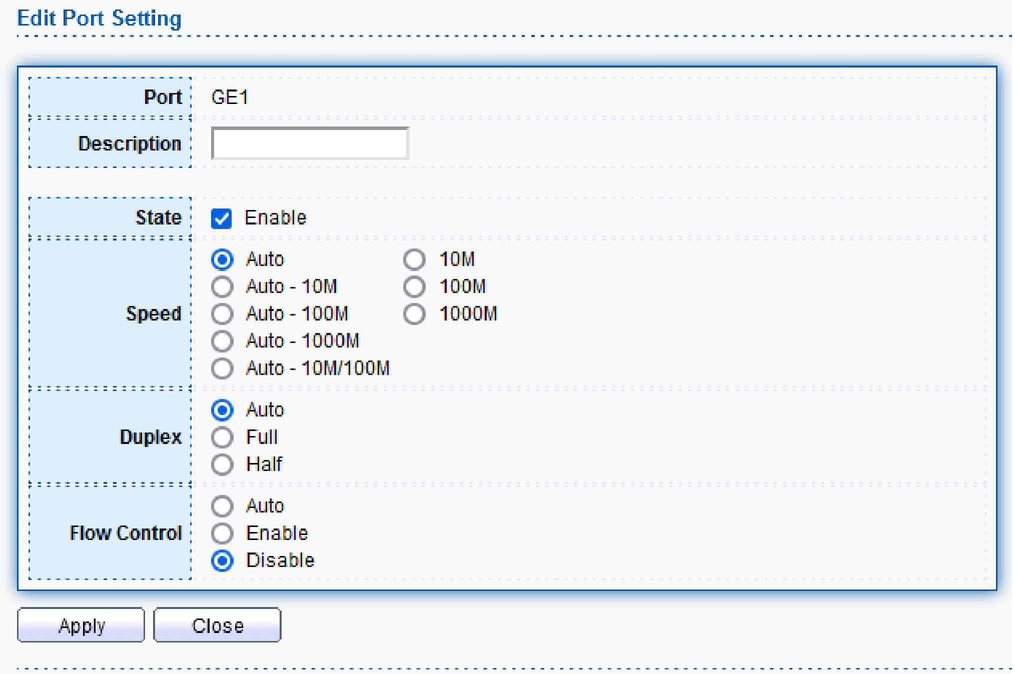
5.1 Port Setting

Available settings are explained as follows.



Port Setting Table

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

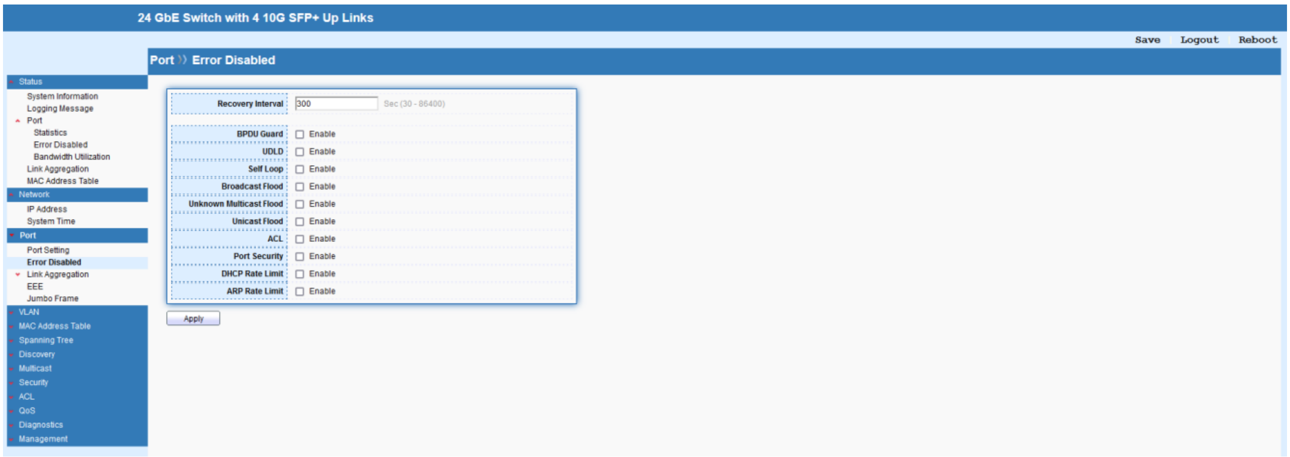


Edit Port Setting

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

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.

5.2 Error Disabled



Recovery Interval: 300 Sec (30 - 86400)

BPDU Guard: □ Enable

UDLD: □ Enable

Self Loop: □ Enable

Broadcast Flood: □ Enable

Unknown Multicast Flood: □ Enable

Unicast Flood: □ Enable

ACL: □ Enable

Port Security: □ Enable

DHCP Rate Limit: □ Enable

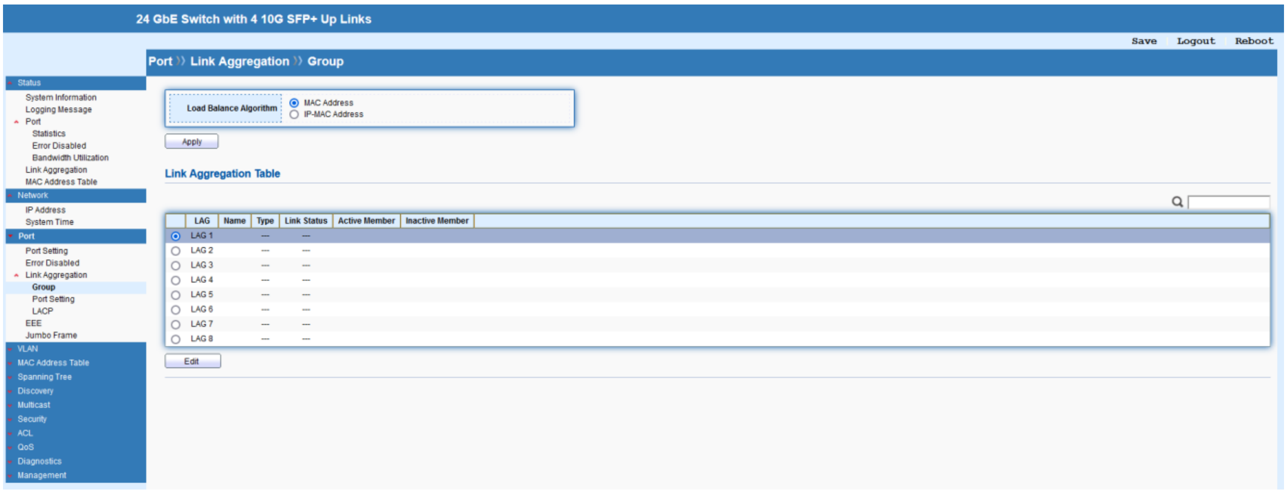
ARP Rate Limit: □ Enable

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.

5.3 Link Aggregation

5.3.1 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.



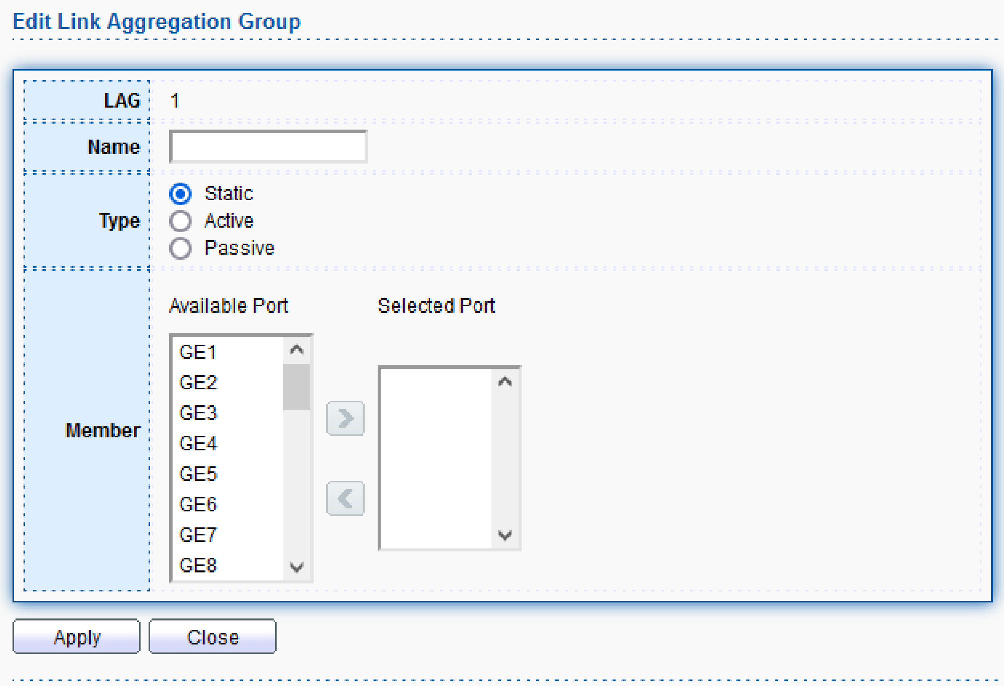
Port » Link Aggregation » Group

Load Balance Algorithm ● MAC Address ○ IP-MAC Address

Link Aggregation Table

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

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.



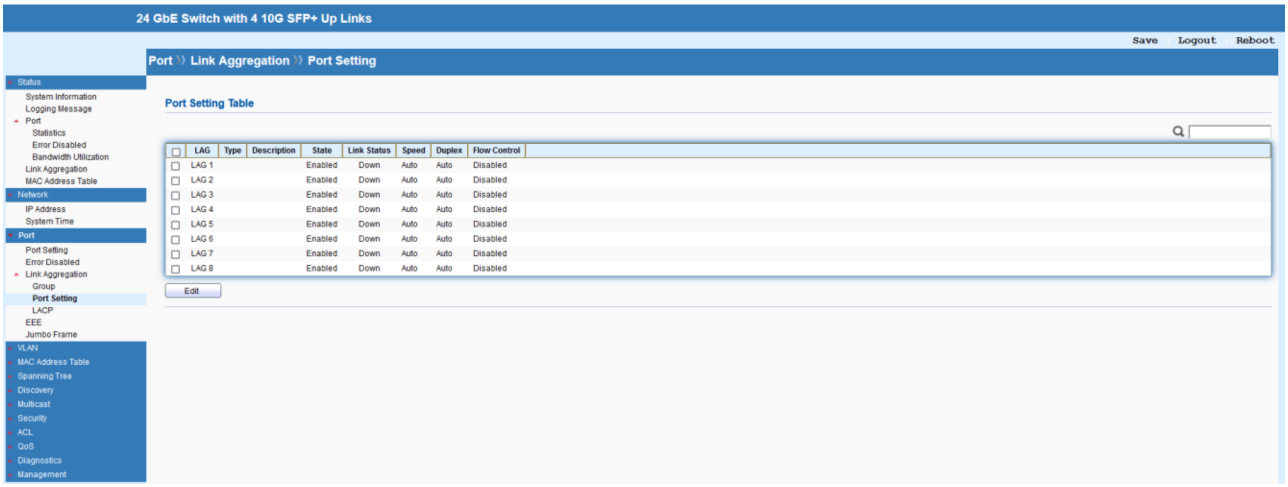
Edit Link Aggregation Group

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

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. **Passive**: The interface is not in an active negotiating state. LACP runs on any link that is configured in a passive mode. The port in a passive mode responds to negotiations requests from other ports that are in an active mode. Ports in passive mode respond to 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.

5.3.2 Port Setting

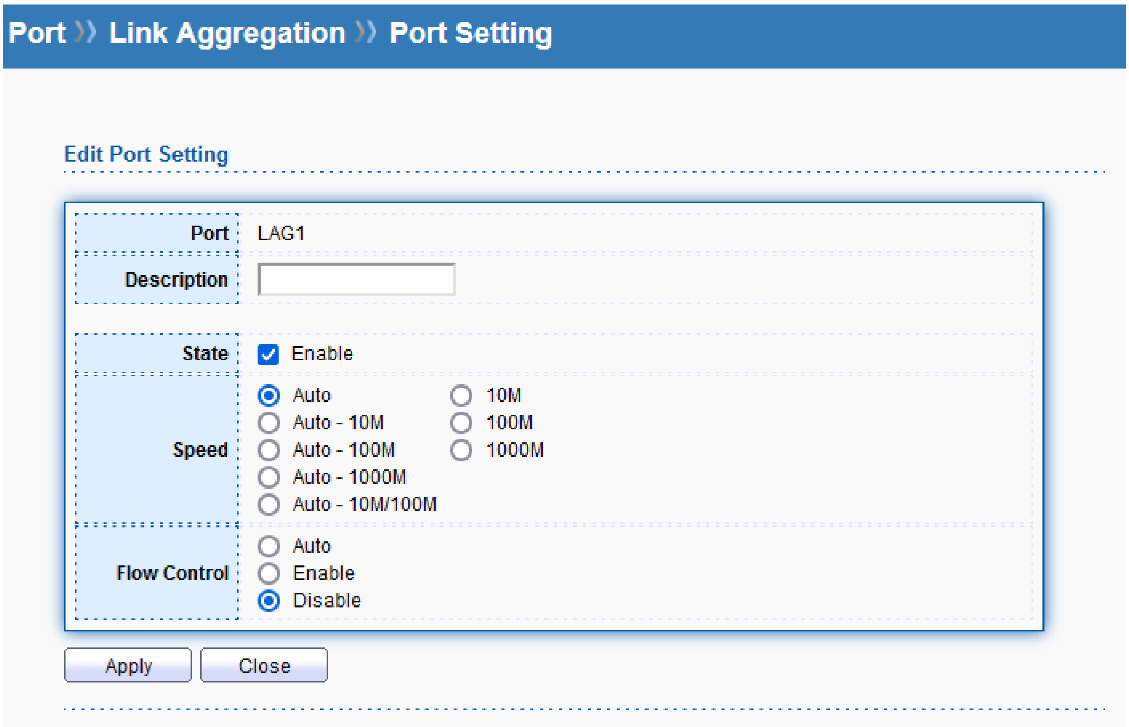
This page defines port setting for each LAG profile (LAG1 to LAG8), including data speed and enabling/disabling the flow control.



Port Setting Table

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

Item	Description
Edit	Edit the settings of LAG port.



Edit Port Setting

Port: LAG1

Description:

State: ☑ Enable

Speed: ● Auto ○ Auto - 10M ○ Auto - 100M ○ Auto - 1000M ○ Auto - 10M/100M ○ 10M ○ 100M ○ 1000M

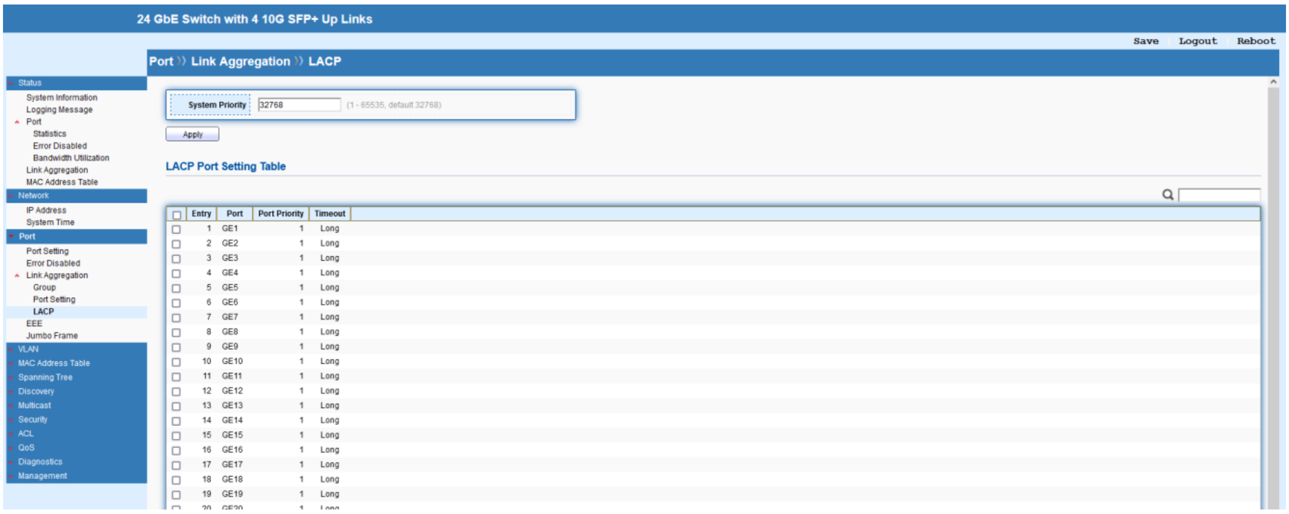
Flow Control: ○ Auto ○ Enable ● Disable

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	Select the mode of Flow Control for current LAG port. Flow Control is used to regulate transmission of signals to

	match the bandwidth of the receiving port. The switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

5.3.3 LACP

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

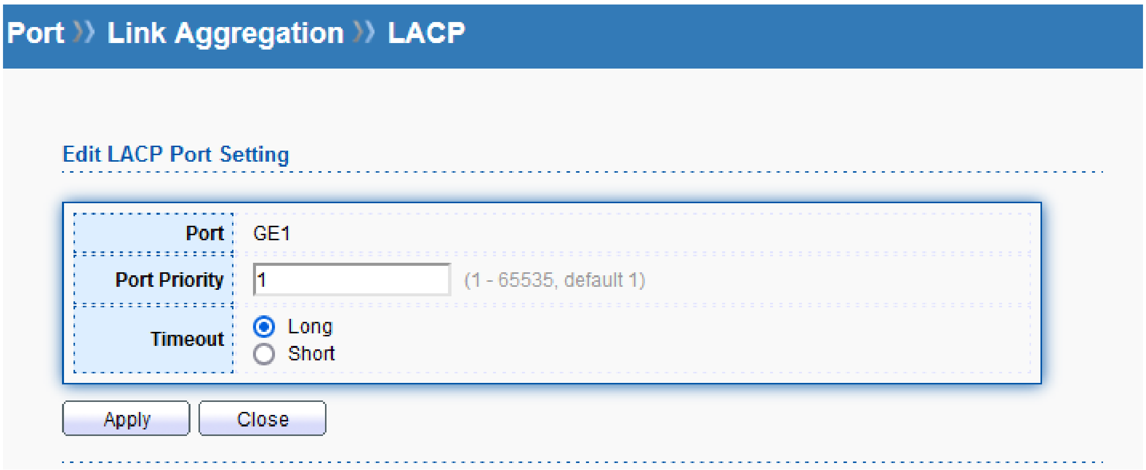


System Priority: 32768 (1 - 65535, default 32768)

LACP Port Setting Table

□	Entry	Port	Port Priority	Timeout
□	1	GE1	1	Long
□	2	GE2	1	Long
□	3	GE3	1	Long
□	4	GE4	1	Long
□	5	GE5	1	Long
□	6	GE6	1	Long
□	7	GE7	1	Long
□	8	GE8	1	Long
□	9	GE9	1	Long
□	10	GE10	1	Long
□	11	GE11	1	Long
□	12	GE12	1	Long
□	13	GE13	1	Long
□	14	GE14	1	Long
□	15	GE15	1	Long
□	16	GE16	1	Long
□	17	GE17	1	Long
□	18	GE18	1	Long
□	19	GE19	1	Long
□	20	GE20	1	Long

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.


Port » Link Aggregation » LACP

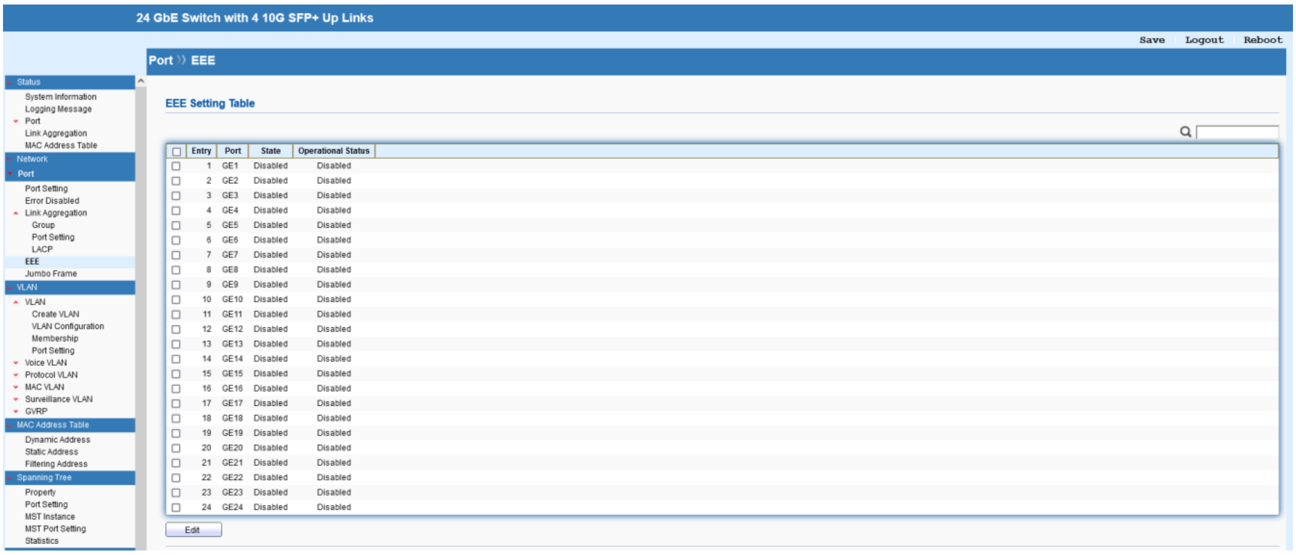
Edit LACP Port Setting

Port	GE1
Port Priority	1 (1 - 65535, default 1)
Timeout	● Long ○ Short

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.

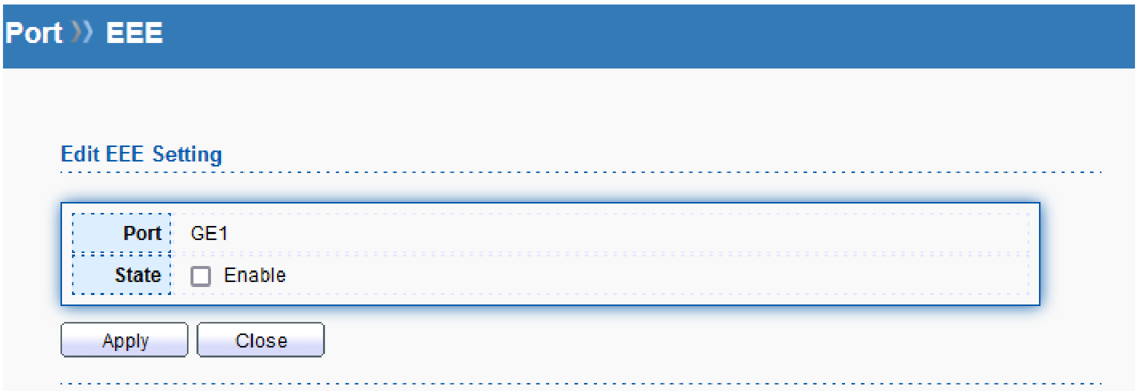
5.4 EEE

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



EEE Setting Table

□	Entry	Port	State	Operational Status
□	1	GE1	Disabled	Disabled
□	2	GE2	Disabled	Disabled
□	3	GE3	Disabled	Disabled
□	4	GE4	Disabled	Disabled
□	5	GE5	Disabled	Disabled
□	6	GE6	Disabled	Disabled
□	7	GE7	Disabled	Disabled
□	8	GE8	Disabled	Disabled
□	9	GE9	Disabled	Disabled
□	10	GE10	Disabled	Disabled
□	11	GE11	Disabled	Disabled
□	12	GE12	Disabled	Disabled
□	13	GE13	Disabled	Disabled
□	14	GE14	Disabled	Disabled
□	15	GE15	Disabled	Disabled
□	16	GE16	Disabled	Disabled
□	17	GE17	Disabled	Disabled
□	18	GE18	Disabled	Disabled
□	19	GE19	Disabled	Disabled
□	20	GE20	Disabled	Disabled
□	21	GE21	Disabled	Disabled
□	22	GE22	Disabled	Disabled
□	23	GE23	Disabled	Disabled
□	24	GE24	Disabled	Disabled



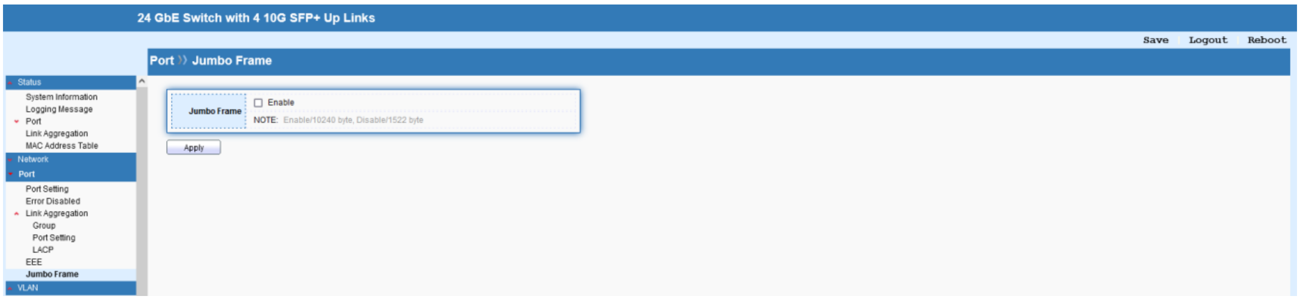
Edit EEE Setting

Port	GE1
State	□ Enable

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.

5.5 Jumbo Frame

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



Jumbo Frame: □ Enable

NOTE: Enable/10240 byte, Disable/1522 byte

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

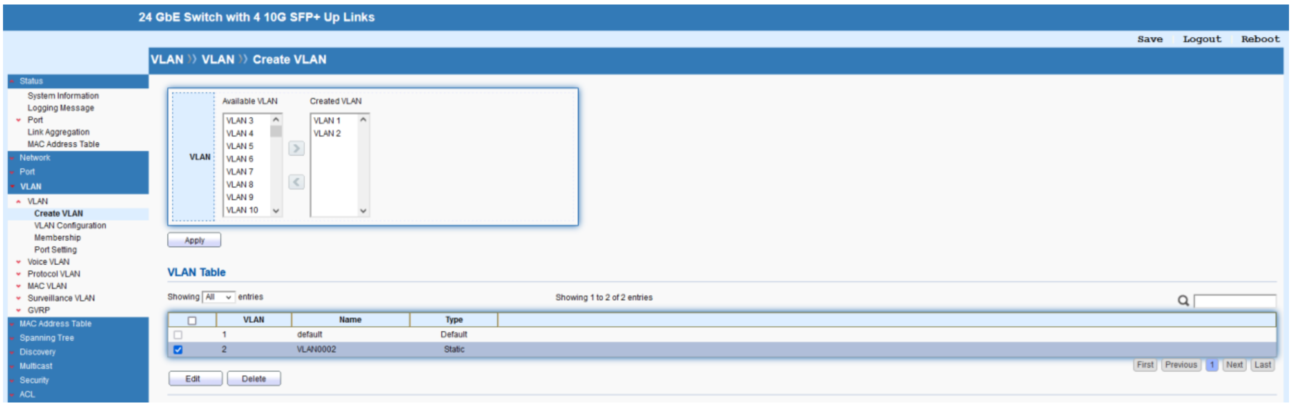
6 VLAN

This section allows for controlling VLAN configuration on the switch

6.1 VLAN

6.1.1 Create VLAN

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



VLAN

Available VLAN: VLAN 3, VLAN 4, VLAN 5, VLAN 6, VLAN 7, VLAN 8, VLAN 9, VLAN 10

Created VLAN: VLAN 1, VLAN 2

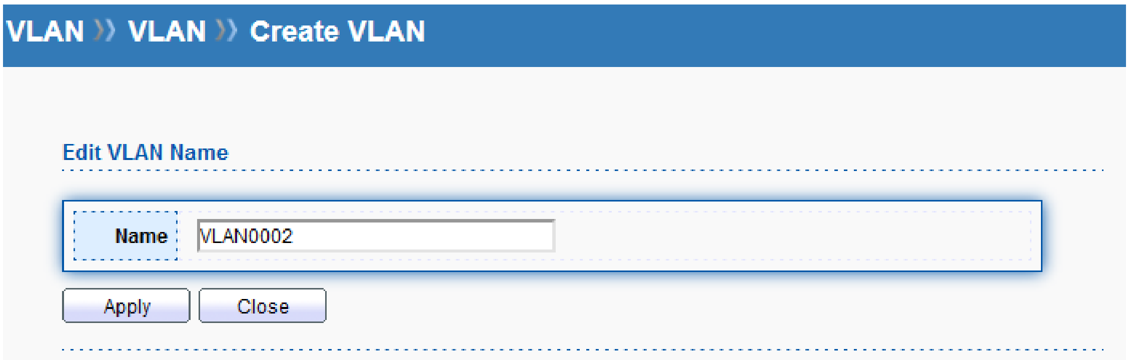
VLAN Table

Showing All entries

Showing 1 to 2 of 2 entries

□	VLAN	Name	Type
□	1	default	Default
☑	2	VLAN0002	Static

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.



VLAN » VLAN » Create VLAN

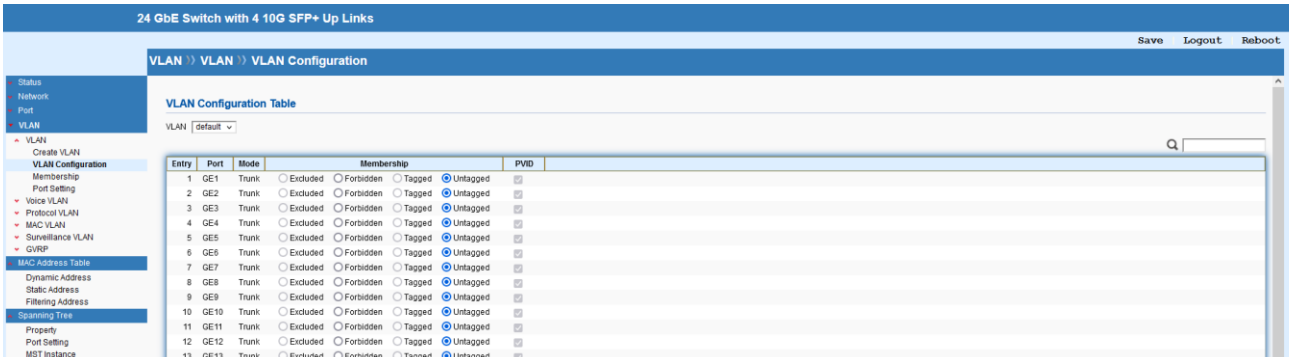
Edit VLAN Name

Name: VLAN0002

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.

6.1.2 VLAN Configuration

This page allows to configure interface setting related to VLAN.



VLAN » VLAN » VLAN Configuration

VLAN Configuration Table

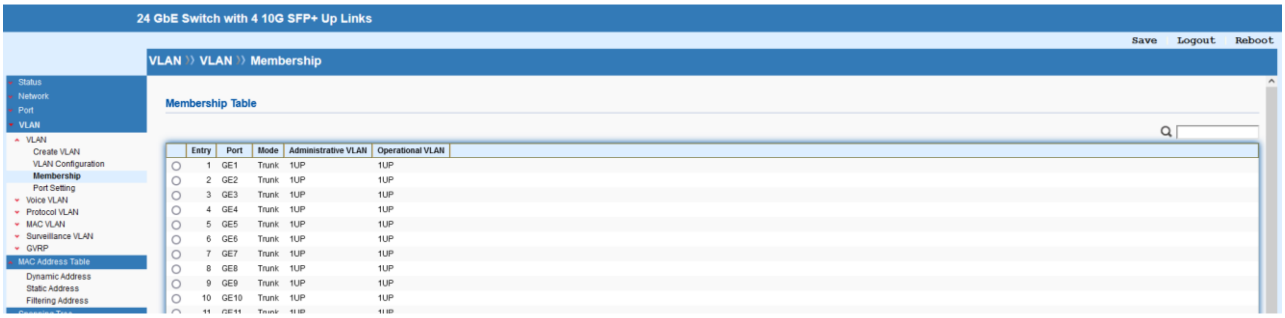
VLAN: default

Entry	Port	Mode	Membership	PVID
1	GE1	Trunk	○ Excluded ○ Forbidden ○ Tagged ● Untagged	☑
2	GE2	Trunk	○ Excluded ○ Forbidden ○ Tagged ● Untagged	☑
3	GE3	Trunk	○ Excluded ○ Forbidden ○ Tagged ● Untagged	☑
4	GE4	Trunk	○ Excluded ○ Forbidden ○ Tagged ● Untagged	☑
5	GE5	Trunk	○ Excluded ○ Forbidden ○ Tagged ● Untagged	☑
6	GE6	Trunk	○ Excluded ○ Forbidden ○ Tagged ● Untagged	☑
7	GE7	Trunk	○ Excluded ○ Forbidden ○ Tagged ● Untagged	☑
8	GE8	Trunk	○ Excluded ○ Forbidden ○ Tagged ● Untagged	☑
9	GE9	Trunk	○ Excluded ○ Forbidden ○ Tagged ● Untagged	☑
10	GE10	Trunk	○ Excluded ○ Forbidden ○ Tagged ● Untagged	☑
11	GE11	Trunk	○ Excluded ○ Forbidden ○ Tagged ● Untagged	☑
12	GE12	Trunk	○ Excluded ○ Forbidden ○ Tagged ● Untagged	☑
13	GE13	Trunk	○ Excluded ○ Forbidden ○ Tagged ● Untagged	

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.

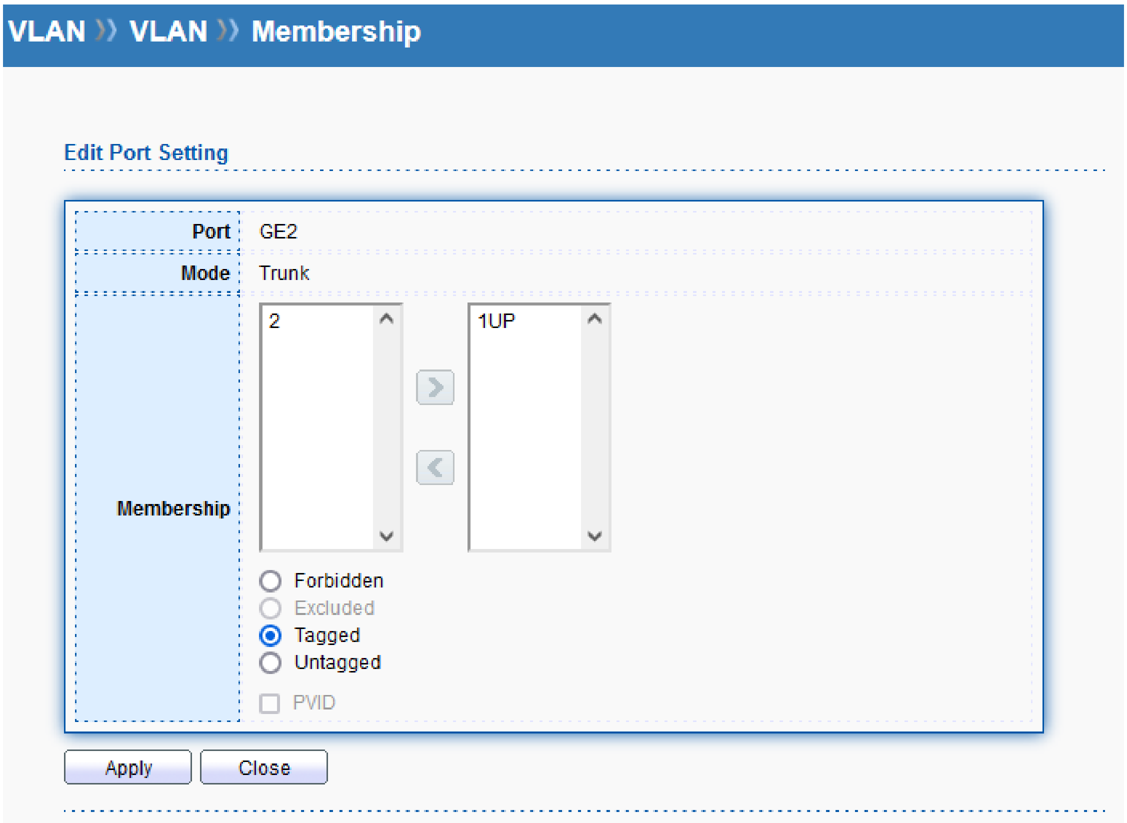
6.1.3 Membership

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



Membership Table

	Entry	Port	Mode	Administrative VLAN	Operational VLAN
○	1	GE1	Trunk	1UP	1UP
○	2	GE2	Trunk	1UP	1UP
○	3	GE3	Trunk	1UP	1UP
○	4	GE4	Trunk	1UP	1UP
○	5	GE5	Trunk	1UP	1UP
○	6	GE6	Trunk	1UP	1UP
○	7	GE7	Trunk	1UP	1UP
○	8	GE8	Trunk	1UP	1UP
○	9	GE9	Trunk	1UP	1UP
○	10	GE10	Trunk	1UP	1UP
○	11	GE11	Trunk	1UP	1UP



Edit Port Setting

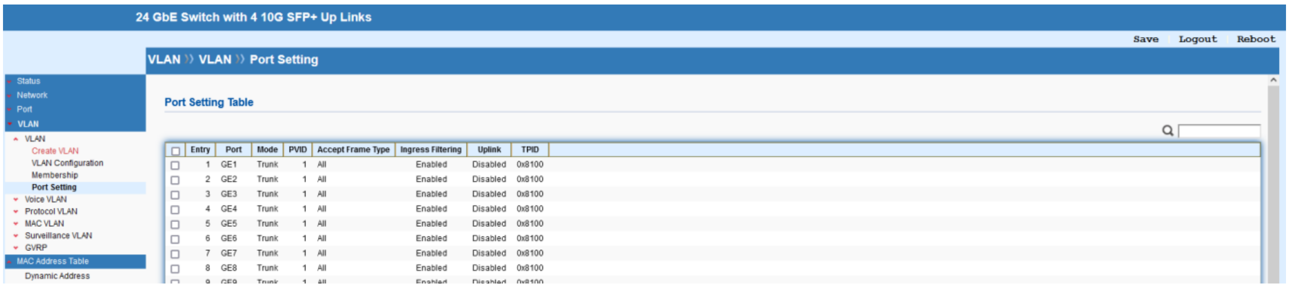
Port	GE2
Mode	Trunk
Membership	2 1UP ○ Forbidden ○ Excluded ● Tagged ○ Untagged □ PVID

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.

6.1.4 Port Setting

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



Port Setting Table

□	Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
□	1	GE1	Trunk	1	All	Enabled	Disabled	0x8100
□	2	GE2	Trunk	1	All	Enabled	Disabled	0x8100
□	3	GE3	Trunk	1	All	Enabled	Disabled	0x8100
□	4	GE4	Trunk	1	All	Enabled	Disabled	0x8100
□	5	GE5	Trunk	1	All	Enabled	Disabled	0x8100
□	6	GE6	Trunk	1	All	Enabled	Disabled	0x8100
□	7	GE7	Trunk	1	All	Enabled	Disabled	0x8100
□	8	GE8	Trunk	1	All	Enabled	Disabled	0x8100
□	9	GE9	Trunk	1	All	Enabled	Disabled	0x8100

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

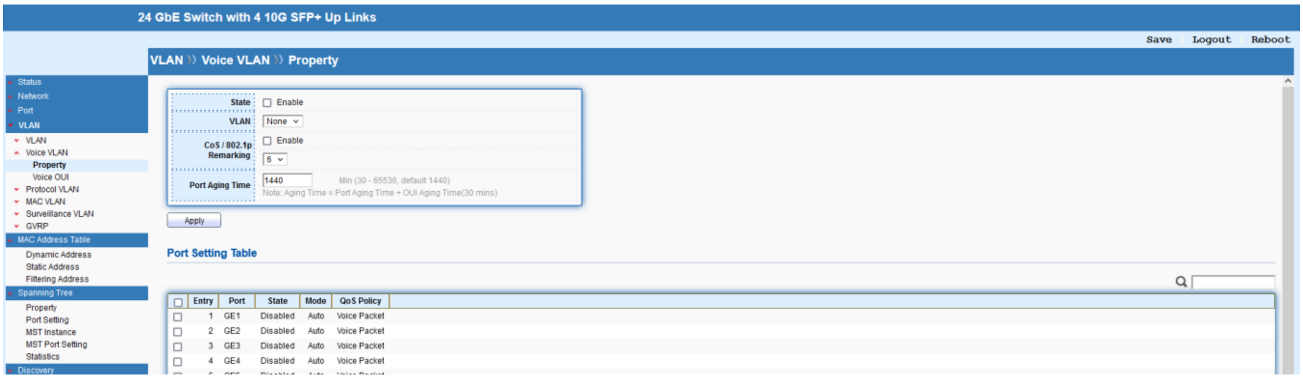
	recognize double tagging on the interface.
TPID	Specify the TPID of the port.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

6.2 Voice VLAN

With such feature, a VLAN will be created temporarily and when the specified OUI device delivers protocol packets related to “VoIP”, the 850X-28 Switch will guide these packets into the specified Voice LAN with specified prioroty tag to speed up the packet transmission. Such voice VLAN is only active inside VigorSwitch for packet transmission. After these packets leave VigorSwitch, the Voice VLAN tag will be removed immediately.

6.2.1 Property

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



State: □ Enable

VLAN: None

CoS / 802.1p Remarking: □ Enable; 6

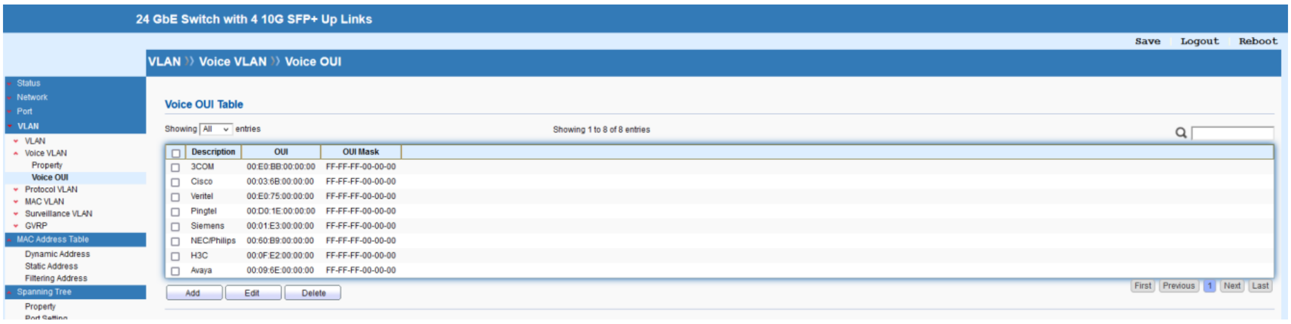
Port Aging Time: 1440 Min (30 - 65536, default 1440)
Note: Aging Time = Port Aging Time + OUI Aging Time(30 mins)

□	Entry	Port	State	Mode	QoS Policy
□	1	GE1	Disabled	Auto	Voice Packet
□	2	GE2	Disabled	Auto	Voice Packet
□	3	GE3	Disabled	Auto	Voice Packet
□	4	GE4	Disabled	Auto	Voice Packet

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.

6.2.2 Voice OUI

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



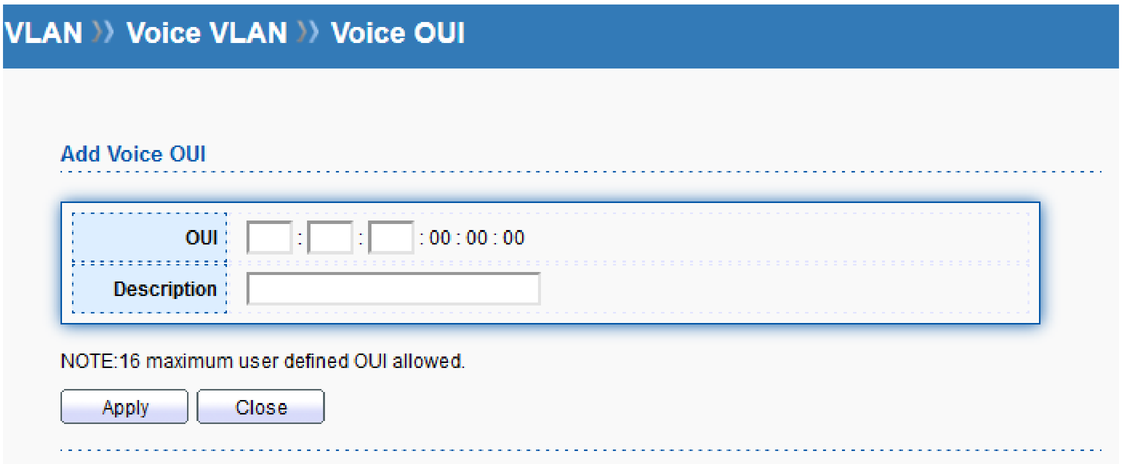
VLAN ›› Voice VLAN ›› Voice OUI

Voice OUI Table

Showing All entries

Showing 1 to 8 of 8 entries

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



VLAN ›› Voice VLAN ›› Voice OUI

Add Voice OUI

OUI: ___ : ___ : ___ : 00 : 00 : 00

Description: ___

NOTE:16 maximum user defined OUI allowed.

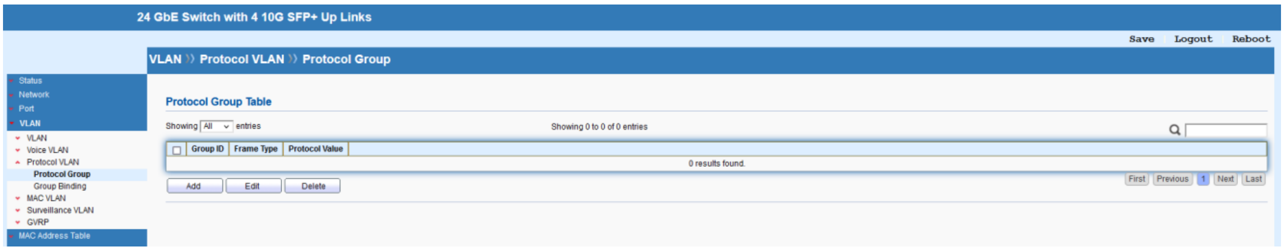
Item	Description
Add	Add a new OUI entry.
Edit	Edit the existing OUI entry.
Delete	Delete the existing OUI entry.
OUI	Type OUI address.
Description	Enter a description of the specified MAC address to the voice VLAN OUI table.
Apply	Apply the settings to the switch.
Close	Close the setting page and back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

6.3 Protocol VLAN

The 850X-28 Switch offers protocol VLANs which allows Network Administrator to filter out untagged
traffic of certain protocol and then assign them a specific VLAN ID.

6.3.1 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.



24 GbE Switch with 4 10G SFP+ Up Links

Save Logout Reboot

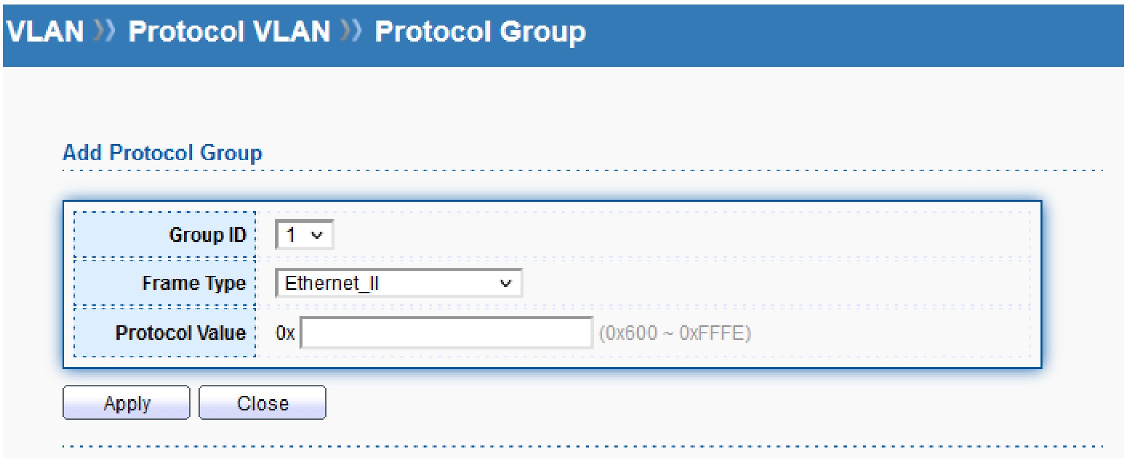
VLAN ›› Protocol VLAN ›› Protocol Group

Protocol Group Table

Showing All entries

Showing 0 to 0 of 0 entries

□	Group ID	Frame Type	Protocol Value
0 results found.			



VLAN ›› Protocol VLAN ›› Protocol Group

Add Protocol Group

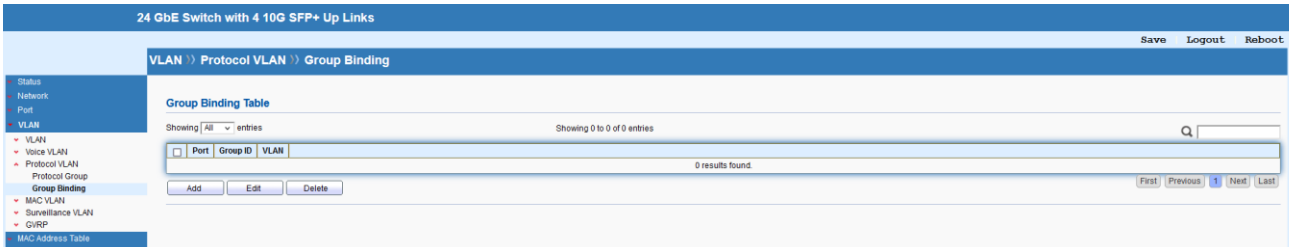
Group ID	1
Frame Type	Ethernet_II
Protocol Value	0x (0x600 ~ 0xFFFE)

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.

6.3.1.1 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.



VLAN » Protocol VLAN » Group Binding

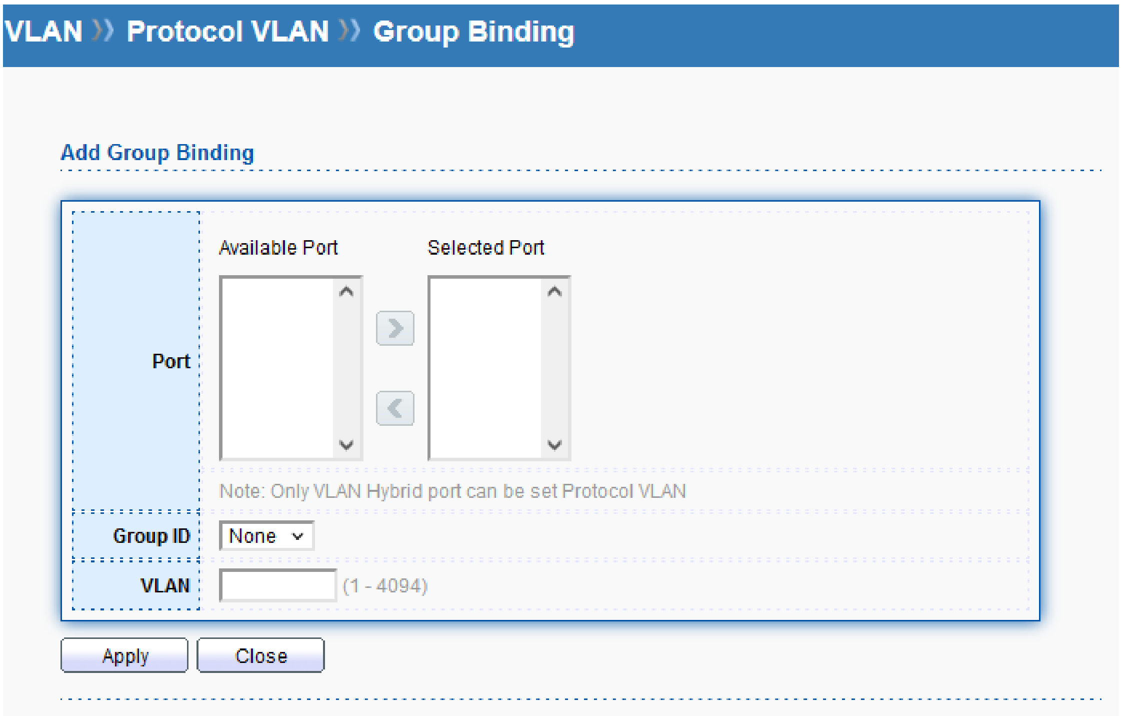
Group Binding Table

Showing All entries

Showing 0 to 0 of 0 entries

□	Port	Group ID	VLAN

0 results found.



VLAN » Protocol VLAN » Group Binding

Add Group Binding

Port: Available Port / Selected Port

Note: Only VLAN Hybrid port can be set Protocol VLAN

Group ID: None

VLAN: (1 - 4094)

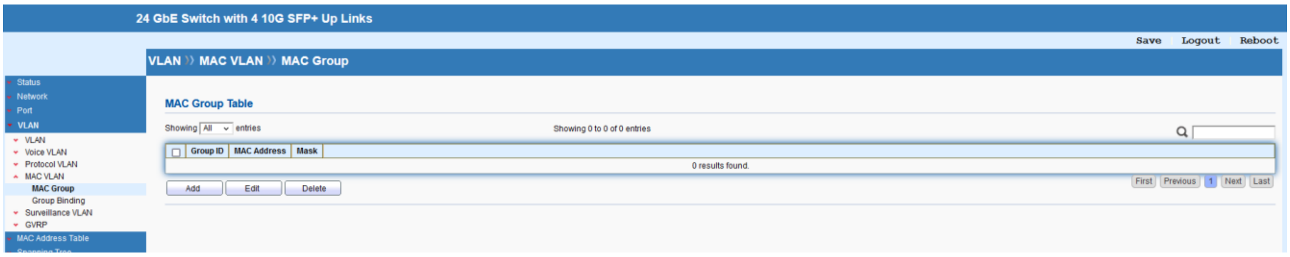
Item	Description
Add	Add a new entry.
Edit	Edit the VLAN number of existing entry.
Delete	Delete the existing entry.
Port	Select one or more ports for applying protocol-based VLAN. Note that protocol-based VLAN can only be applied to the ports of which Interface VLAN Mode is set to “Hybrid”.
Group ID	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.

6.4 MAC VLAN

The MAC VLAN allows you to statically assign a VLAN ID to a host with specific MAC address(es). The 850X-28 Swtich allows you configure multiple groups with configured MAC address and mask to be
active on ports and to be bound with VLAN ID.

6.4.1 MAC Group

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



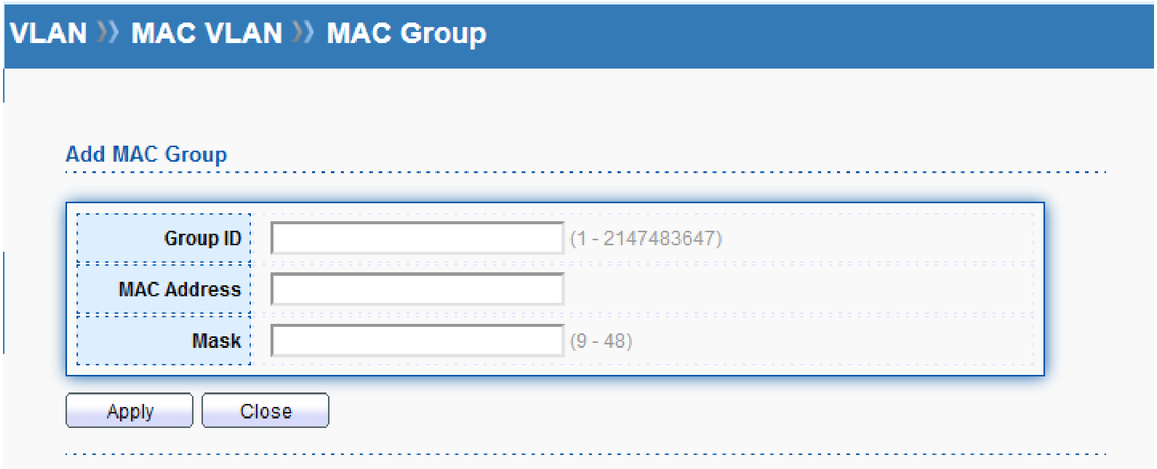
MAC Group Table

Showing All entries

Showing 0 to 0 of 0 entries

□	Group ID	MAC Address	Mask

0 results found.



Add MAC Group

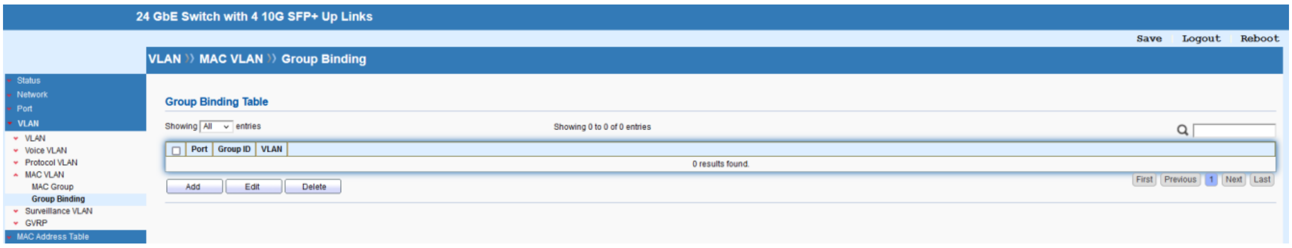
Group ID		(1 - 2147483647)
MAC Address		
Mask		(9 - 48)

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.

6.4.2 Group Binding

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

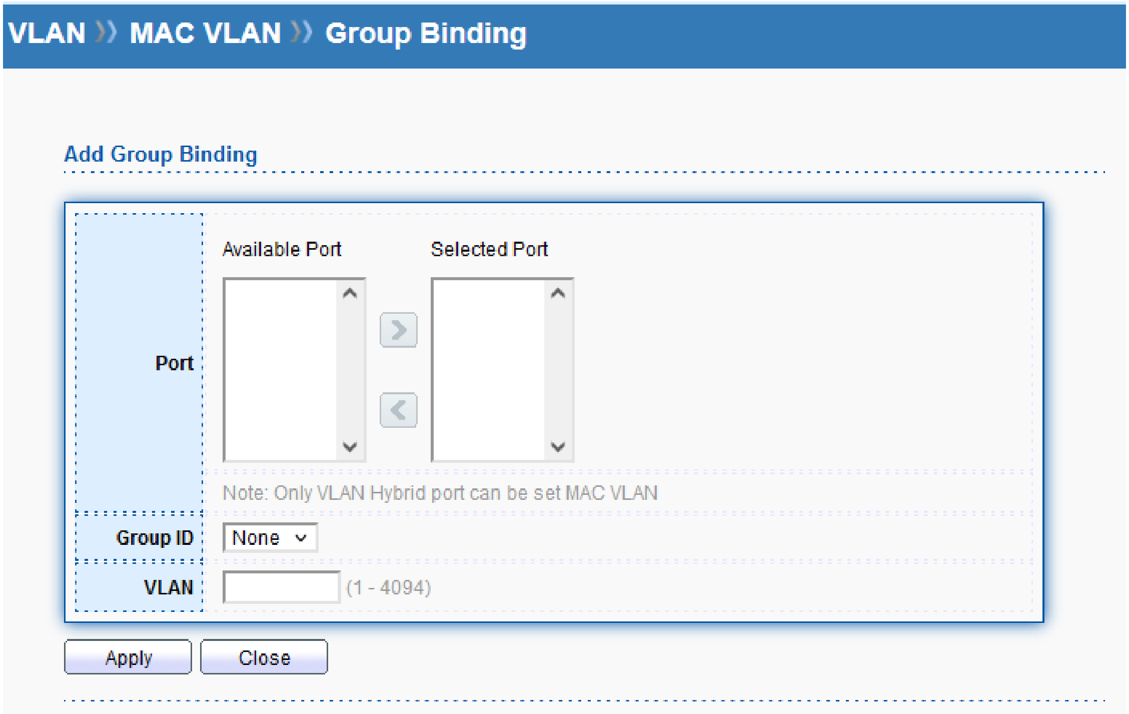


Showing All entries

Showing 0 to 0 of 0 entries

□	Port	Group ID	VLAN

0 results found.



Note: Only VLAN Hybrid port can be set MAC VLAN

Group ID: None

VLAN: (1 - 4094)

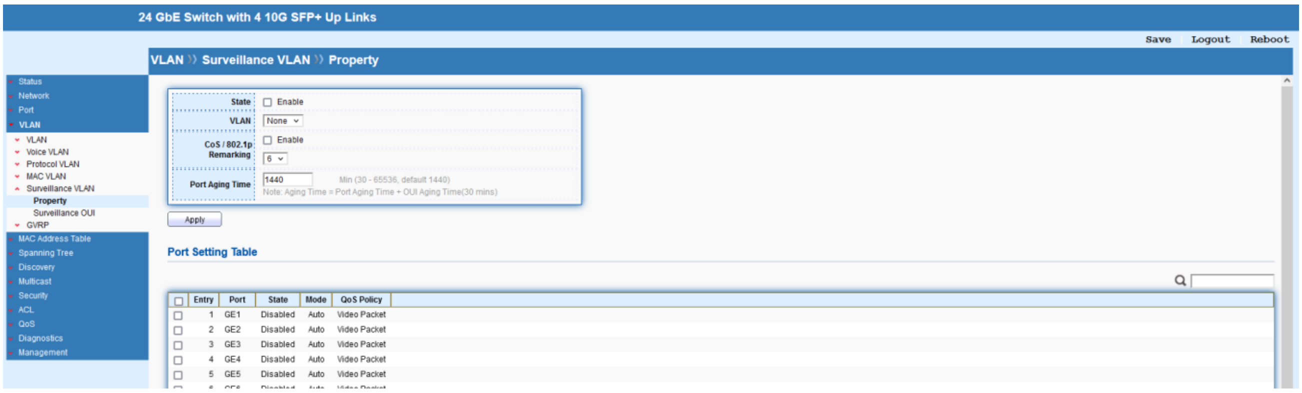
Item	Description
Add	Add a new entry.
Edit	Edit the existing entry.
Delete	Delete the existing entry.
Port	Select the ports you wish to be bound with specified MAC address group.
Group ID	Choose the group ID you have created in section MAC VLAN ➔ MAC Group.
VLAN	Enter the VLAN ID that you wish to be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

6.5 Surveillance VLAN

Surveillance VLAN can be configured for the 850X-28 Swtich 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.

6.5.1 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.

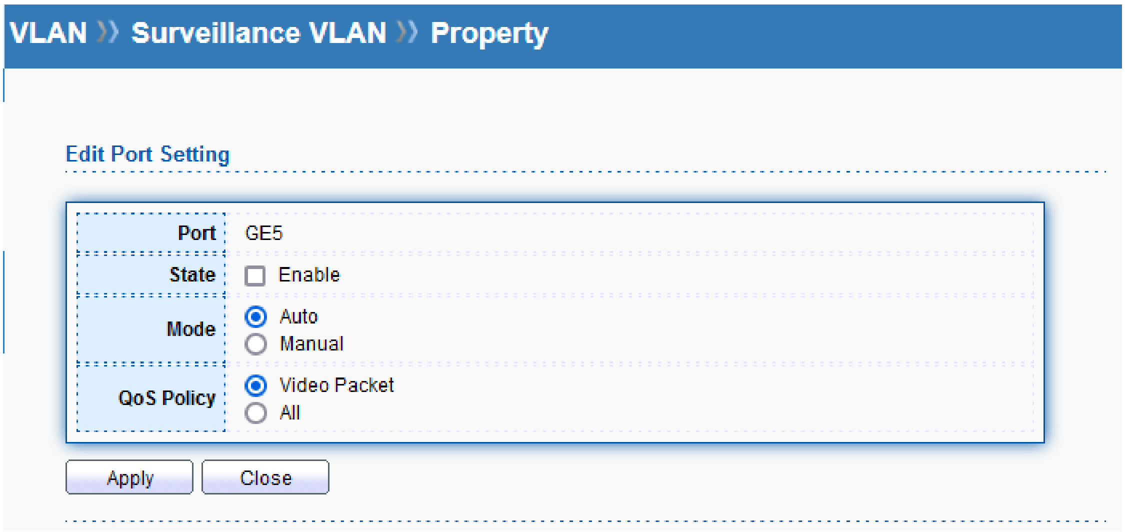


VLAN » Surveillance VLAN » Property

State	□ Enable
VLAN	None
CoS / 802.1p Remarking	□ Enable 6
Port Aging Time	1440 Min (30 - 65536, default 1440) Note: Aging Time = Port Aging Time + OUI Aging Time(30 mins)

Port Setting Table

□	Entry	Port	State	Mode	QoS Policy
□	1	GE1	Disabled	Auto	Video Packet
□	2	GE2	Disabled	Auto	Video Packet
□	3	GE3	Disabled	Auto	Video Packet
□	4	GE4	Disabled	Auto	Video Packet
□	5	GE5	Disabled	Auto	Video Packet



VLAN » Surveillance VLAN » Property

Edit Port Setting

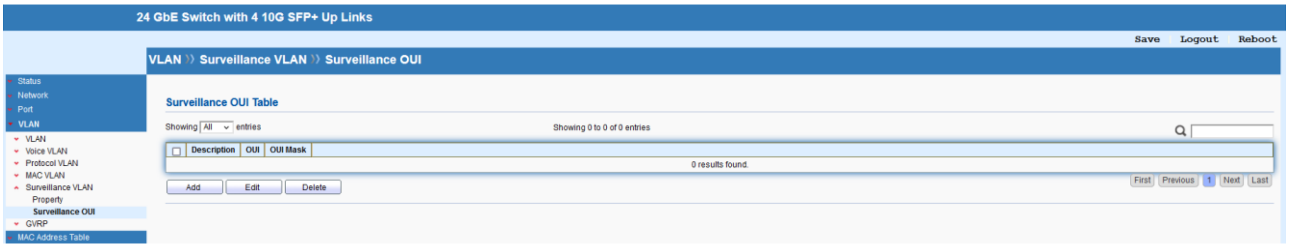
Port	GE5
State	□ Enable
Mode	● Auto ○ Manual
QoS Policy	● Video Packet ○ All

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.

6.5.2 Surveillance OUI

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



Surveillance OUI Table

Showing All entries

Showing 0 to 0 of 0 entries

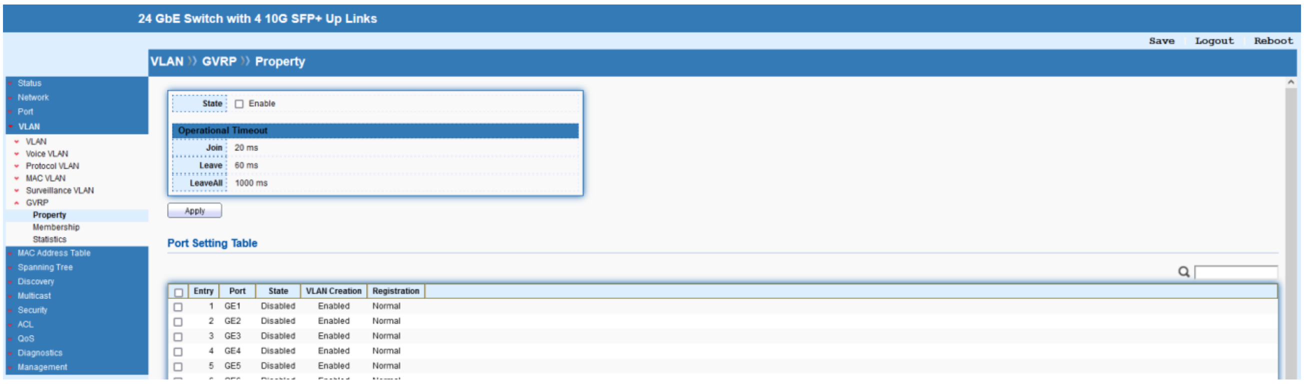
□	Description	OUI	OUI Mask
0 results found.			

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.

6.6 GVRP

6.6.1 Property

This page allows to enable or disable the GVRP function.



VLAN » GVRP » Property

State ☐ Enable

Operational Timeout

Join 20 ms

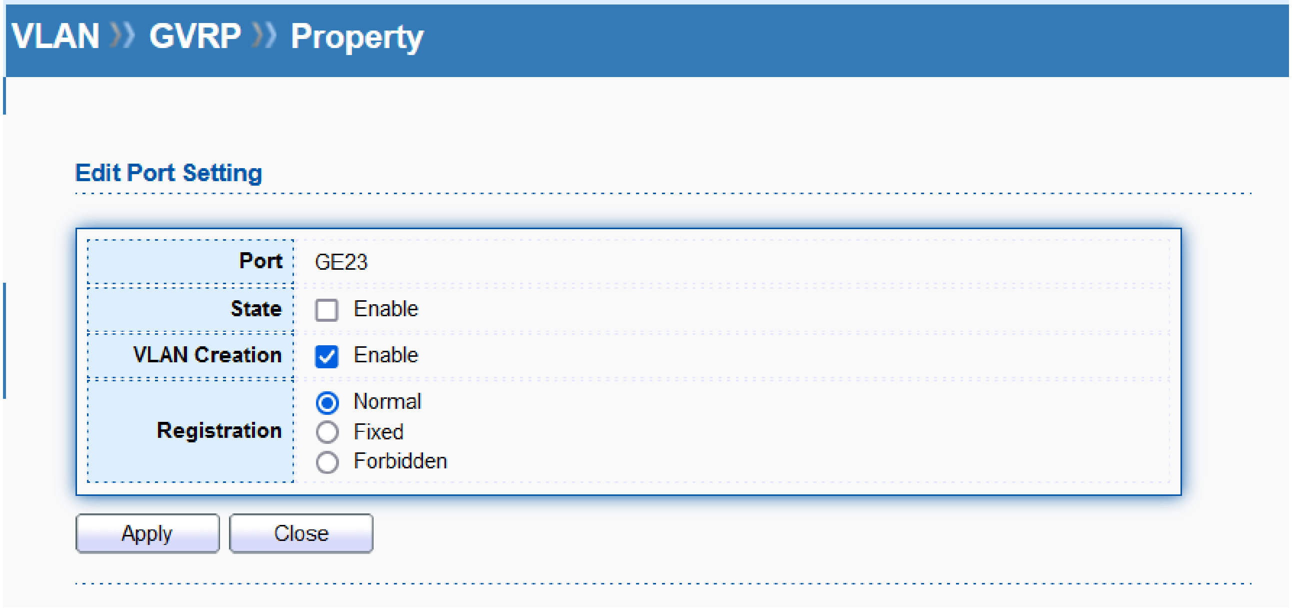
Leave 60 ms

LeaveAll 1000 ms

Port Setting Table

☐	Entry	Port	State	VLAN Creation	Registration
☐	1	GE1	Disabled	Enabled	Normal
☐	2	GE2	Disabled	Enabled	Normal
☐	3	GE3	Disabled	Enabled	Normal
☐	4	GE4	Disabled	Enabled	Normal
☐	5	GE5	Disabled	Enabled	Normal

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.



VLAN » GVRP » Property

Edit Port Setting

Port GE23

State ☐ Enable

VLAN Creation ☑ Enable

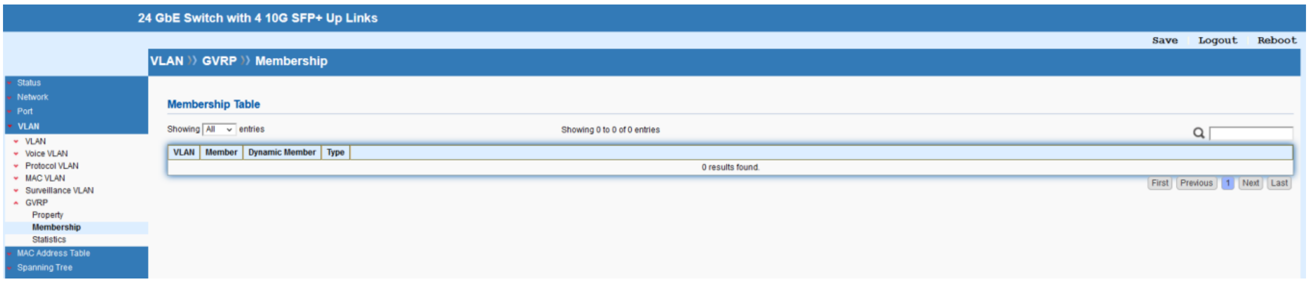
Registration ● Normal ○ Fixed ○ Forbidden

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.

6.6.2 Membership

This page displays information about membership of GVRP.



VLAN » GVRP » Membership

Membership Table

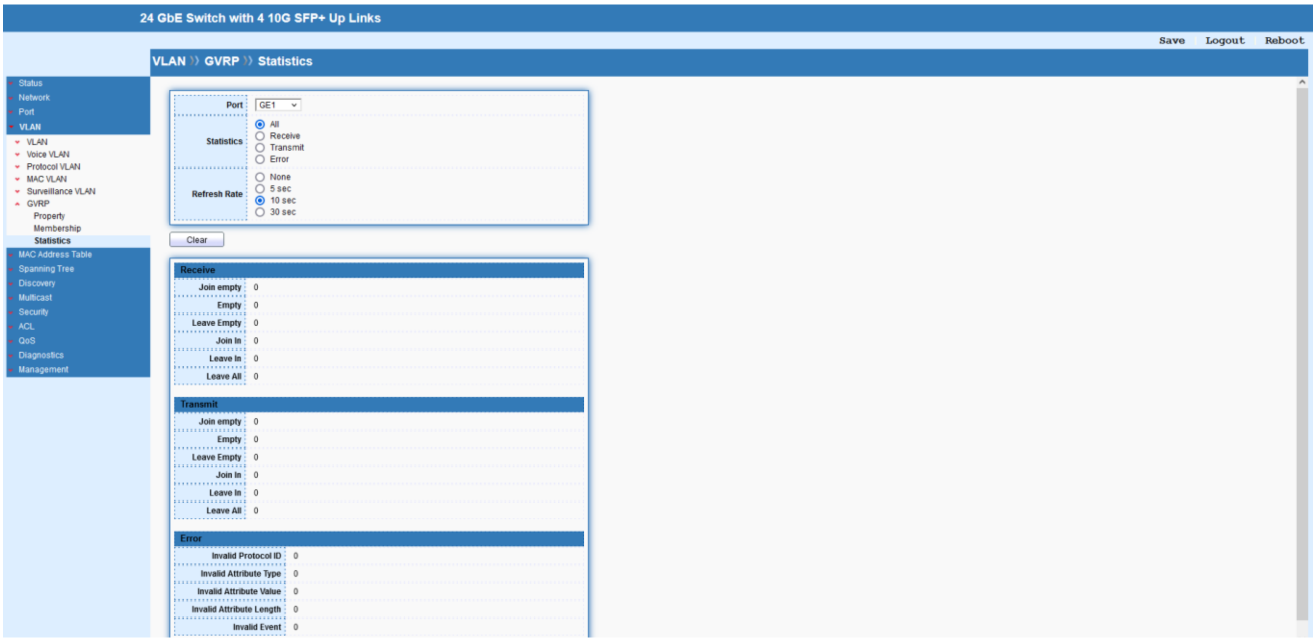
Showing All entries

Showing 0 to 0 of 0 entries

VLAN	Member	Dynamic Member	Type
0 results found.			

6.6.3 Statistics

This page displays detailed statistics of each port.



VLAN » GVRP » Statistics

Port: GE1

Statistics: ● All ○ Receive ○ Transmit ○ Error

Refresh Rate: ○ None ○ 5 sec ● 10 sec ○ 30 sec

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

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

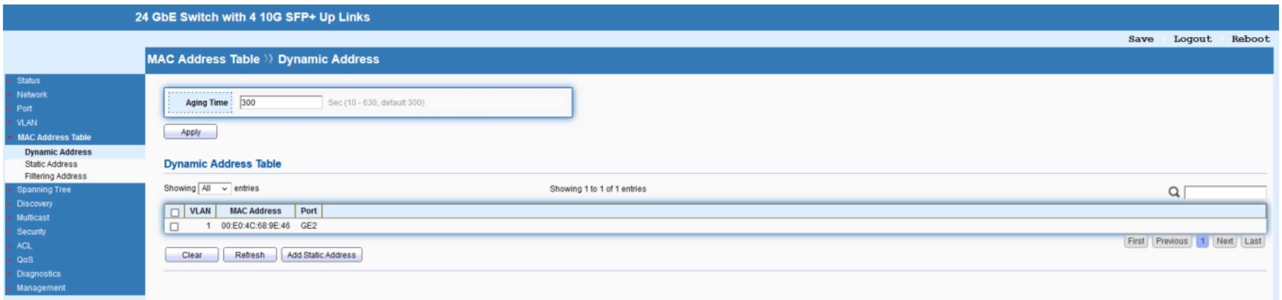
Error	
Invalid Protocol ID	0
Invalid Attribute Type	0
Invalid Attribute Value	0
Invalid Attribute Length	0
Invalid Event	0

7 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.

7.1 Dynamic Address

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



24 GbE Switch with 4 10G SFP+ Up Links

MAC Address Table ›› Dynamic Address

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

Dynamic Address Table

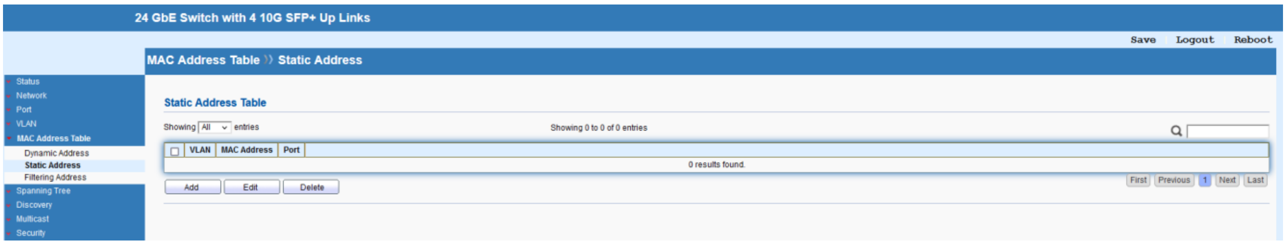
Showing All entries — Showing 1 to 1 of 1 entries

□	VLAN	MAC Address	Port
□	1	00:E0:4C:68:9E:46	GE2

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.

7.2 Static Address

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



24 GbE Switch with 4 10G SFP+ Up Links

MAC Address Table ›› Static Address

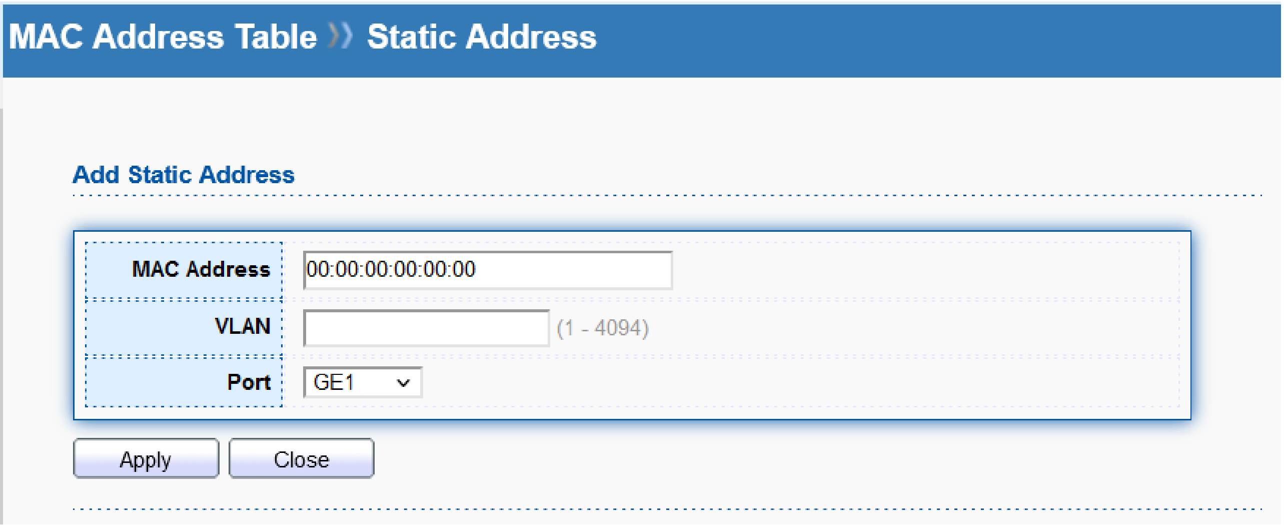
Static Address Table

Showing All entries — Showing 0 to 0 of 0 entries

□	VLAN	MAC Address	Port

0 results found.

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.

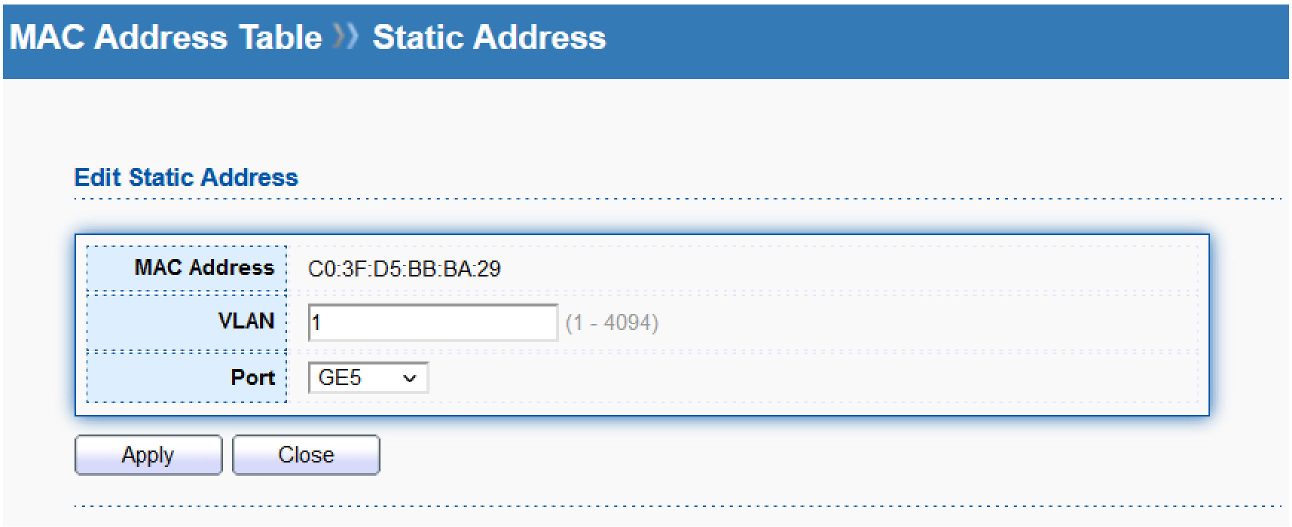


MAC Address Table ›› Static Address

Add Static Address

MAC Address	00:00:00:00:00:00
VLAN	(1 - 4094)
Port	GE1

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.



MAC Address Table ›› Static Address

Edit Static Address

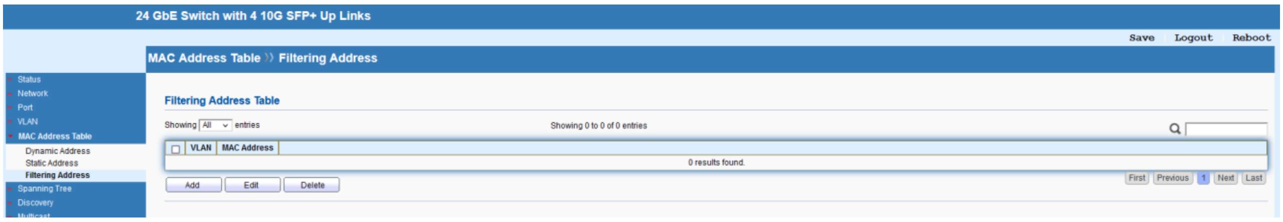
MAC Address	C0:3F:D5:BB:BA:29
VLAN	1 (1 - 4094)
Port	GE5

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.

7.3 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.



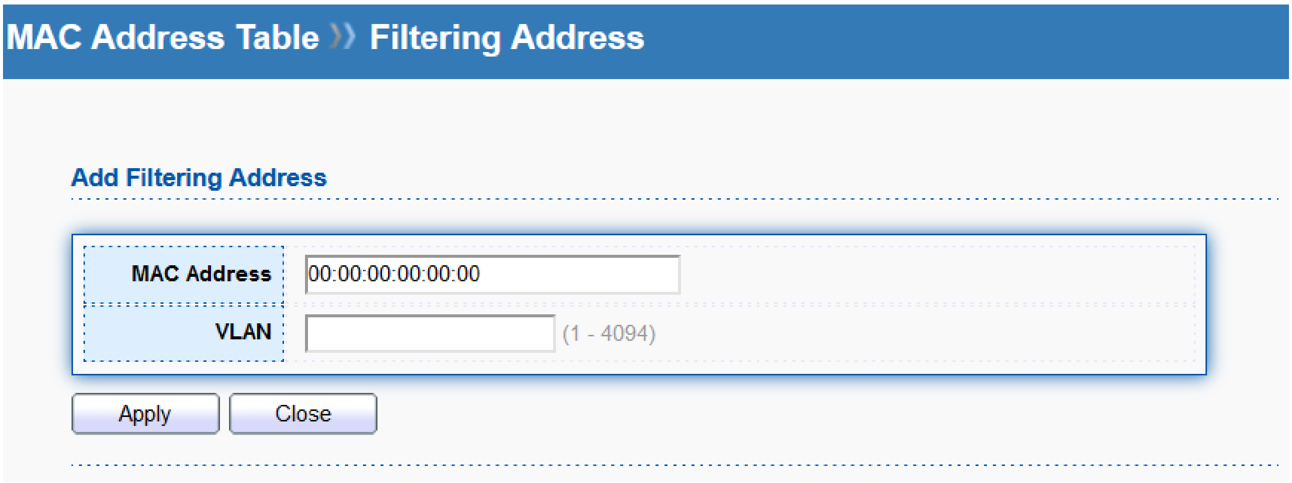
Showing All entries

Showing 0 to 0 of 0 entries

□	VLAN	MAC Address

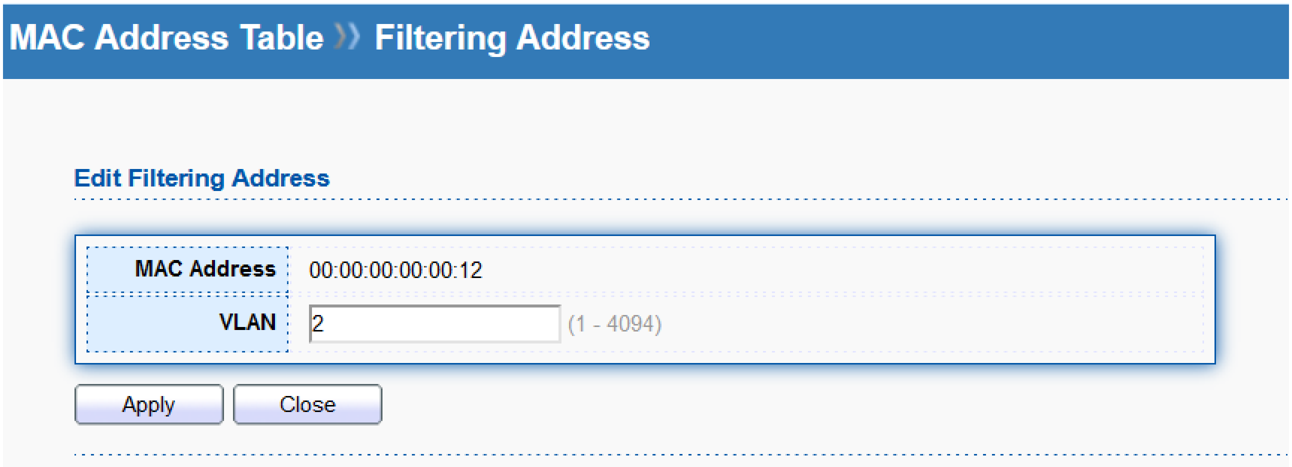
0 results found.

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.



MAC Address	00:00:00:00:00:00
VLAN	(1 - 4094)

Item	Description
MAC Address	Enter the MAC address that will be dropped.
VLAN	This is the VLAN group to which the MAC address belongs.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.



MAC Address Table » Filtering Address

Edit Filtering Address

MAC Address	00:00:00:00:00:12
VLAN	2 (1 - 4094)

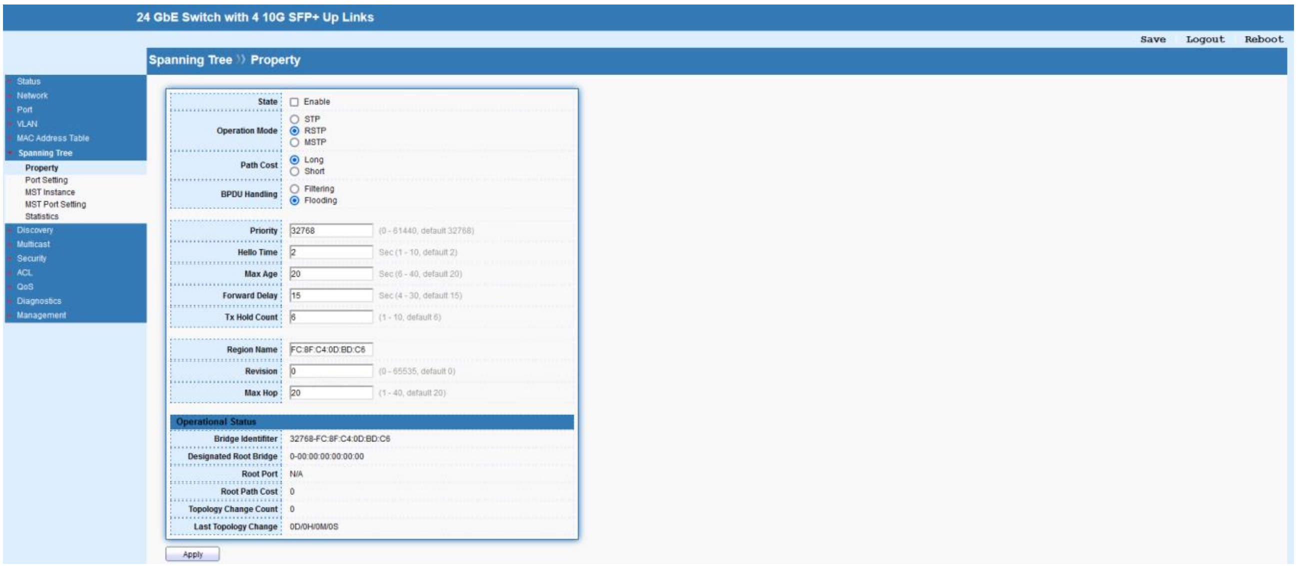
Item	Description
MAC Address	The MAC address that will be dropped.
VLAN	This is the VLAN group to which the MAC address belongs.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

8 Spanning Tree

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

8.1 Property

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



Spanning Tree » Property

State	□ Enable
Operation Mode	○ STP ● RSTP ○ MSTP
Path Cost	● Long ○ Short
BPDU Handling	○ Filtering ● Flooding
Priority	32768 (0 - 61440, default 32768)
Hello Time	2 Sec (1 - 10, default 2)
Max Age	20 Sec (6 - 40, default 20)
Forward Delay	15 Sec (4 - 30, default 15)
Tx Hold Count	6 (1 - 10, default 6)
Region Name	FC:8F:C4:0D:BD:C6
Revision	0 (0 - 65535, default 0)
Max Hop	20 (1 - 40, default 20)

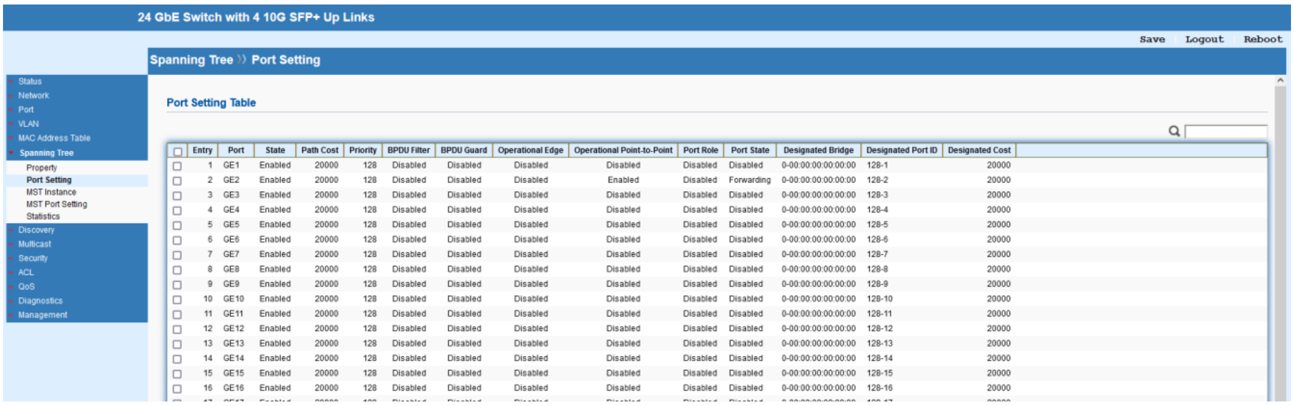
Operational Status

Bridge Identifier	32768-FC:8F:C4:0D:BD:C6
Designated Root Bridge	0-00:00:00:00:00:00
Root Port	N/A
Root Path Cost	0
Topology Change Count	0
Last Topology Change	0D/0H/0M/0S

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. **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.

8.2 Port Setting

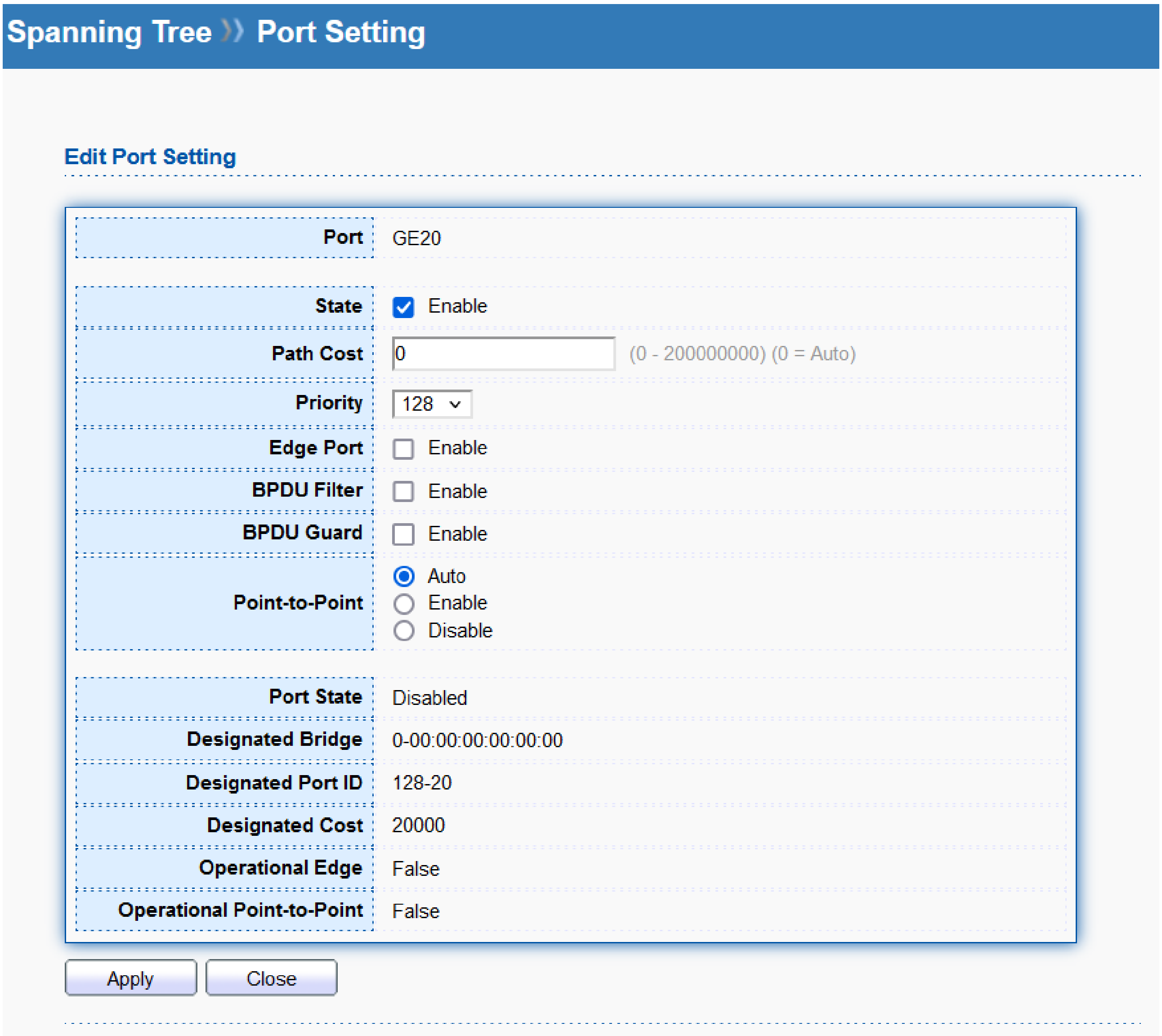
This page allows to configure and display Spanning Tree Protocol (STP) port settings.



Port Setting Table

□	Entry	Port	State	Path Cost	Priority	BPDU Filter	BPDU Guard	Operational Edge	Operational Point-to-Point	Port Role	Port State	Designated Bridge	Designated Port ID	Designated Cost
□	1	GE1	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-1	20000
□	2	GE2	Enabled	20000	128	Disabled	Disabled	Disabled	Enabled	Disabled	Forwarding	0-00:00:00:00:00:00	128-2	20000
□	3	GE3	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-3	20000
□	4	GE4	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-4	20000
□	5	GE5	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-5	20000
□	6	GE6	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-6	20000
□	7	GE7	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-7	20000
□	8	GE8	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-8	20000
□	9	GE9	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-9	20000
□	10	GE10	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-10	20000
□	11	GE11	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-11	20000
□	12	GE12	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-12	20000
□	13	GE13	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-13	20000
□	14	GE14	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-14	20000
□	15	GE15	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-15	20000
□	16	GE16	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-16	20000

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



Spanning Tree » Port Setting

Edit Port Setting

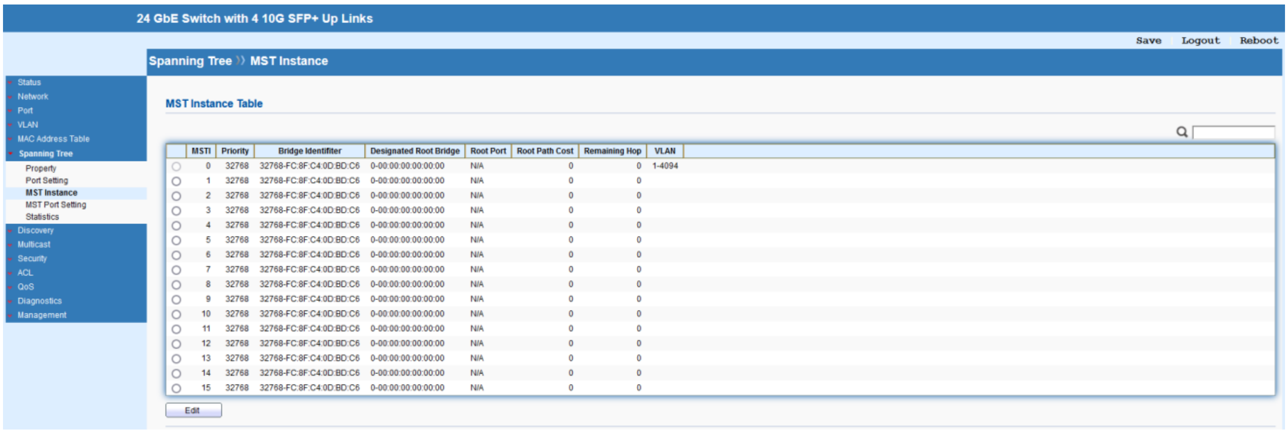
Port	GE20
State	☑ Enable
Path Cost	0 (0 - 200000000) (0 = Auto)
Priority	128
Edge Port	□ Enable
BPDU Filter	□ Enable
BPDU Guard	□ Enable
Point-to-Point	● Auto ○ Enable ○ Disable
Port State	Disabled
Designated Bridge	0-00:00:00:00:00:00
Designated Port ID	128-20
Designated Cost	20000
Operational Edge	False
Operational Point-to-Point	False

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.

8.3 MST Instance

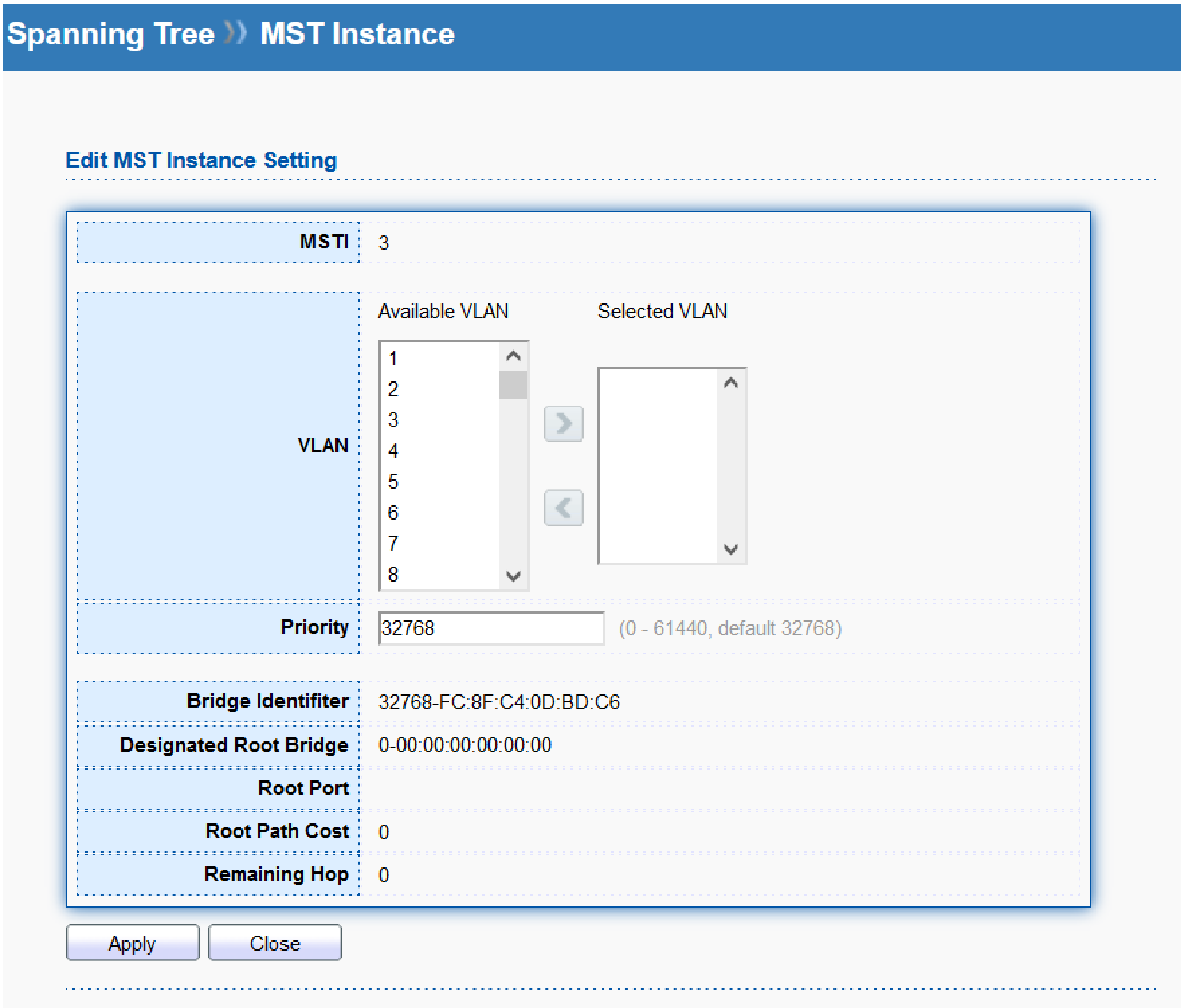
MSTP allows traffic of different VLAN to be mapped into different MST Instances, the 850X-28 supports up to 16 independent MST instances (0~15) with which the VLAN can be associated.



Spanning Tree ›› MST Instance

MST Instance Table

	MSTI	Priority	Bridge Identifiter	Designated Root Bridge	Root Port	Root Path Cost	Remaining Hop	VLAN
○	0	32768	32768-FC:8F:C4:0D:BD:C6	0-00:00:00:00:00:00	N/A	0	0	1-4094
○	1	32768	32768-FC:8F:C4:0D:BD:C6	0-00:00:00:00:00:00	N/A	0	0	
○	2	32768	32768-FC:8F:C4:0D:BD:C6	0-00:00:00:00:00:00	N/A	0	0	
○	3	32768	32768-FC:8F:C4:0D:BD:C6	0-00:00:00:00:00:00	N/A	0	0	
○	4	32768	32768-FC:8F:C4:0D:BD:C6	0-00:00:00:00:00:00	N/A	0	0	
○	5	32768	32768-FC:8F:C4:0D:BD:C6	0-00:00:00:00:00:00	N/A	0	0	
○	6	32768	32768-FC:8F:C4:0D:BD:C6	0-00:00:00:00:00:00	N/A	0	0	
○	7	32768	32768-FC:8F:C4:0D:BD:C6	0-00:00:00:00:00:00	N/A	0	0	
○	8	32768	32768-FC:8F:C4:0D:BD:C6	0-00:00:00:00:00:00	N/A	0	0	
○	9	32768	32768-FC:8F:C4:0D:BD:C6	0-00:00:00:00:00:00	N/A	0	0	
○	10	32768	32768-FC:8F:C4:0D:BD:C6	0-00:00:00:00:00:00	N/A	0	0	
○	11	32768	32768-FC:8F:C4:0D:BD:C6	0-00:00:00:00:00:00	N/A	0	0	
○	12	32768	32768-FC:8F:C4:0D:BD:C6	0-00:00:00:00:00:00	N/A	0	0	
○	13	32768	32768-FC:8F:C4:0D:BD:C6	0-00:00:00:00:00:00	N/A	0	0	
○	14	32768	32768-FC:8F:C4:0D:BD:C6	0-00:00:00:00:00:00	N/A	0	0	
○	15	32768	32768-FC:8F:C4:0D:BD:C6	0-00:00:00:00:00:00	N/A	0	0	



Spanning Tree ›› MST Instance

Edit MST Instance Setting

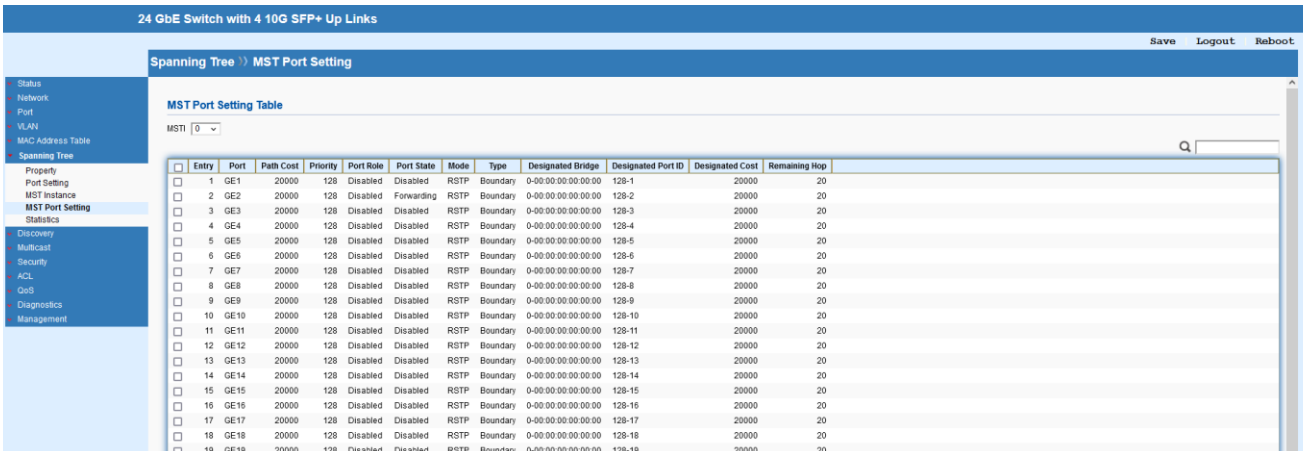
MSTI	3
VLAN	Available VLAN: 1, 2, 3, 4, 5, 6, 7, 8 Selected VLAN:
Priority	32768 (0 - 61440, default 32768)
Bridge Identifiter	32768-FC:8F:C4:0D:BD:C6
Designated Root Bridge	0-00:00:00:00:00:00
Root Port	
Root Path Cost	0
Remaining Hop	0

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.

8.4 MST Port Setting

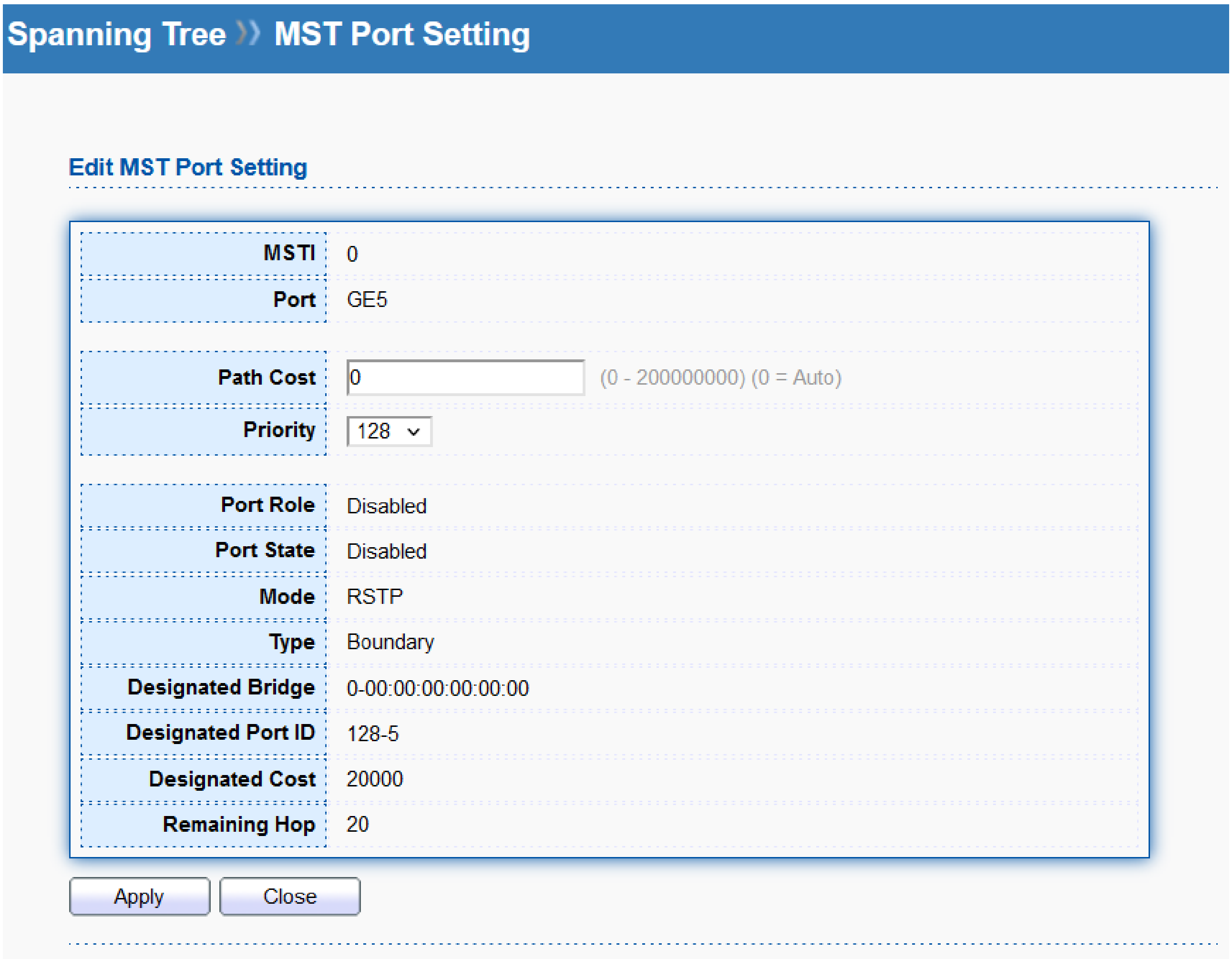
MST Port Settings is used to configure the GE port / LAG group settings for each MST instance. The table displays the MST parameters for each port.



MST Port Setting Table

MSTI 0

□	Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Type	Designated Bridge	Designated Port ID	Designated Cost	Remaining Hop
□	1	GE1	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-1	20000	20
□	2	GE2	20000	128	Disabled	Forwarding	RSTP	Boundary	0-00:00:00:00:00:00	128-2	20000	20
□	3	GE3	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-3	20000	20
□	4	GE4	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-4	20000	20
□	5	GE5	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-5	20000	20
□	6	GE6	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-6	20000	20
□	7	GE7	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-7	20000	20
□	8	GE8	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-8	20000	20
□	9	GE9	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-9	20000	20
□	10	GE10	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-10	20000	20
□	11	GE11	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-11	20000	20
□	12	GE12	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-12	20000	20
□	13	GE13	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-13	20000	20
□	14	GE14	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-14	20000	20
□	15	GE15	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-15	20000	20
□	16	GE16	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-16	20000	20
□	17	GE17	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-17	20000	20
□	18	GE18	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-18	20000	20
□	19	GE19	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-19	20000	20



Spanning Tree » MST Port Setting

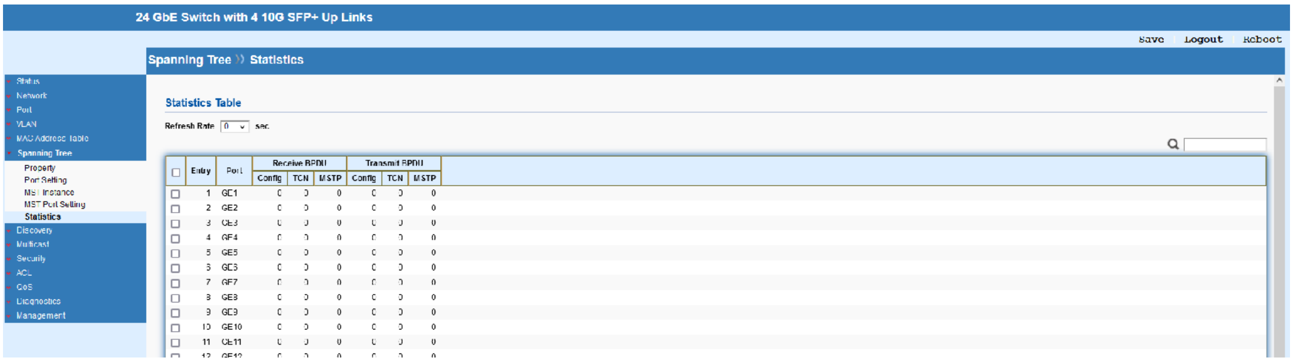
Edit MST Port Setting

MSTI	0
Port	GE5
Path Cost	0 (0 - 200000000) (0 = Auto)
Priority	128
Port Role	Disabled
Port State	Disabled
Mode	RSTP
Type	Boundary
Designated Bridge	0-00:00:00:00:00:00
Designated Port ID	128-5
Designated Cost	20000
Remaining Hop	20

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.

8.5 Statistics

This page displays the statistics of BPDU on each port.



Statistics Table

Refresh Rate 0 sec

□	Entry	Port	Receive BPDU			Transmit BPDU		
			Config	TCN	MSTP	Config	TCN	MSTP
□	1	GE1	0	0	0	0	0	0
□	2	GE2	0	0	0	0	0	0
□	3	GE3	0	0	0	0	0	0
□	4	GE4	0	0	0	0	0	0
□	5	GE5	0	0	0	0	0	0
□	6	GE6	0	0	0	0	0	0
□	7	GE7	0	0	0	0	0	0
□	8	GE8	0	0	0	0	0	0
□	9	GE9	0	0	0	0	0	0
□	10	GE10	0	0	0	0	0	0
□	11	GE11	0	0	0	0	0	0
□	12	GE12	0	0	0	0	0	0

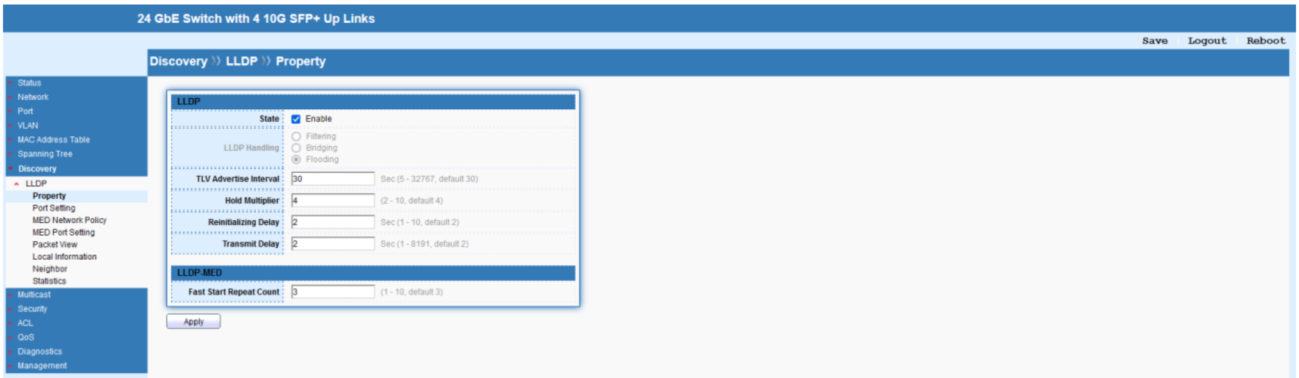
9 Discovery

9.1 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.

9.1.1 Property

This page allows to configure general settings of LLDP.



LLDP

State ☑ Enable

LLDP Handling ○ Filtering ○ Bridging ● Flooding

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

Hold Multiplier 4 (2 - 10, default 4)

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

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

LLDP-MED

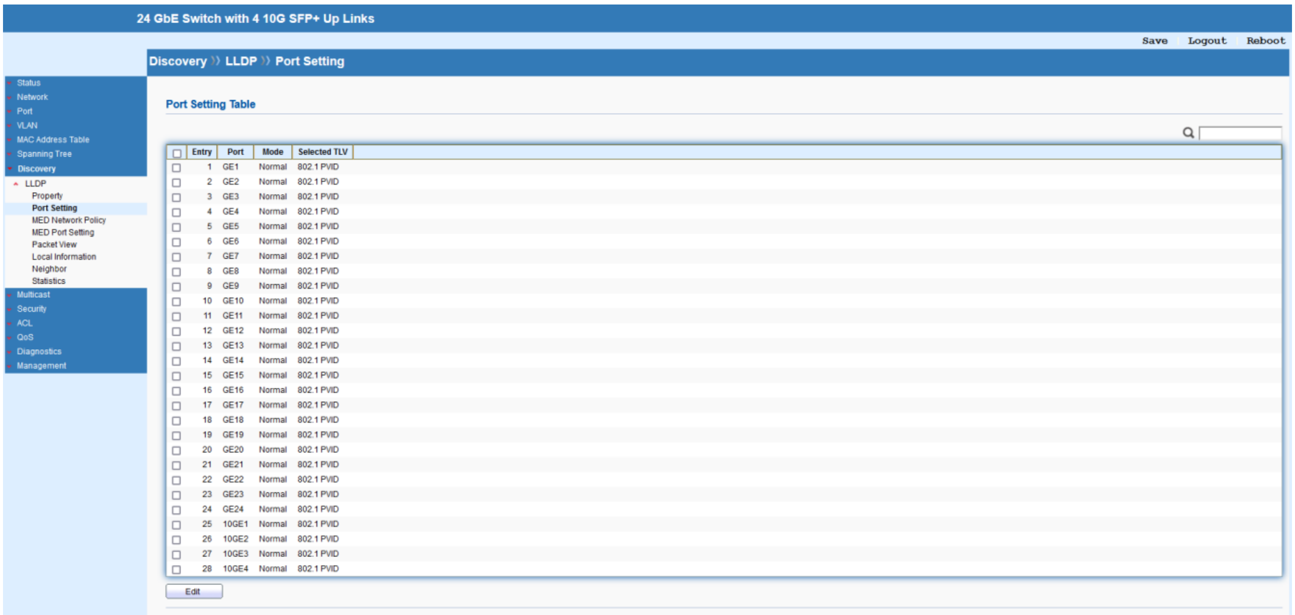
Fast Start Repeat Count 3 (1 - 10, default 3)

Item	Description
State	Enable or disable the LLDP protocol on this switch.
LLDP Handling	Select the handling mode for LLDP protocol.
TLV Advertise Interval	Select the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 5–32768seconds.
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.

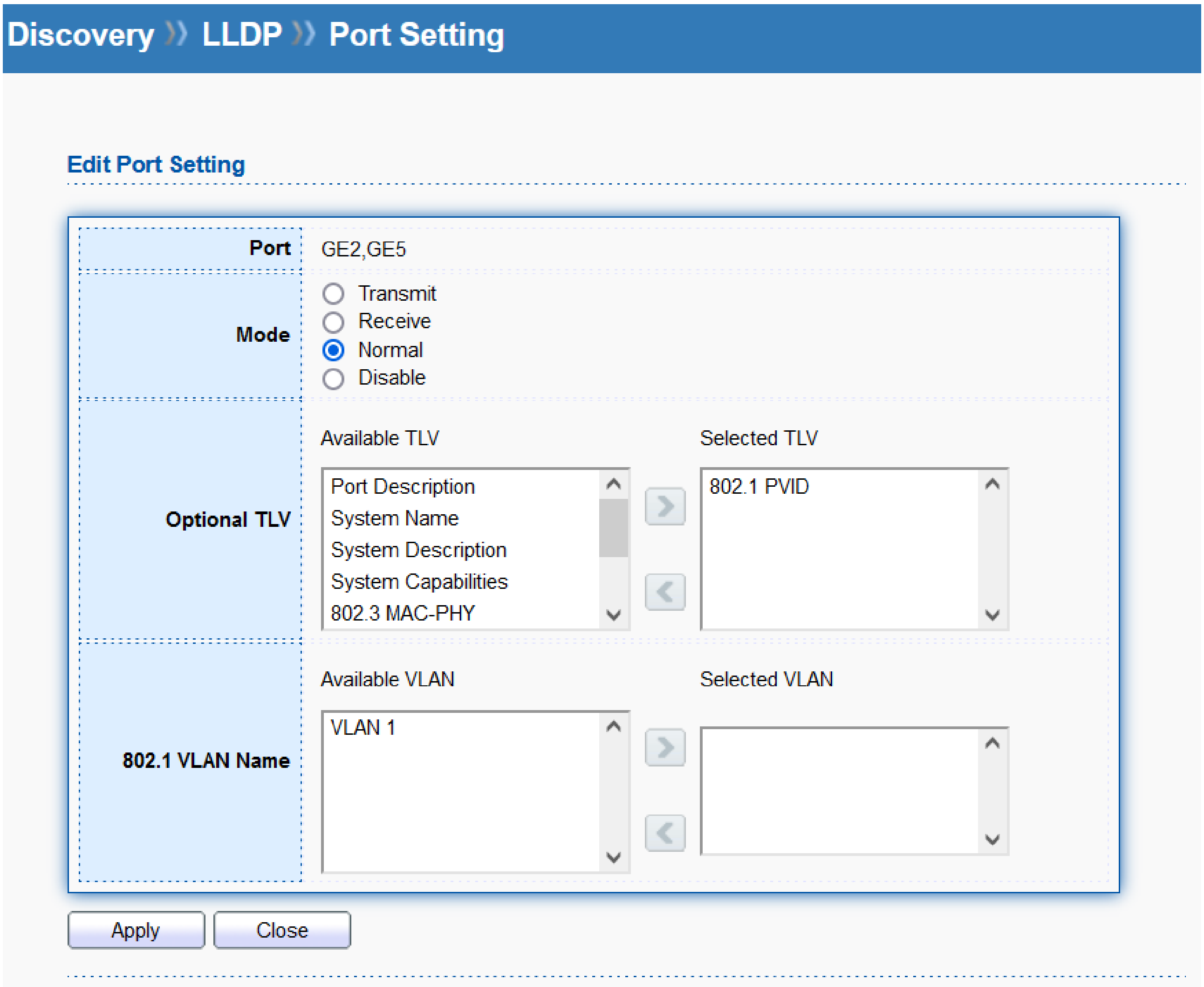
9.1.2 Port Setting

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



Port Setting Table

□	Entry	Port	Mode	Selected TLV
□	1	GE1	Normal	802.1 PVID
□	2	GE2	Normal	802.1 PVID
□	3	GE3	Normal	802.1 PVID
□	4	GE4	Normal	802.1 PVID
□	5	GE5	Normal	802.1 PVID
□	6	GE6	Normal	802.1 PVID
□	7	GE7	Normal	802.1 PVID
□	8	GE8	Normal	802.1 PVID
□	9	GE9	Normal	802.1 PVID
□	10	GE10	Normal	802.1 PVID
□	11	GE11	Normal	802.1 PVID
□	12	GE12	Normal	802.1 PVID
□	13	GE13	Normal	802.1 PVID
□	14	GE14	Normal	802.1 PVID
□	15	GE15	Normal	802.1 PVID
□	16	GE16	Normal	802.1 PVID
□	17	GE17	Normal	802.1 PVID
□	18	GE18	Normal	802.1 PVID
□	19	GE19	Normal	802.1 PVID
□	20	GE20	Normal	802.1 PVID
□	21	GE21	Normal	802.1 PVID
□	22	GE22	Normal	802.1 PVID
□	23	GE23	Normal	802.1 PVID
□	24	GE24	Normal	802.1 PVID
□	25	10GE1	Normal	802.1 PVID
□	26	10GE2	Normal	802.1 PVID
□	27	10GE3	Normal	802.1 PVID
□	28	10GE4	Normal	802.1 PVID


Discovery » LLDP » Port Setting

Edit Port Setting

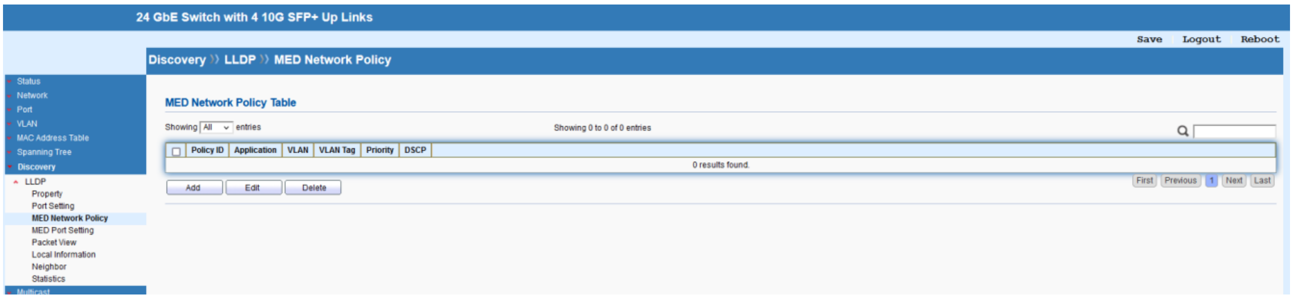
Port	GE2,GE5
Mode	○ Transmit ○ Receive ● Normal ○ Disable
Optional TLV	Available TLV: Port Description, System Name, System Description, System Capabilities, 802.3 MAC-PHY Selected TLV: 802.1 PVID
802.1 VLAN Name	Available VLAN: VLAN 1 Selected VLAN:

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.

9.1.3 MED Network Policy

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



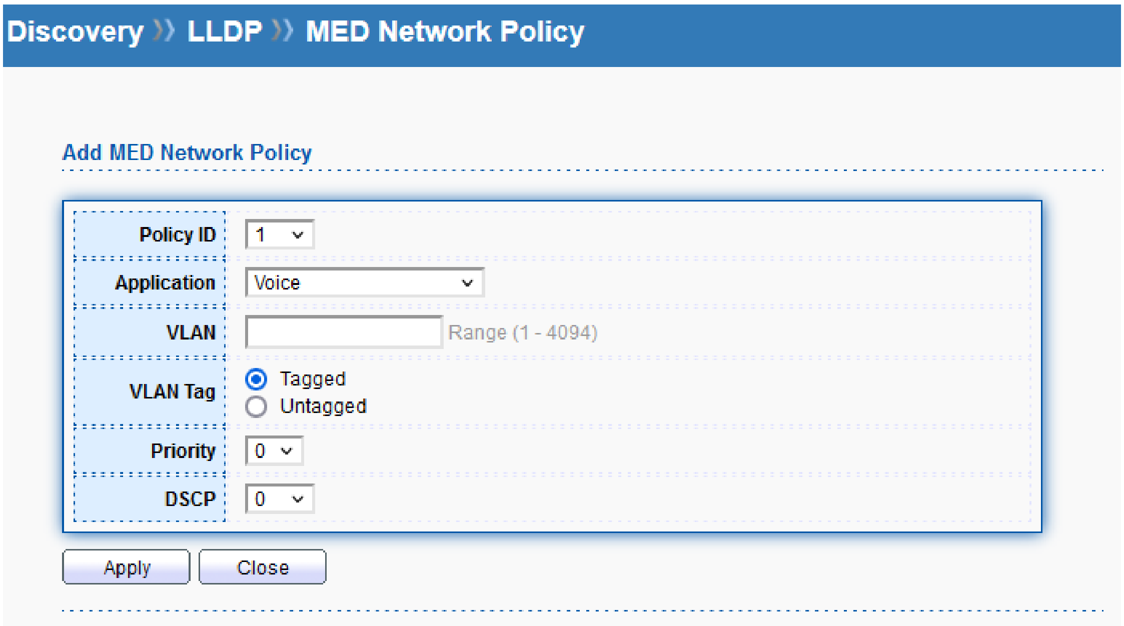
Discovery » LLDP » MED Network Policy

MED Network Policy Table

Showing All entries   Showing 0 to 0 of 0 entries

□	Policy ID	Application	VLAN	VLAN Tag	Priority	DSCP
0 results found.						

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.



Discovery » LLDP » MED Network Policy

Add MED Network Policy

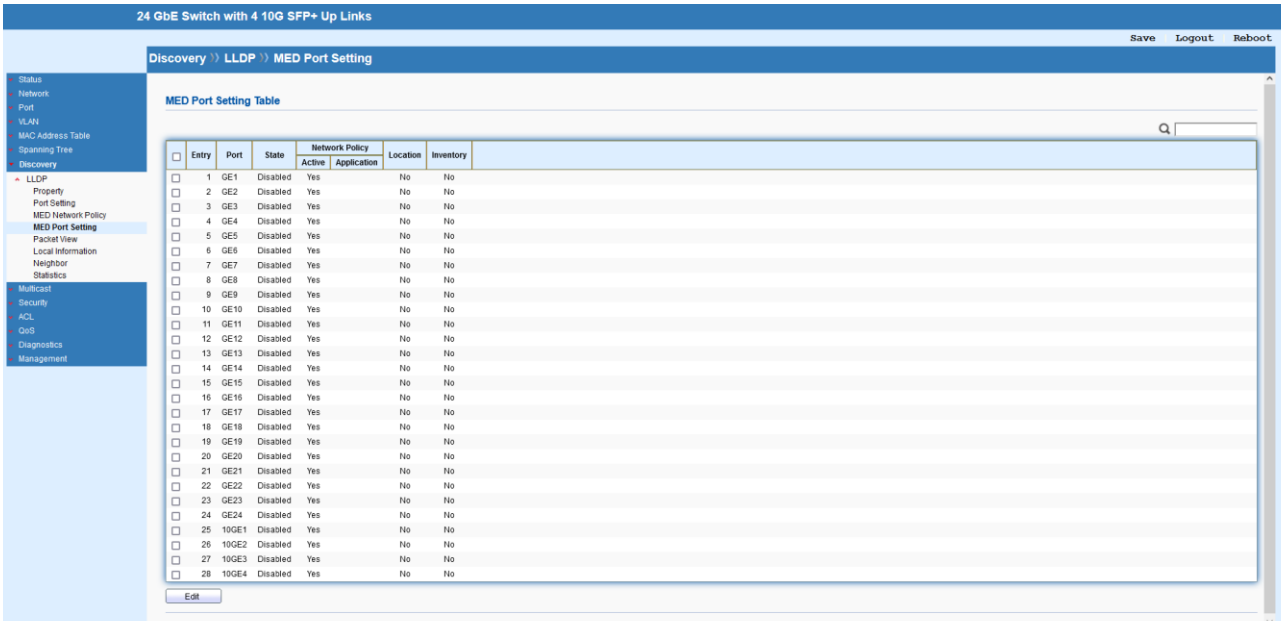
Policy ID	1
Application	Voice
VLAN	Range (1 - 4094)
VLAN Tag	● Tagged ○ Untagged
Priority	0
DSCP	0

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.

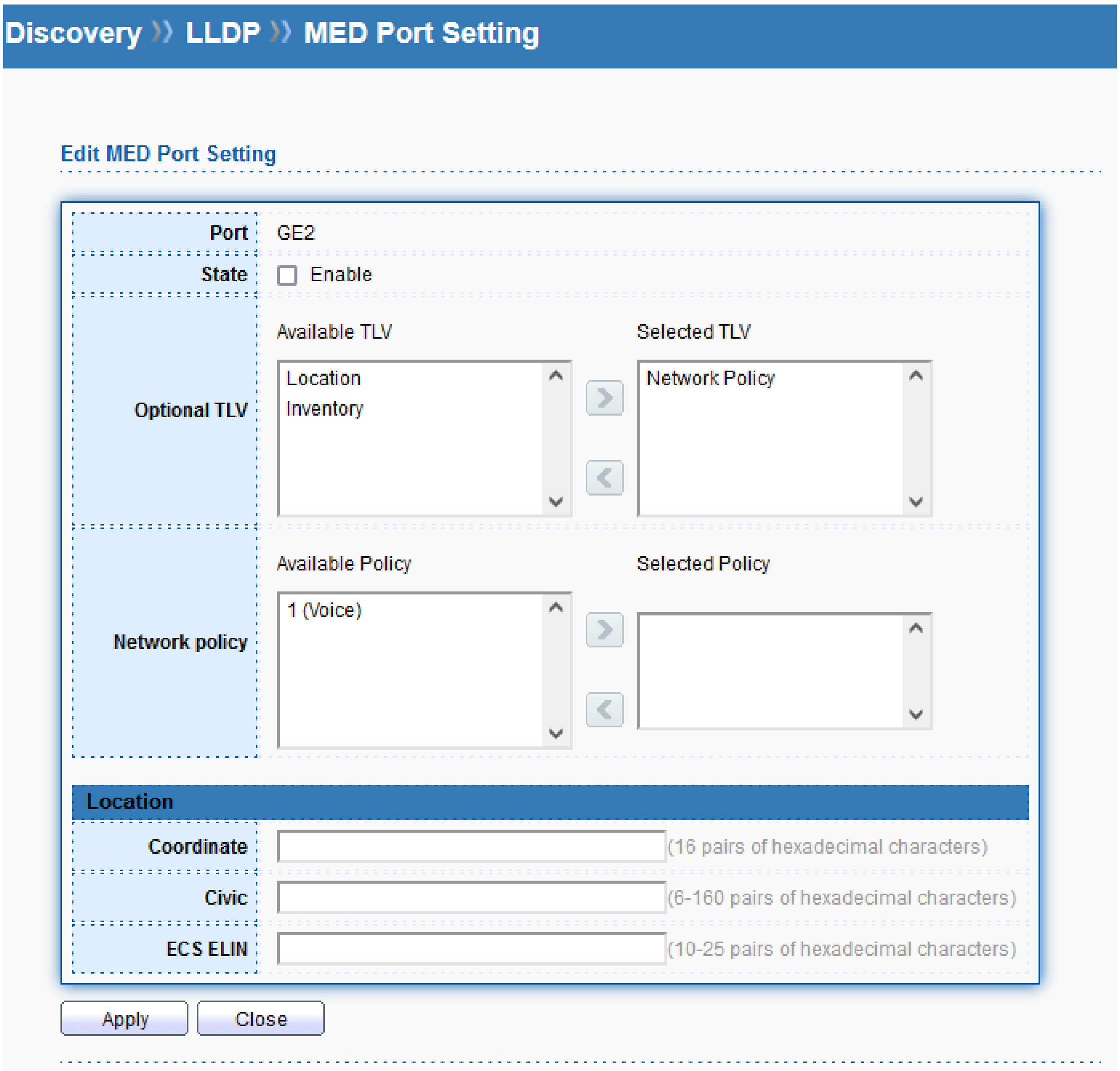
9.1.4 MED Port Setting

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



MED Port Setting Table

□	Entry	Port	State	Network Policy		Location	Inventory
				Active	Application		
□	1	GE1	Disabled	Yes		No	No
□	2	GE2	Disabled	Yes		No	No
□	3	GE3	Disabled	Yes		No	No
□	4	GE4	Disabled	Yes		No	No
□	5	GE5	Disabled	Yes		No	No
□	6	GE6	Disabled	Yes		No	No
□	7	GE7	Disabled	Yes		No	No
□	8	GE8	Disabled	Yes		No	No
□	9	GE9	Disabled	Yes		No	No
□	10	GE10	Disabled	Yes		No	No
□	11	GE11	Disabled	Yes		No	No
□	12	GE12	Disabled	Yes		No	No
□	13	GE13	Disabled	Yes		No	No
□	14	GE14	Disabled	Yes		No	No
□	15	GE15	Disabled	Yes		No	No
□	16	GE16	Disabled	Yes		No	No
□	17	GE17	Disabled	Yes		No	No
□	18	GE18	Disabled	Yes		No	No
□	19	GE19	Disabled	Yes		No	No
□	20	GE20	Disabled	Yes		No	No
□	21	GE21	Disabled	Yes		No	No
□	22	GE22	Disabled	Yes		No	No
□	23	GE23	Disabled	Yes		No	No
□	24	GE24	Disabled	Yes		No	No
□	25	10GE1	Disabled	Yes		No	No
□	26	10GE2	Disabled	Yes		No	No
□	27	10GE3	Disabled	Yes		No	No
□	28	10GE4	Disabled	Yes		No	No



Discovery » LLDP » MED Port Setting

Edit MED Port Setting

Port	GE2
State	□ Enable
Optional TLV	Available TLV: Location Inventory Selected TLV: Network Policy
Network policy	Available Policy: 1 (Voice) Selected Policy:

Location

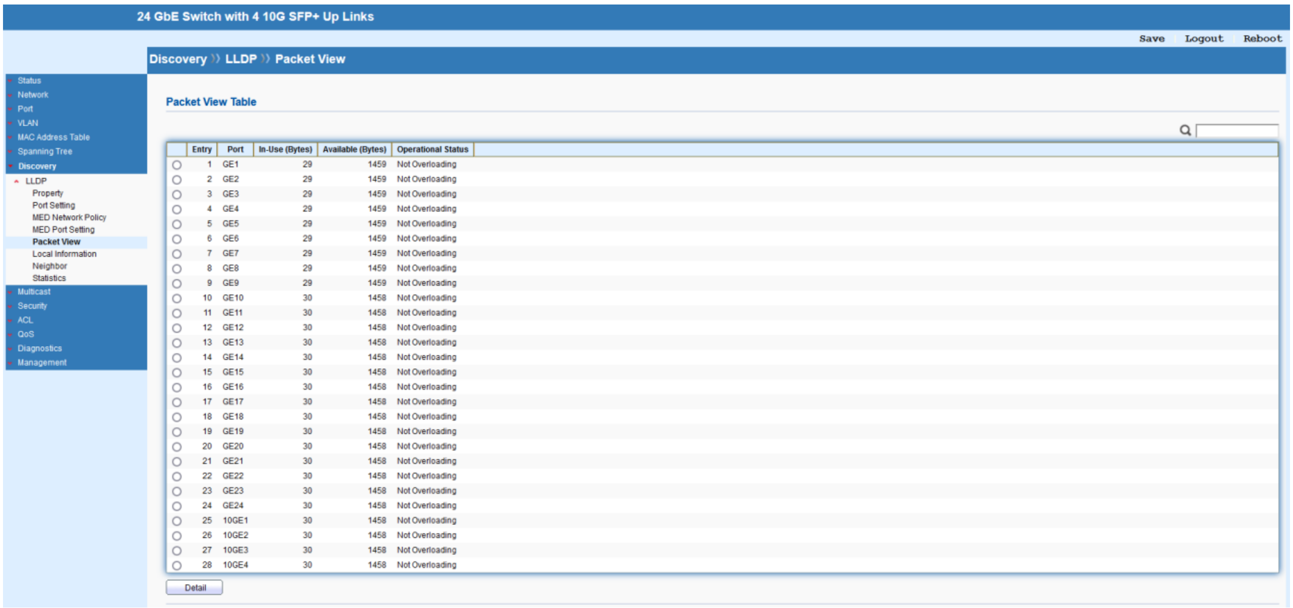
Coordinate		(16 pairs of hexadecimal characters)
Civic		(6-160 pairs of hexadecimal characters)
ECS ELIN		(10-25 pairs of hexadecimal characters)

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.

9.1.5 Packet View

This page provides packet view detail of each port.

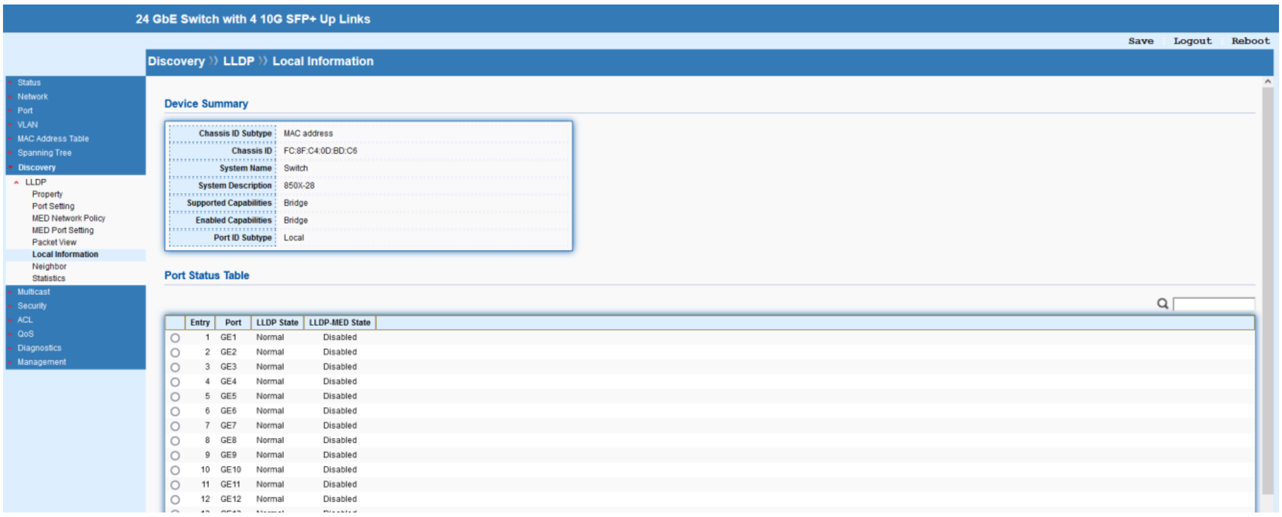


Packet View Table

	Entry	Port	In-Use (Bytes)	Available (Bytes)	Operational Status
○	1	GE1	29	1459	Not Overloading
○	2	GE2	29	1459	Not Overloading
○	3	GE3	29	1459	Not Overloading
○	4	GE4	29	1459	Not Overloading
○	5	GE5	29	1459	Not Overloading
○	6	GE6	29	1459	Not Overloading
○	7	GE7	29	1459	Not Overloading
○	8	GE8	29	1459	Not Overloading
○	9	GE9	29	1459	Not Overloading
○	10	GE10	30	1458	Not Overloading
○	11	GE11	30	1458	Not Overloading
○	12	GE12	30	1458	Not Overloading
○	13	GE13	30	1458	Not Overloading
○	14	GE14	30	1458	Not Overloading
○	15	GE15	30	1458	Not Overloading
○	16	GE16	30	1458	Not Overloading
○	17	GE17	30	1458	Not Overloading
○	18	GE18	30	1458	Not Overloading
○	19	GE19	30	1458	Not Overloading
○	20	GE20	30	1458	Not Overloading
○	21	GE21	30	1458	Not Overloading
○	22	GE22	30	1458	Not Overloading
○	23	GE23	30	1458	Not Overloading
○	24	GE24	30	1458	Not Overloading
○	25	10GE1	30	1458	Not Overloading
○	26	10GE2	30	1458	Not Overloading
○	27	10GE3	30	1458	Not Overloading
○	28	10GE4	30	1458	Not Overloading

9.1.6 Local Information

This page shows detailed local information of LLDP.



Device Summary

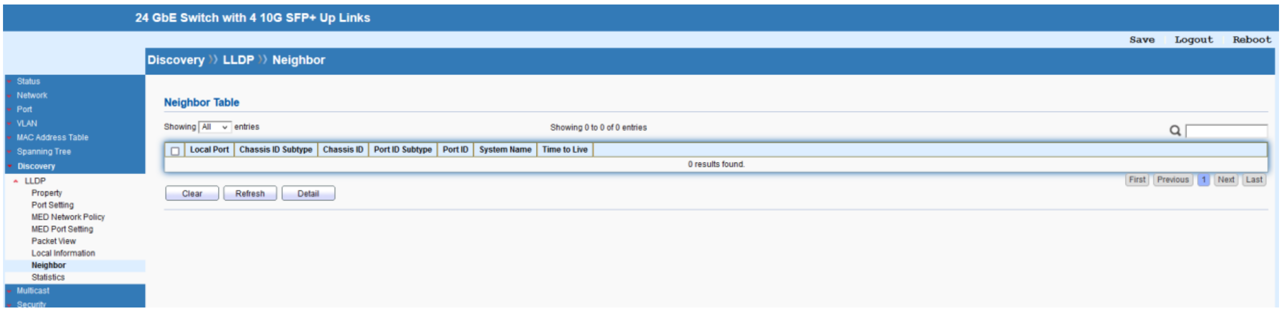
Chassis ID Subtype	MAC address
Chassis ID	FC:8F:C4:0D:BD:C6
System Name	Switch
System Description	850X-28
Supported Capabilities	Bridge
Enabled Capabilities	Bridge
Port ID Subtype	Local

Port Status Table

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

9.1.7 Neighbor

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



Neighbor Table

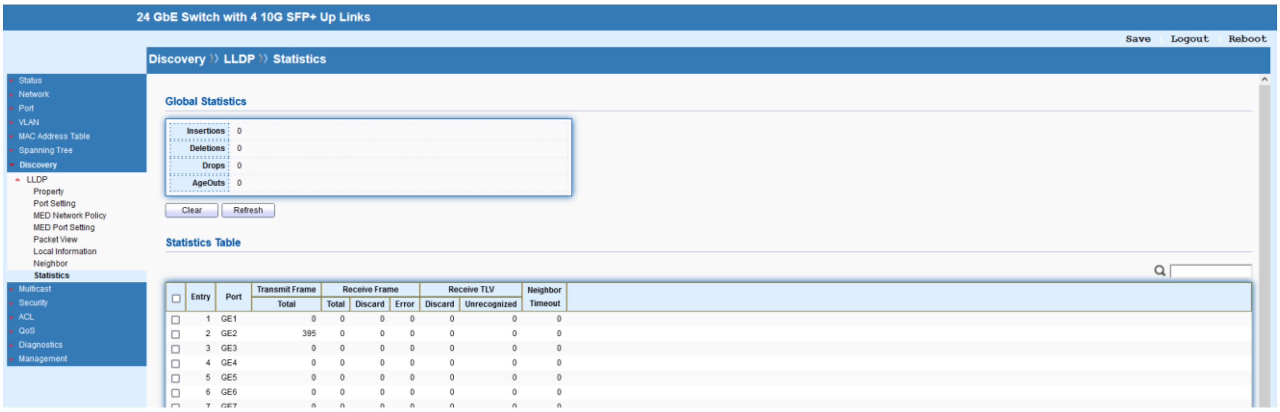
Showing All entries

Showing 0 to 0 of 0 entries

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

9.1.8 Statistics

This page shows global statistics and statistics of each port.



Global Statistics

Insertions	0
Deletions	0
Drops	0
AgeOuts	0

Statistics Table

□	Entry	Port	Transmit Frame	Receive Frame			Receive TLV		Neighbor
			Total	Total	Discard	Error	Discard	Unrecognized	Timeout
□	1	GE1	0	0	0	0	0	0	0
□	2	GE2	395	0	0	0	0	0	0
□	3	GE3	0	0	0	0	0	0	0
□	4	GE4	0	0	0	0	0	0	0
□	5	GE5	0	0	0	0	0	0	0
□	6	GE6	0	0	0	0	0	0	0
□	7	GE7	0	0	0	0	0	0	0

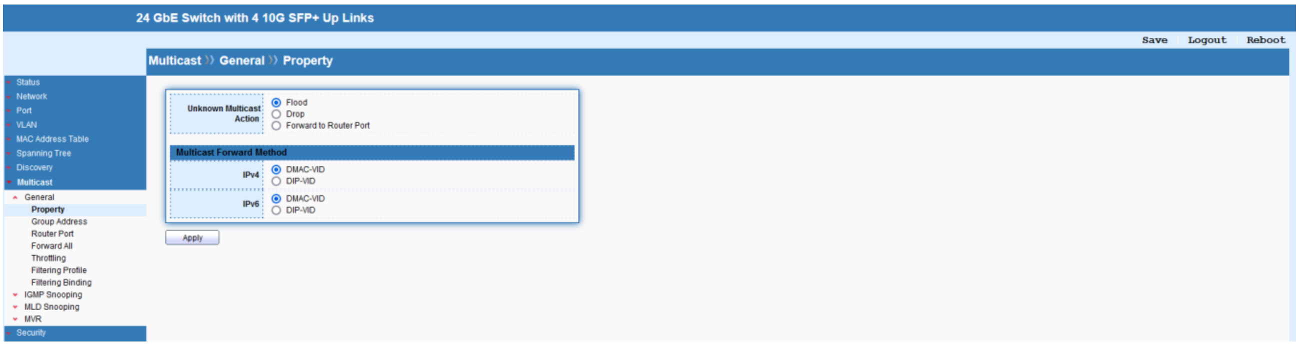
10 Multicast

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).

10.1 General

10.1.1 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.



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

Multicast Forward Method

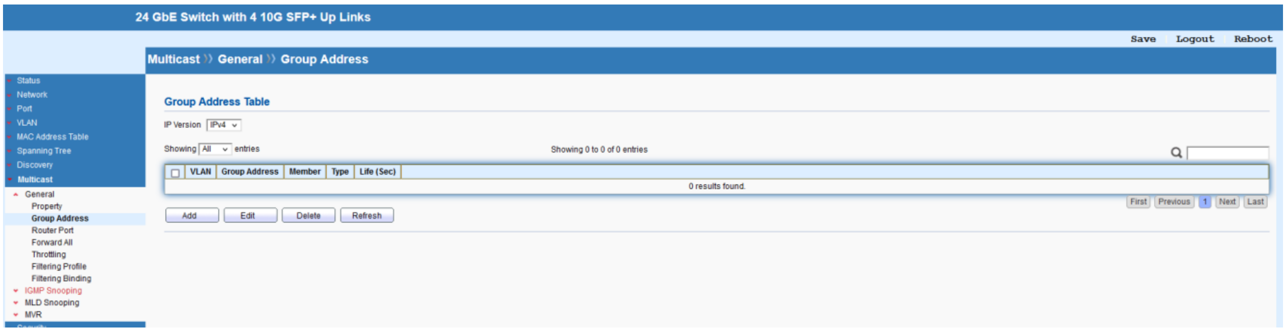
IPv4: ● DMAC-VID ○ DIP-VID

IPv6: ● DMAC-VID ○ DIP-VID

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.

10.1.2 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.



Group Address Table

IP Version: IPv4

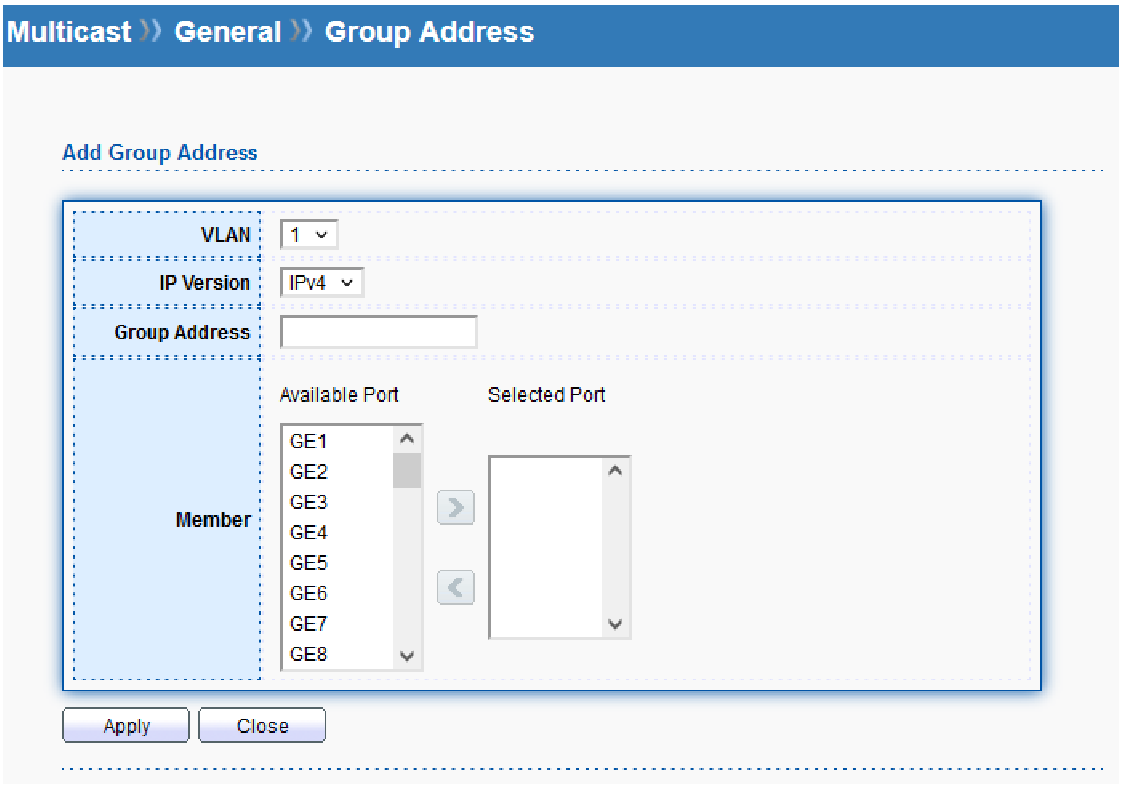
Showing All entries

Showing 0 to 0 of 0 entries

□	VLAN	Group Address	Member	Type	Life (Sec)

0 results found.

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.



Add Group Address

VLAN: 1

IP Version: IPv4

Group Address:

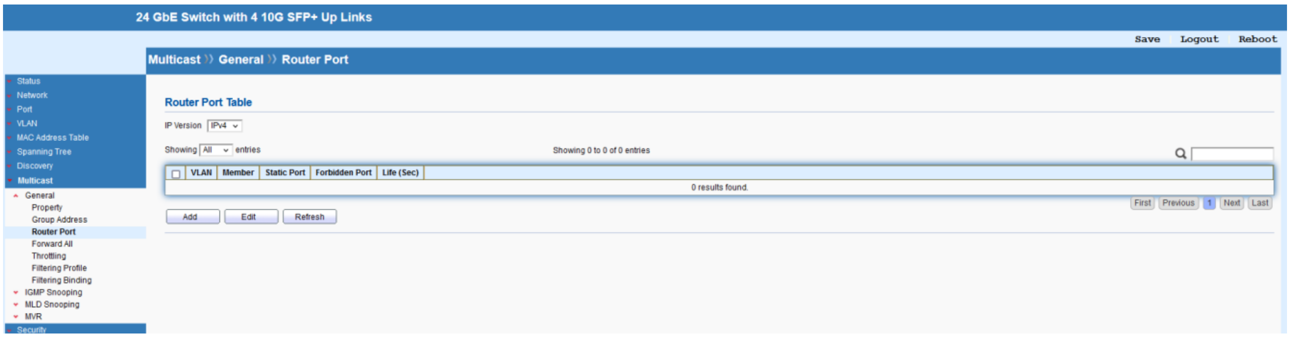
Member

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.

10.1.3 Router Port

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



Router Port Table

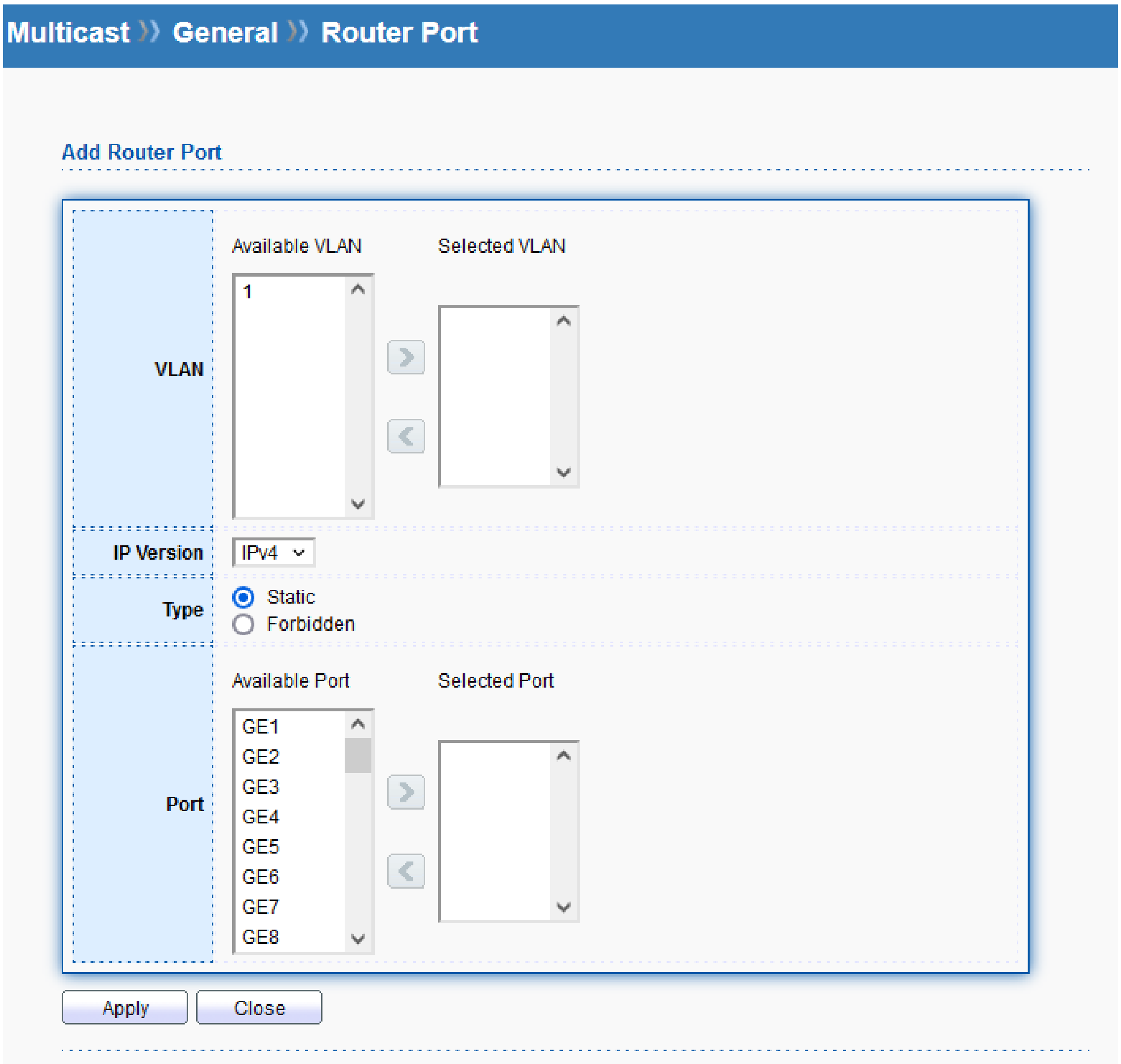
IP Version IPv4

Showing All entries

Showing 0 to 0 of 0 entries

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

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.


Multicast >> General >> Router Port

Add Router Port

VLAN

Available VLAN

1

Selected VLAN

IP Version: IPv4

Type: ● Static ○ Forbidden

Port

Available Port

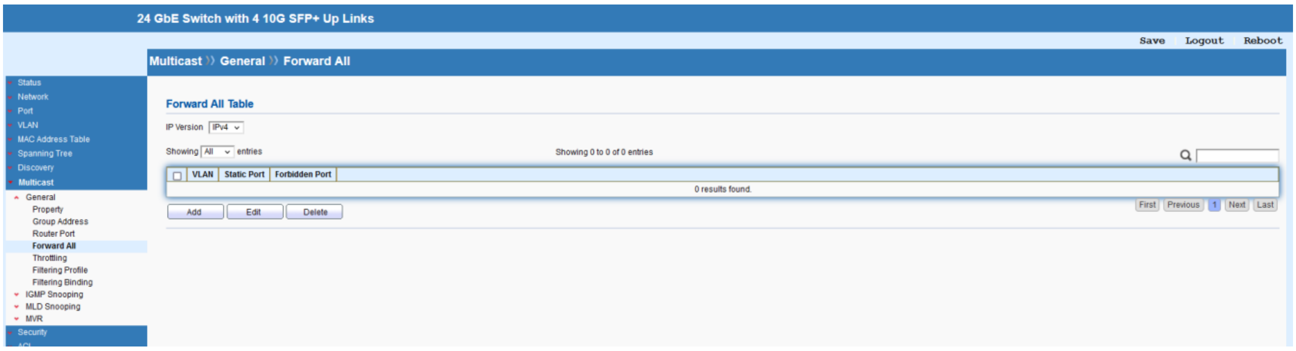
GE1
GE2
GE3
GE4
GE5
GE6
GE7
GE8

Selected Port

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.

10.1.4 Forward All

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



Forward All Table

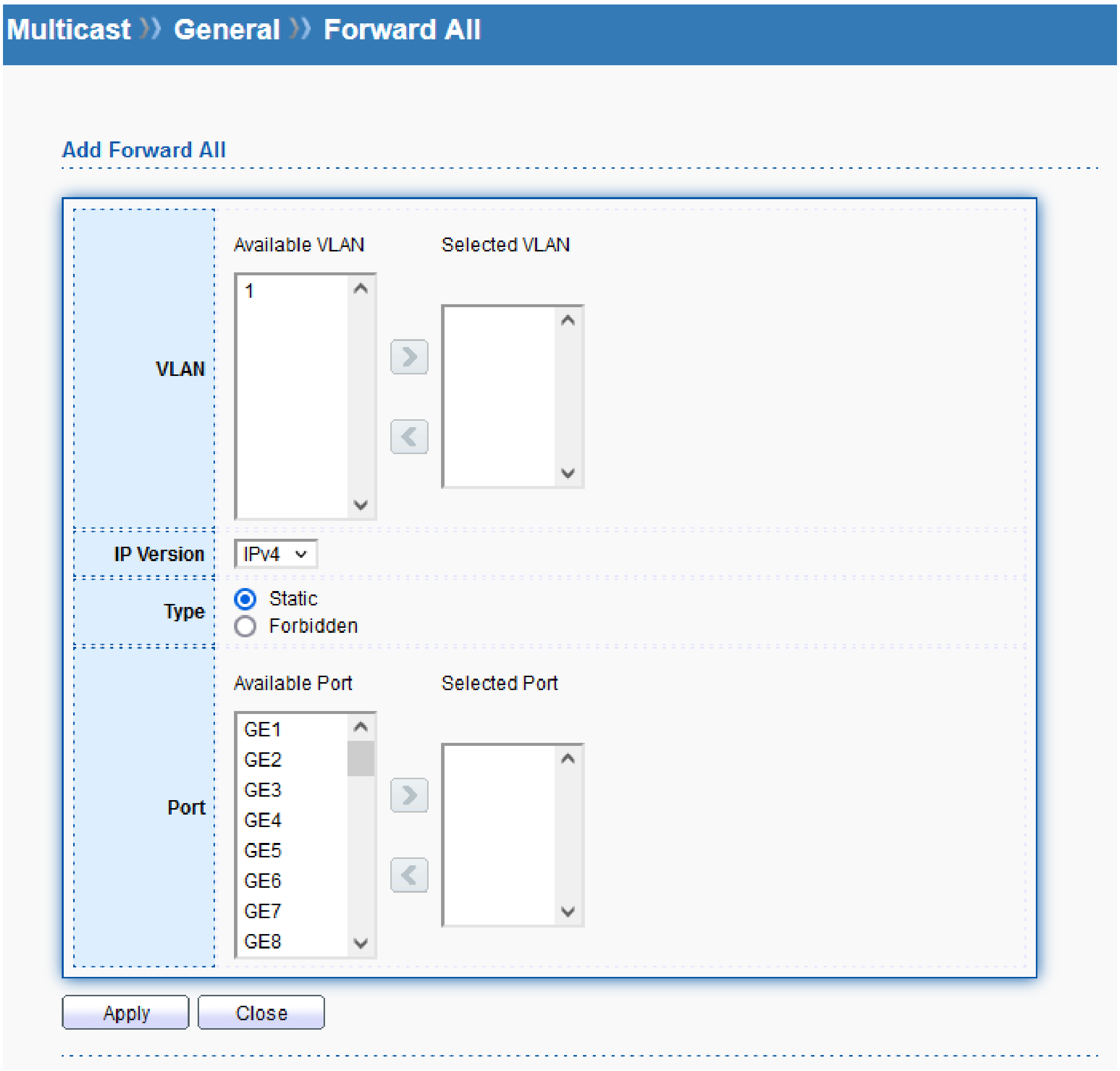
IP Version IPv4

Showing All entries

Showing 0 to 0 of 0 entries

□	VLAN	Static Port	Forbidden Port
0 results found.			

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.


Multicast » General » Forward All

Add Forward All

VLAN: Available VLAN: 1 — Selected VLAN:

IP Version: IPv4

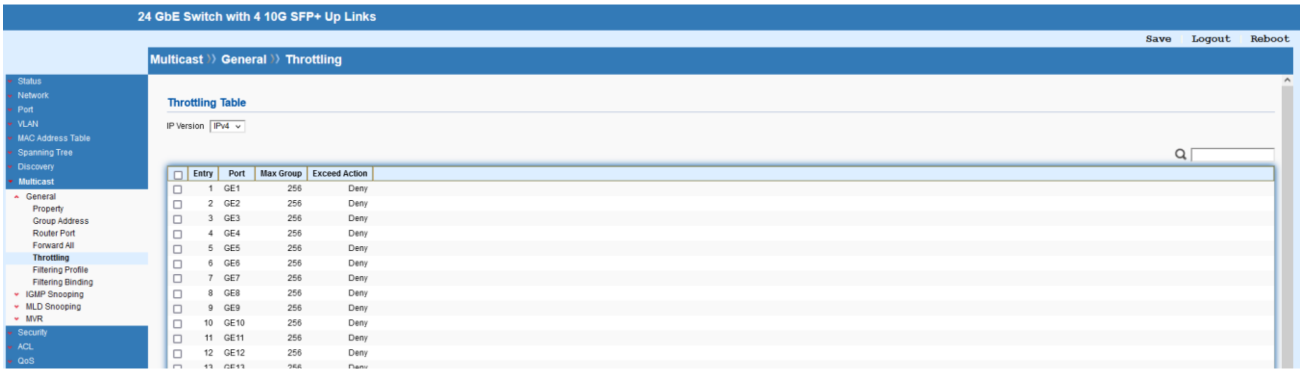
Type: ● Static ○ Forbidden

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

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.

10.1.5 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.

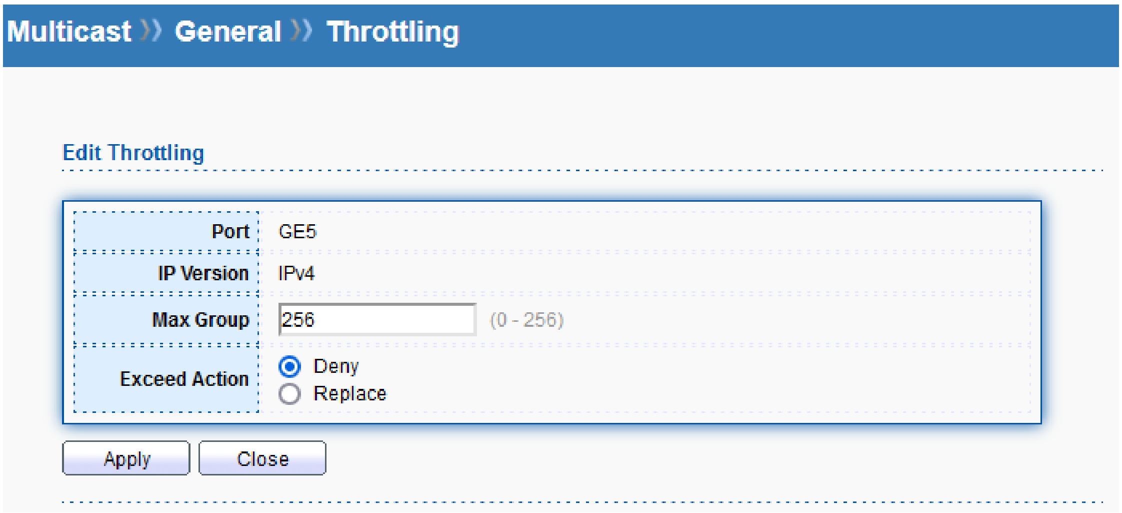


Throttling Table

IP Version IPv4

□	Entry	Port	Max Group	Exceed Action
□	1	GE1	256	Deny
□	2	GE2	256	Deny
□	3	GE3	256	Deny
□	4	GE4	256	Deny
□	5	GE5	256	Deny
□	6	GE6	256	Deny
□	7	GE7	256	Deny
□	8	GE8	256	Deny
□	9	GE9	256	Deny
□	10	GE10	256	Deny
□	11	GE11	256	Deny
□	12	GE12	256	Deny
□	13	GE13	256	Deny

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



Edit Throttling

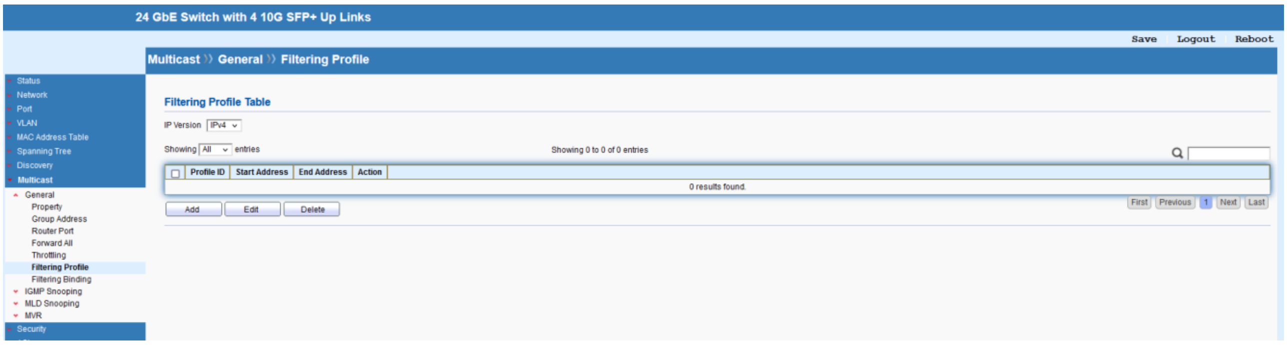
Port	GE5
IP Version	IPv4
Max Group	256 (0 - 256)
Exceed Action	● Deny ○ Replace

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.

10.1.6 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.



Multicast ›› General ›› Filtering Profile

Filtering Profile Table

IP Version: IPv4

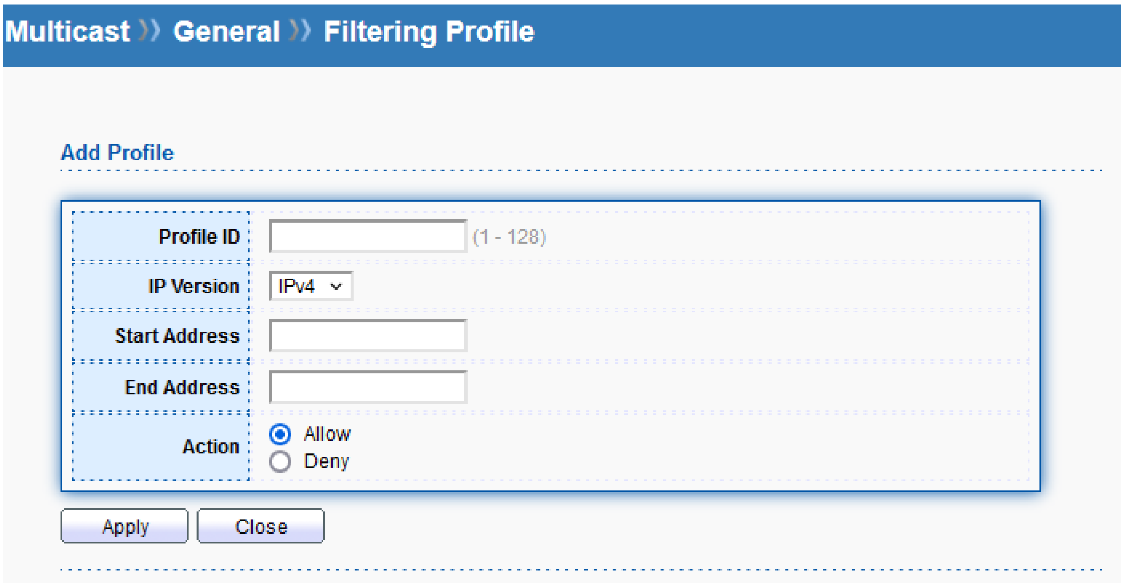
Showing All entries

Showing 0 to 0 of 0 entries

□	Profile ID	Start Address	End Address	Action

0 results found.

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.



Multicast ›› General ›› Filtering Profile

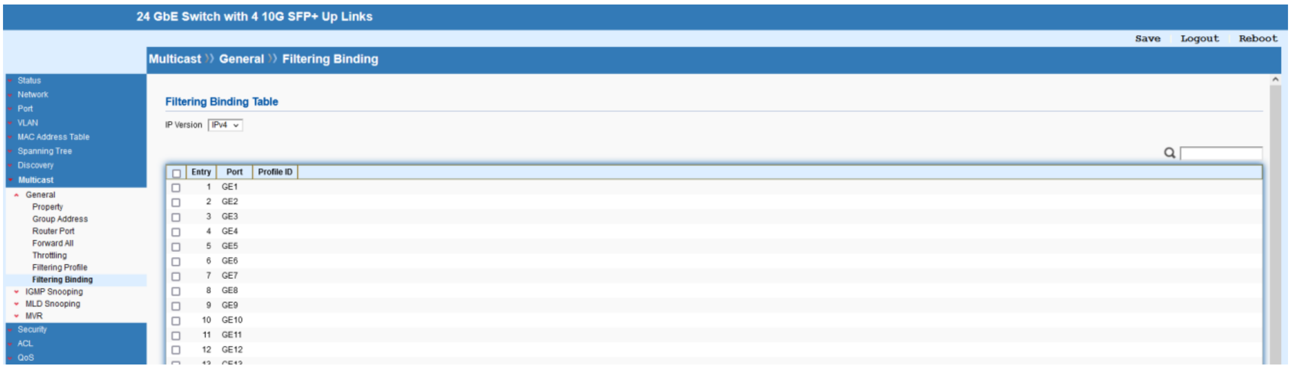
Add Profile

Profile ID	(1 - 128)
IP Version	IPv4
Start Address	
End Address	
Action	● Allow ○ Deny

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.

10.1.7 Filtering Binding

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

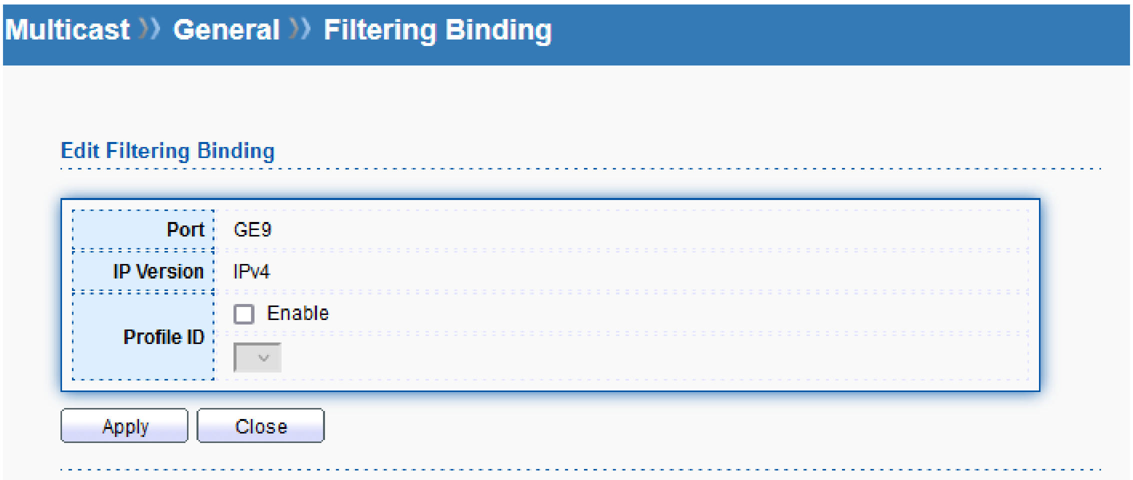


Filtering Binding Table

IP Version: IPv4

□	Entry	Port	Profile ID
□	1	GE1	
□	2	GE2	
□	3	GE3	
□	4	GE4	
□	5	GE5	
□	6	GE6	
□	7	GE7	
□	8	GE8	
□	9	GE9	
□	10	GE10	
□	11	GE11	
□	12	GE12	
□	13	GE13	

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



Edit Filtering Binding

Port	GE9
IP Version	IPv4
Profile ID	□ Enable

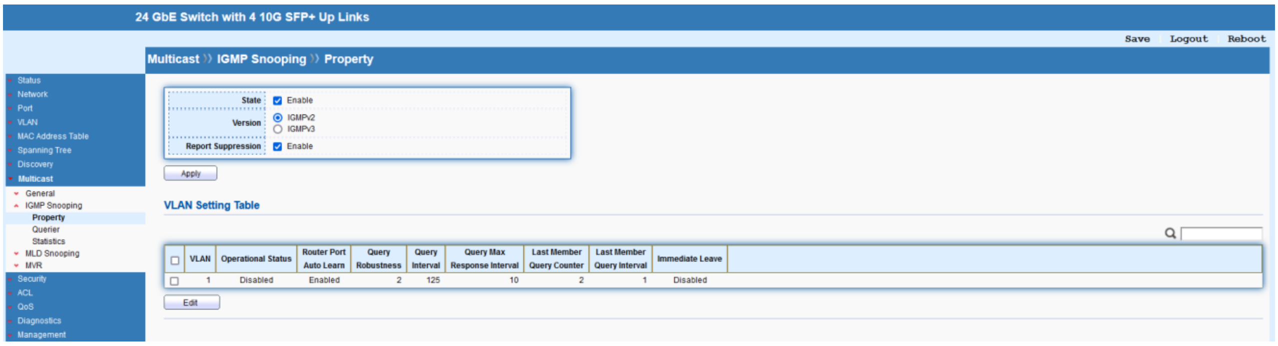
Item	Description
Port	The index number of selected port.
IP Version	The selected IP Version.
Profile ID	Enable of disable selected filtering profile for the selected port/interface.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

10.2 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.

10.2.1 Property

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



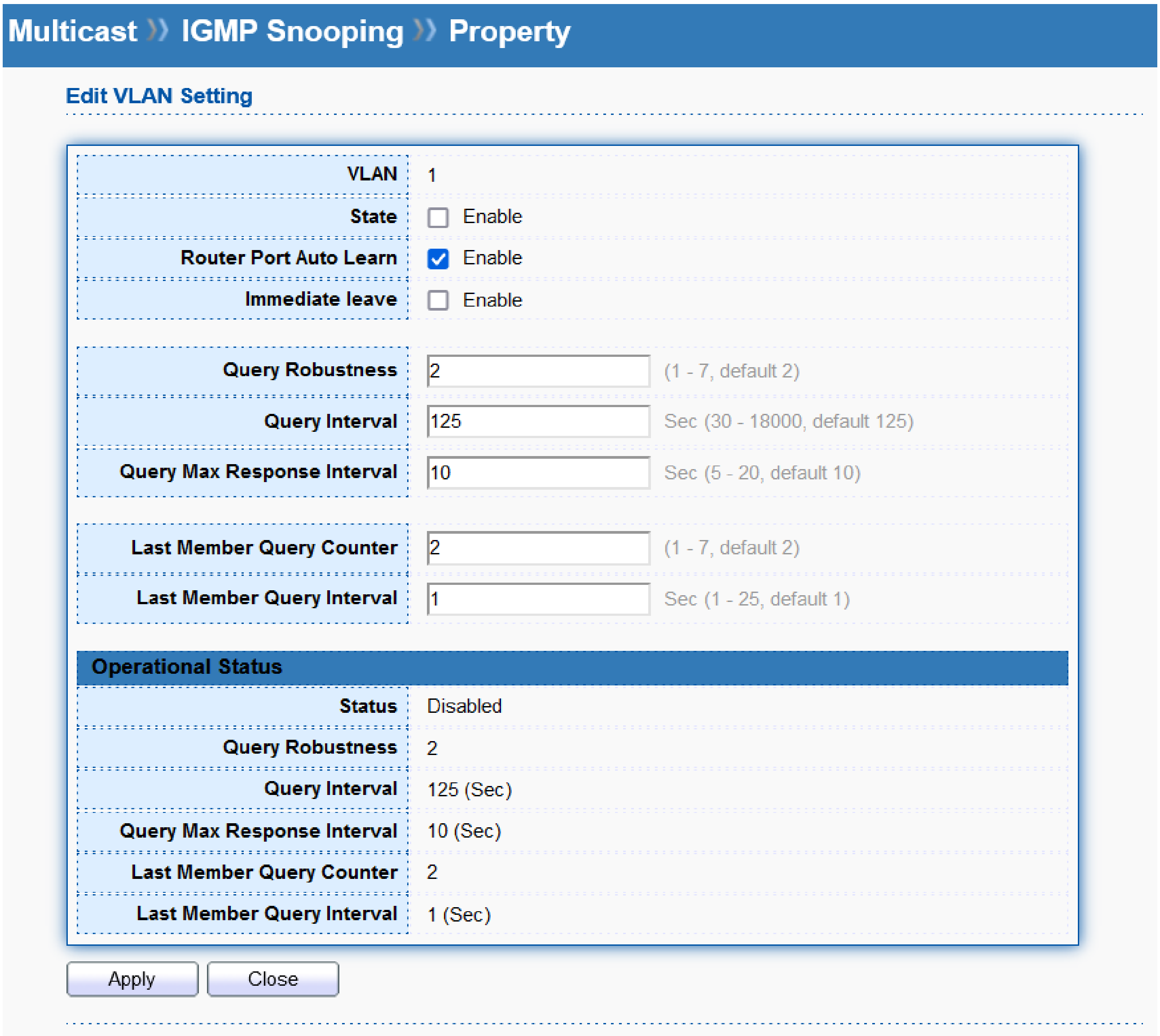
Multicast » IGMP Snooping » Property

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

VLAN Setting Table

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

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.



Multicast » IGMP Snooping » Property

Edit VLAN Setting

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

Operational Status

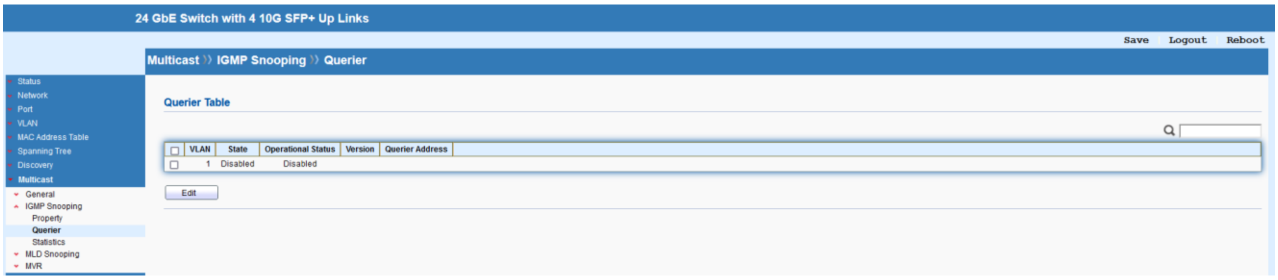
Status	Disabled
Query Robustness	2
Query Interval	125 (Sec)
Query Max Response Interval	10 (Sec)
Last Member Query Counter	2
Last Member Query Interval	1 (Sec)

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	It specifies the maximum allowed time before sending a

Interval	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.

10.2.2 Querier

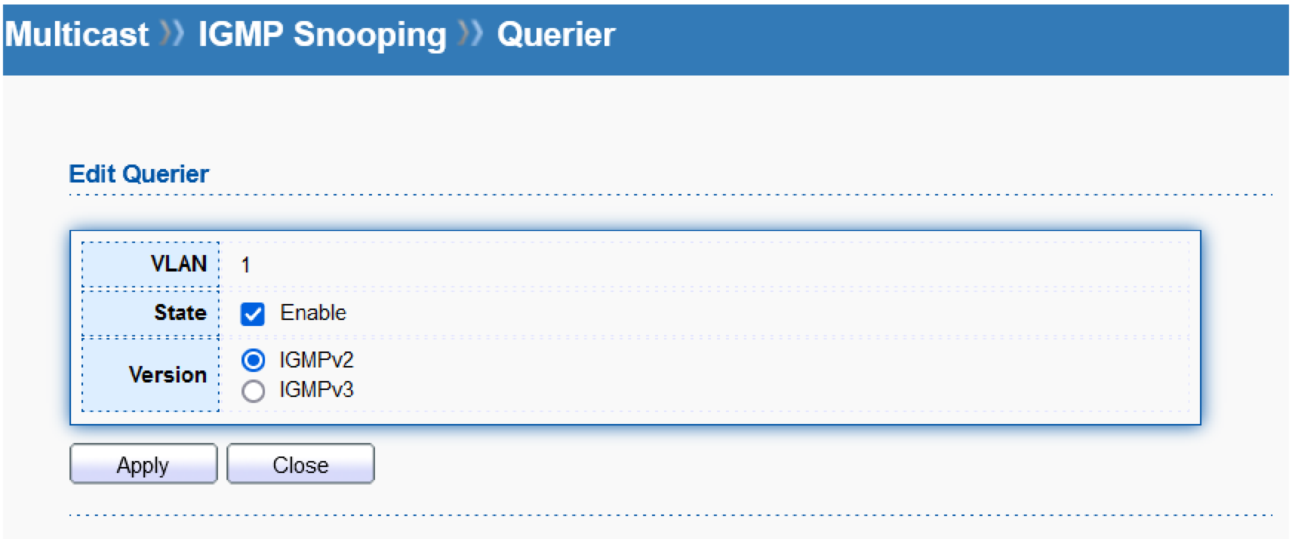
This page allows to configure querier settings on specific VLAN of IGMP Snooping.



Multicast » IGMP Snooping » Querier

Querier Table

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



Multicast » IGMP Snooping » Querier

Edit Querier

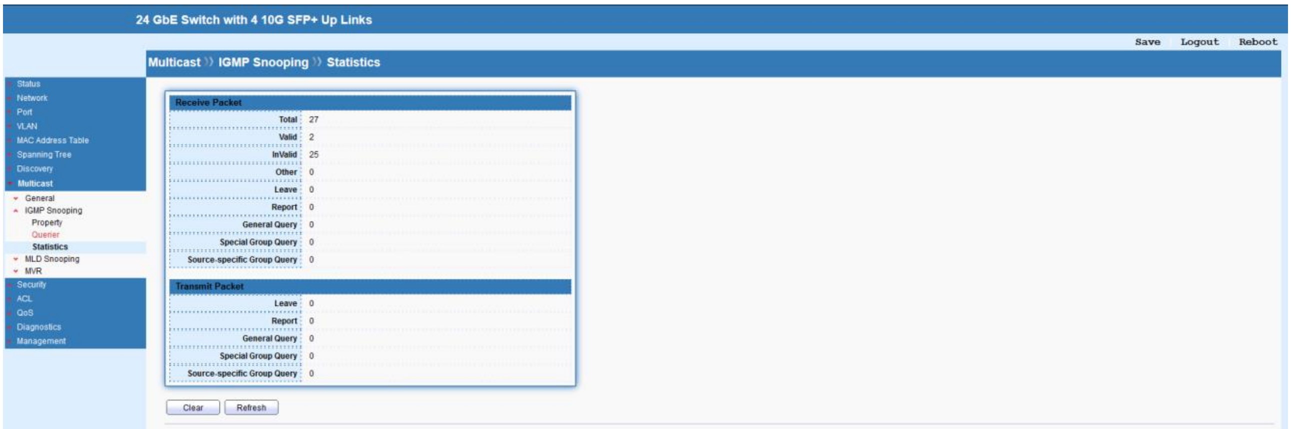
VLAN	1
State	☑ Enable
Version	● IGMPv2 ○ IGMPv3

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.

10.2.3 Statistics

This page displays the statistics of IGMP snooping.



Receive Packet

Total	27
Valid	2
InValid	25
Other	0
Leave	0
Report	0
General Query	0
Special Group Query	0
Source-specific Group Query	0

Transmit Packet

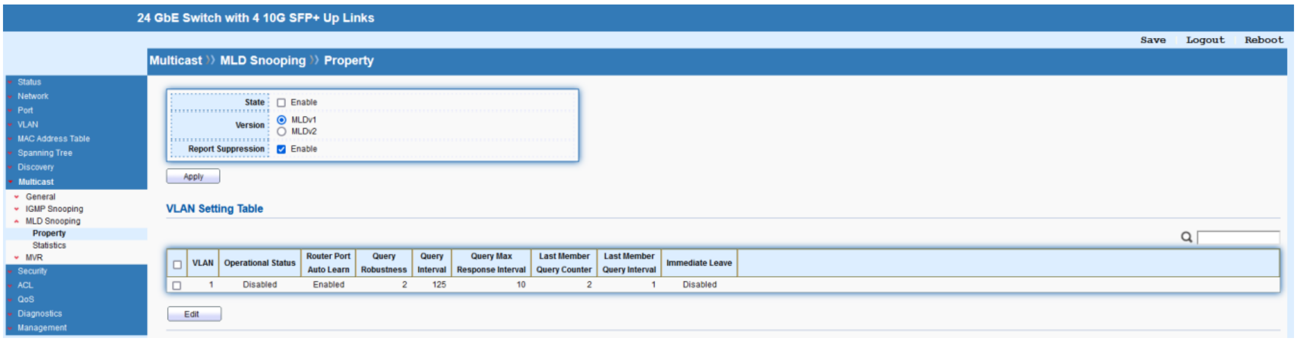
Leave	0
Report	0
General Query	0
Special Group Query	0
Source-specific Group Query	0

10.3 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.

10.3.1 Property

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



State: □ Enable

Version: ● MLDv1 ○ MLDv2

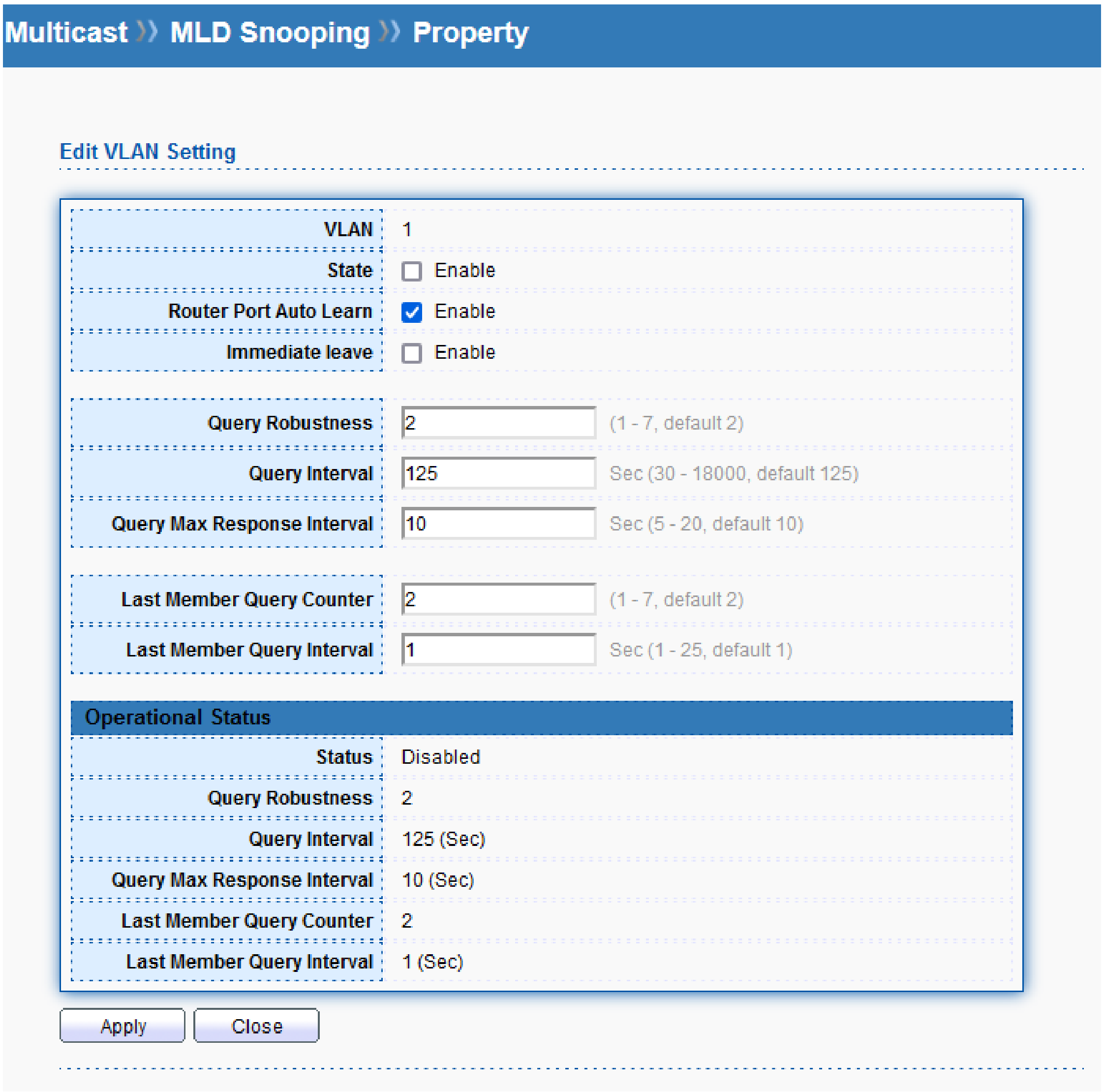
Report Suppression: ☑ Enable

VLAN Setting Table

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

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.


Multicast » MLD Snooping » Property

Edit VLAN Setting

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

Operational Status

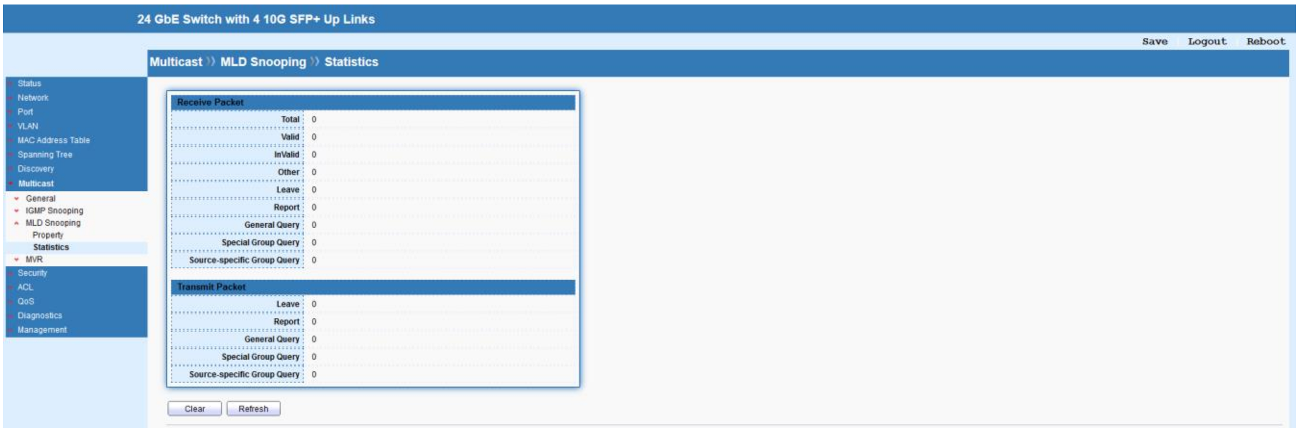
Status	Disabled
Query Robustness	2
Query Interval	125 (Sec)
Query Max Response Interval	10 (Sec)
Last Member Query Counter	2
Last Member Query Interval	1 (Sec)

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 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 operational status.
Apply	Apply the settings to the switch.
Edit	Edit the selected entry.

10.3.2 Statistics

This page displays the statistics of MLD snooping.



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

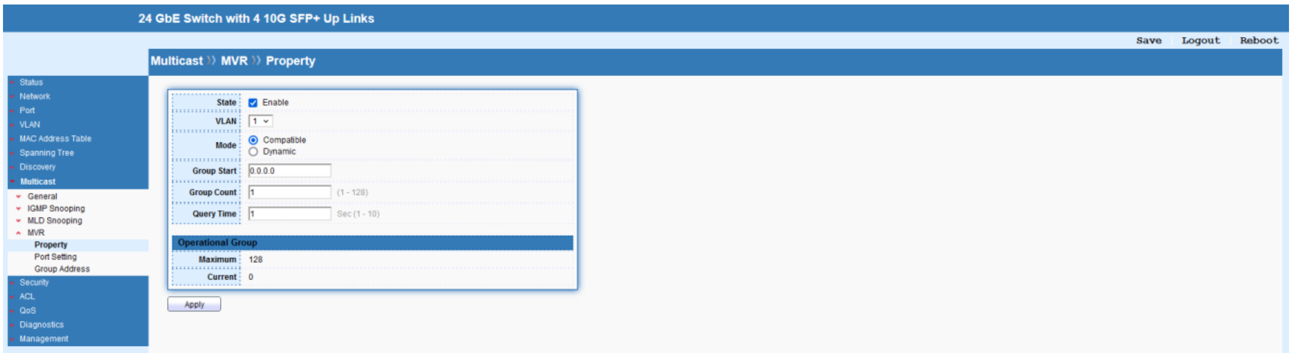
Transmit Packet	
Leave	0
Report	0
General Query	0
Special Group Query	0
Source-specific Group Query	0

10.4 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.

10.4.1 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.



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

Operational Group

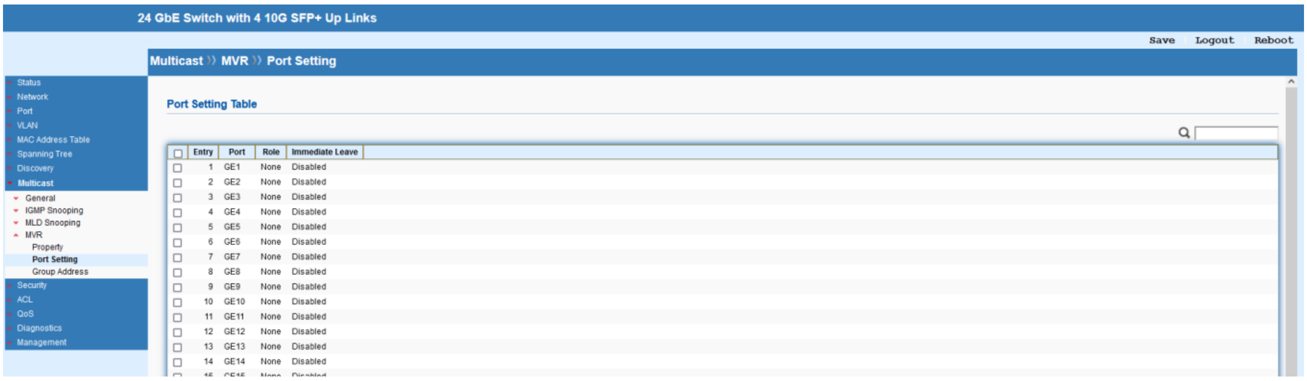
Maximum	128
Current	0

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.

10.4.2 Port Setting

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

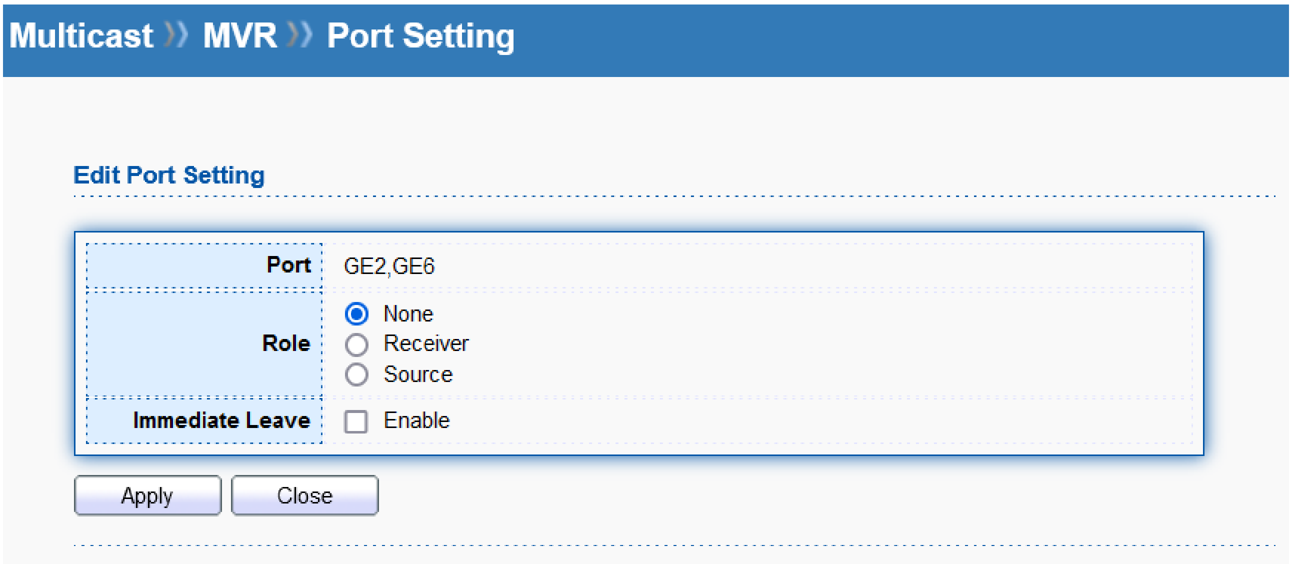
Available



Port Setting Table

□	Entry	Port	Role	Immediate Leave
□	1	GE1	None	Disabled
□	2	GE2	None	Disabled
□	3	GE3	None	Disabled
□	4	GE4	None	Disabled
□	5	GE5	None	Disabled
□	6	GE6	None	Disabled
□	7	GE7	None	Disabled
□	8	GE8	None	Disabled
□	9	GE9	None	Disabled
□	10	GE10	None	Disabled
□	11	GE11	None	Disabled
□	12	GE12	None	Disabled
□	13	GE13	None	Disabled
□	14	GE14	None	Disabled
□	15	GE15	None	Disabled

Item	Description
Edit	Edit the selected entry.



Edit Port Setting

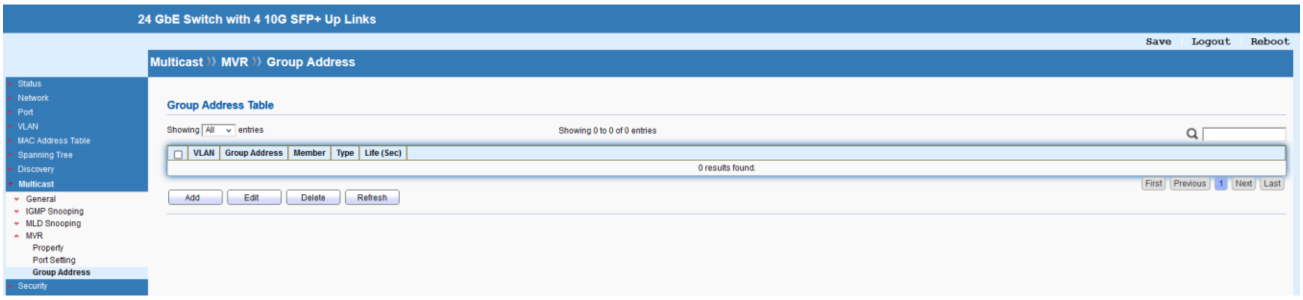
Port	GE2,GE6
Role	● None ○ Receiver ○ Source
Immediate Leave	□ Enable

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.

10.4.3 Group Address

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



Group Address Table

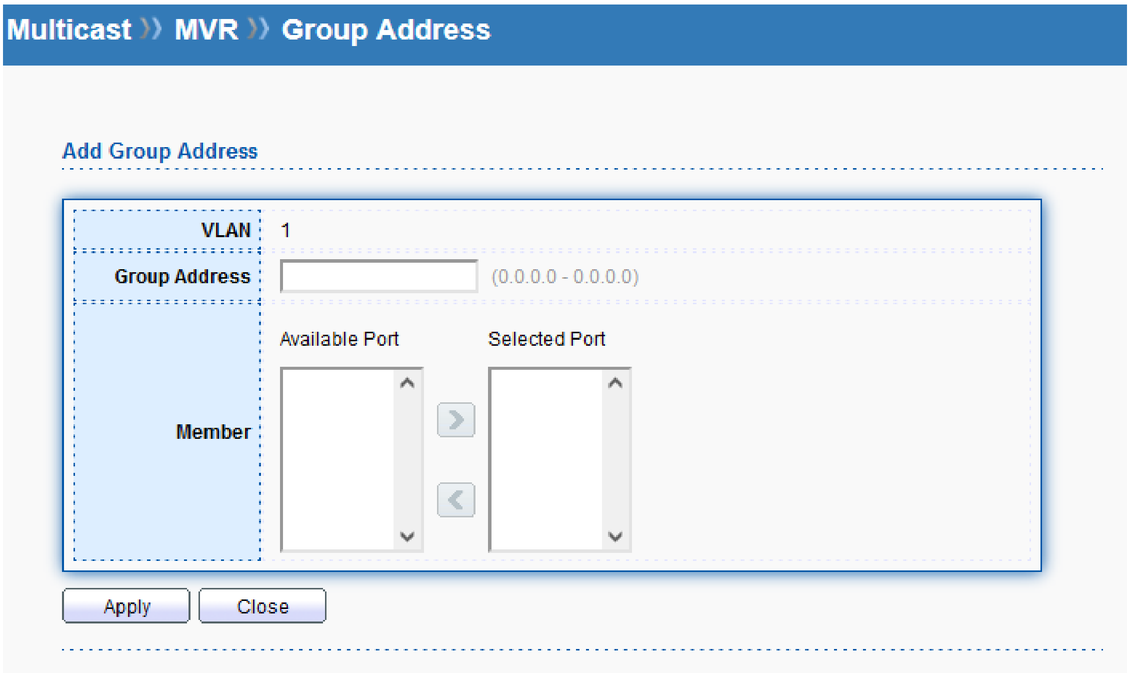
Showing All entries

Showing 0 to 0 of 0 entries

□	VLAN	Group Address	Member	Type	Life (Sec)

0 results found.

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



Add Group Address

VLAN	1
Group Address	(0.0.0.0 - 0.0.0.0)
Member	

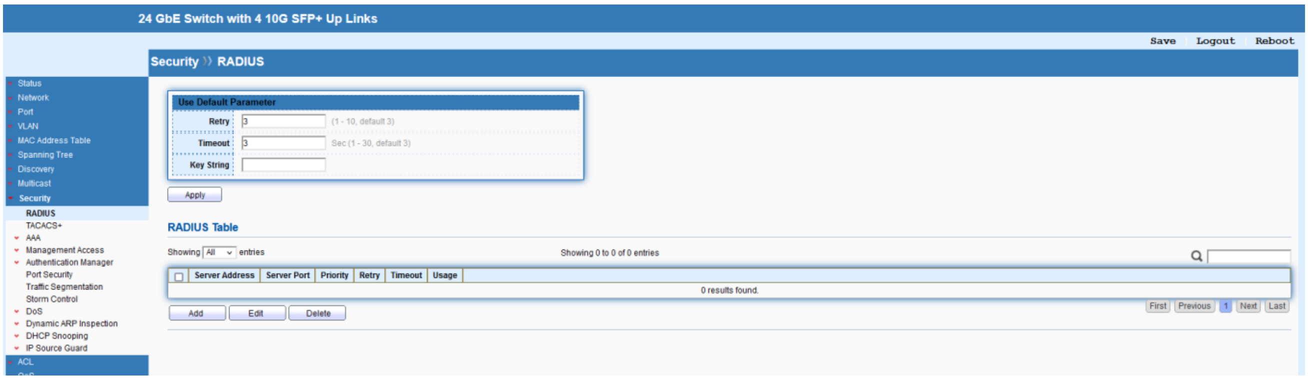
Item	Description
VLAN	The index number of selected VLAN ID.
Group Address	Define a range of IP address(es) with the format of “xxx.xxx.xxx.xxx – xxx.xxx.xxx.xxx”.

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.

11 Security

11.1 RADIUS

This page allows to add and configure multiple RADIUS servers.



Use Default Parameter

Retry: 3 (1 - 10, default 3)

Timeout: 3 Sec (1 - 30, default 3)

Key String:

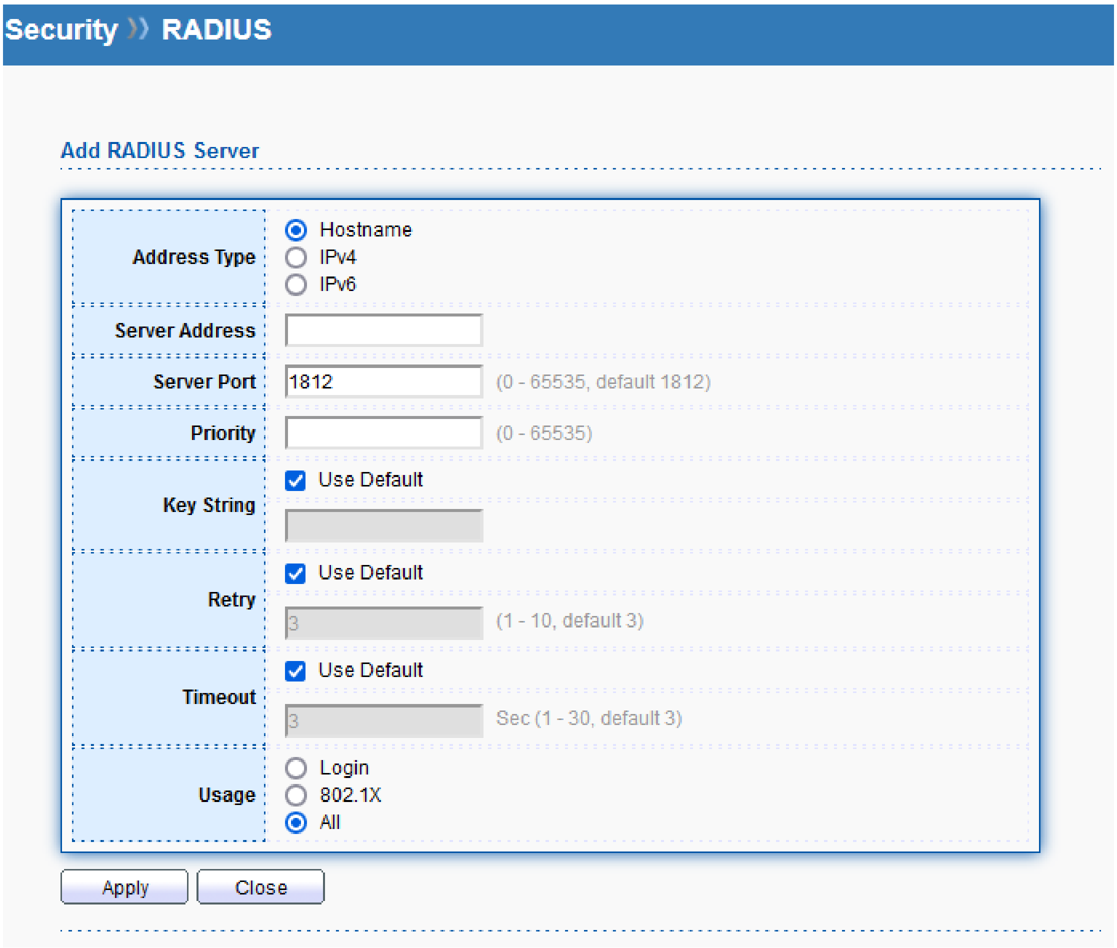
RADIUS Table

Showing All entries

Showing 0 to 0 of 0 entries

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

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.



Security » RADIUS

Add RADIUS Server

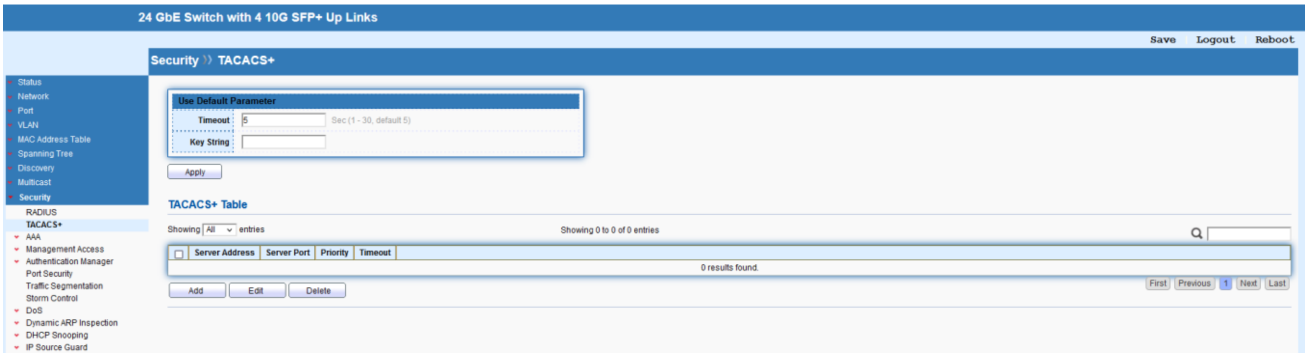
Address Type	● Hostname ○ IPv4 ○ IPv6
Server Address	
Server Port	1812 (0 - 65535, default 1812)
Priority	(0 - 65535)
Key String	☑ Use Default
Retry	☑ Use Default 3 (1 - 10, default 3)
Timeout	☑ Use Default 3 Sec (1 - 30, default 3)
Usage	○ Login ○ 802.1X ● All

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.

TACACS+

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



Use Default Parameter

Timeout: 5 Sec (1 - 30, default 5)

Key String:

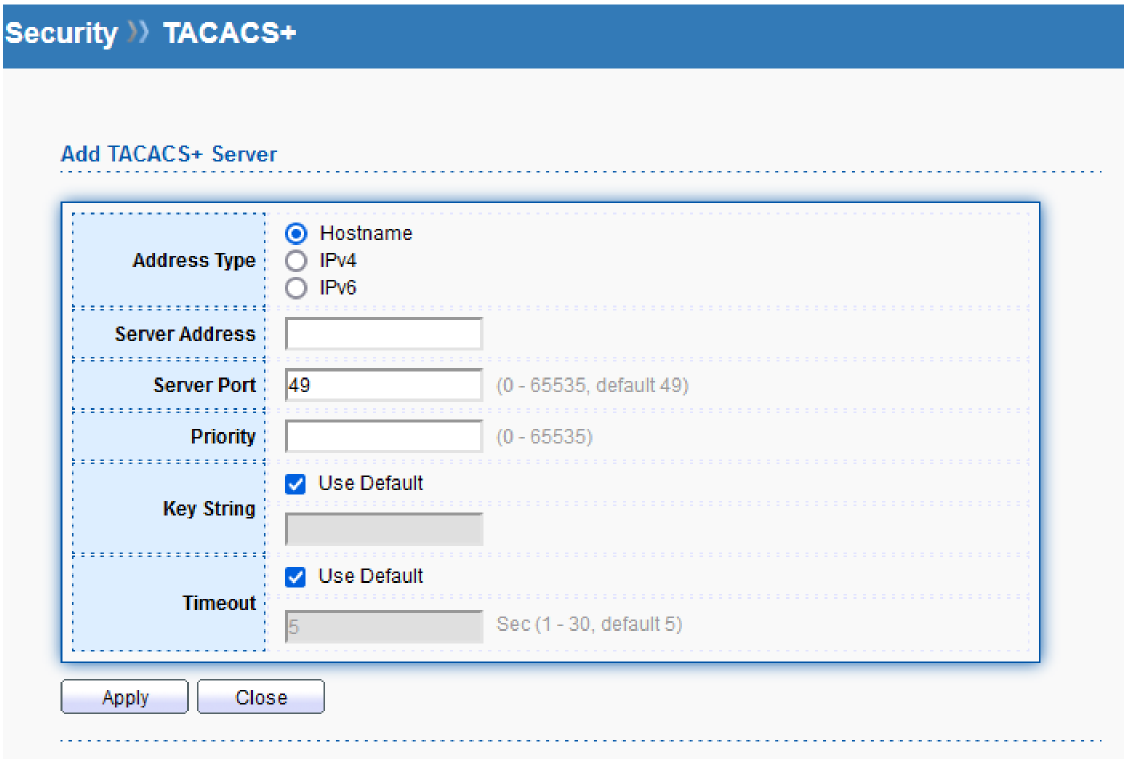
TACACS+ Table

Showing All entries

Showing 0 to 0 of 0 entries

□	Server Address	Server Port	Priority	Timeout
0 results found.				

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.


Security » TACACS+

Add TACACS+ Server

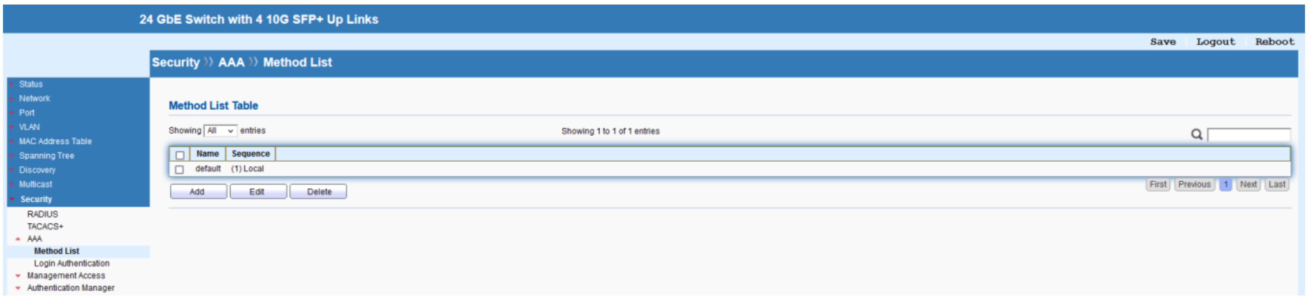
Address Type	● Hostname ○ IPv4 ○ IPv6
Server Address	
Server Port	49 (0 - 65535, default 49)
Priority	(0 - 65535)
Key String	☑ Use Default
Timeout	☑ Use Default 5 Sec (1 - 30, default 5)

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.

11.2 AAA

11.2.1 Method List

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



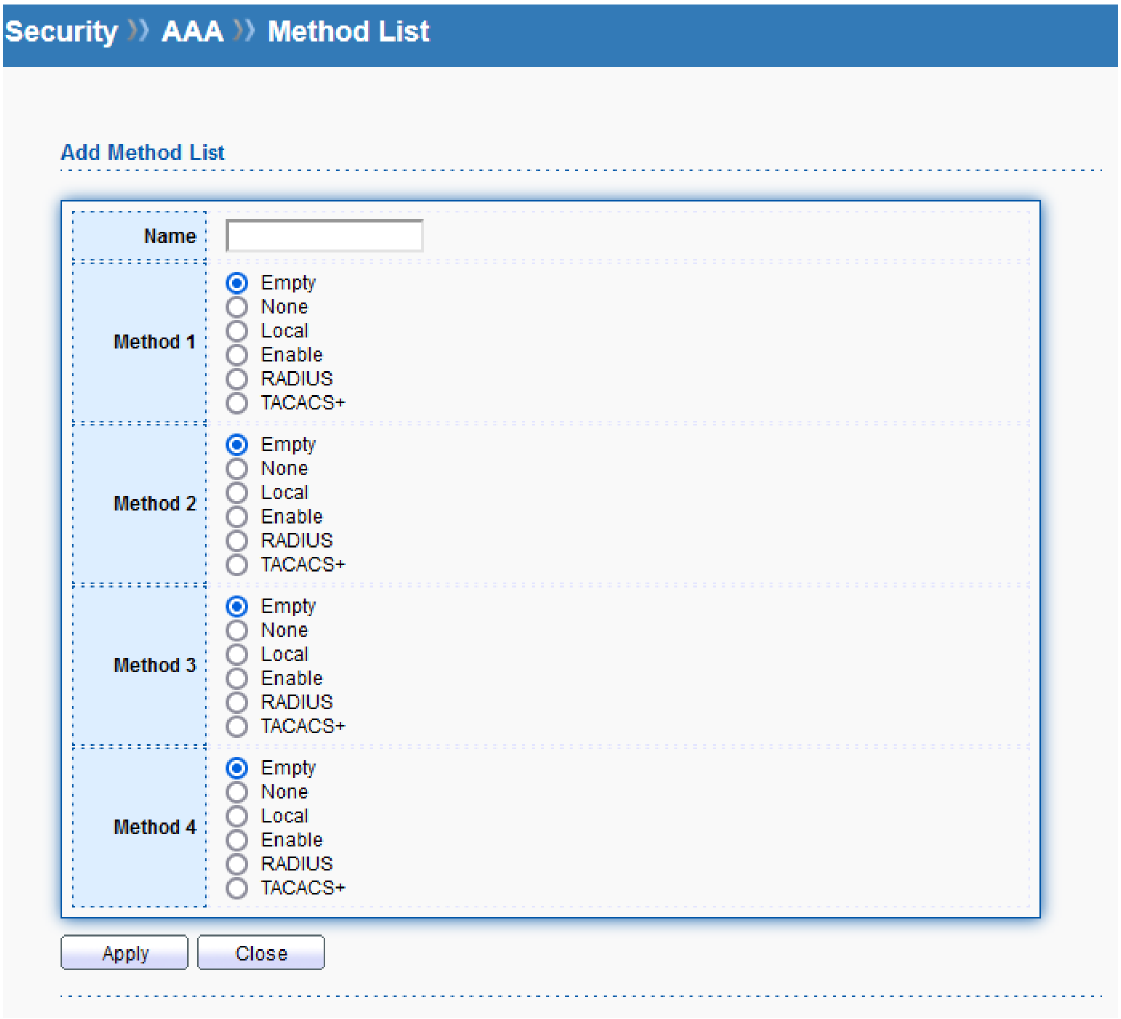
Method List Table

Showing All entries

Showing 1 to 1 of 1 entries

☐	Name	Sequence
☐	default	(1) Local

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



Add Method List

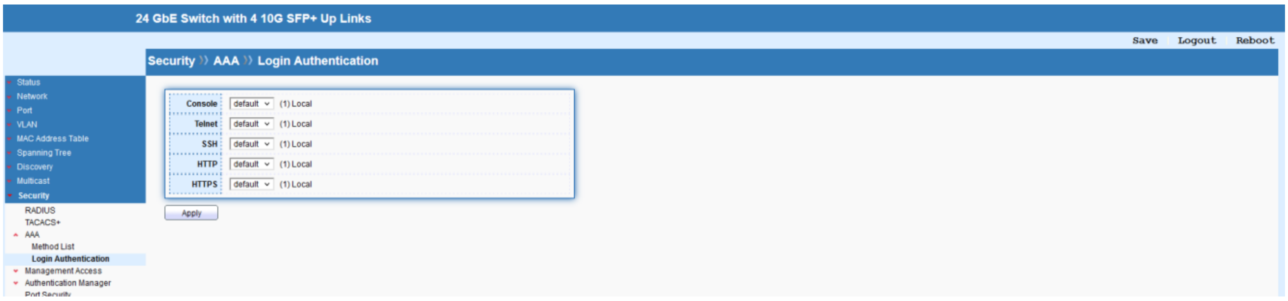
Name	
Method 1	● Empty ○ None ○ Local ○ Enable ○ RADIUS ○ TACACS+
Method 2	● Empty ○ None ○ Local ○ Enable ○ RADIUS ○ TACACS+
Method 3	● Empty ○ None ○ Local ○ Enable ○ RADIUS ○ TACACS+
Method 4	● Empty ○ None ○ Local ○ Enable ○ RADIUS ○ TACACS+

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.

11.2.2 Login Authentication

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



Console: default (1) Local

Telnet: default (1) Local

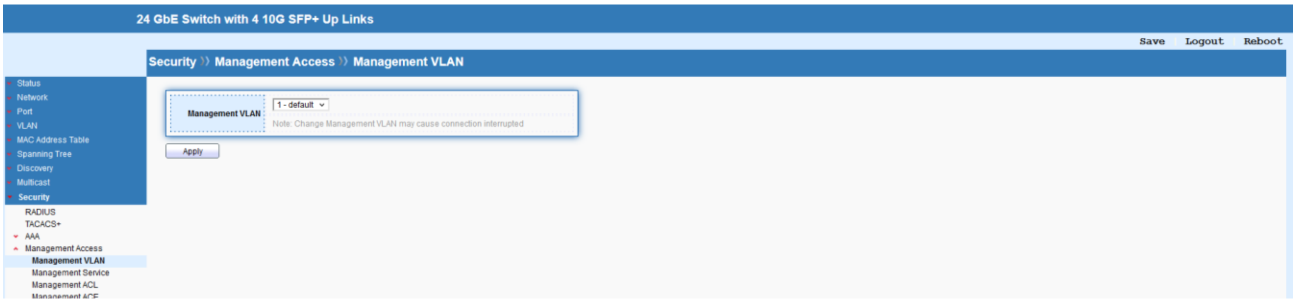
SSH: default (1) Local

HTTP: default (1) Local

HTTPS: default (1) Local

11.3 Management Access

11.3.1 Management VLAN



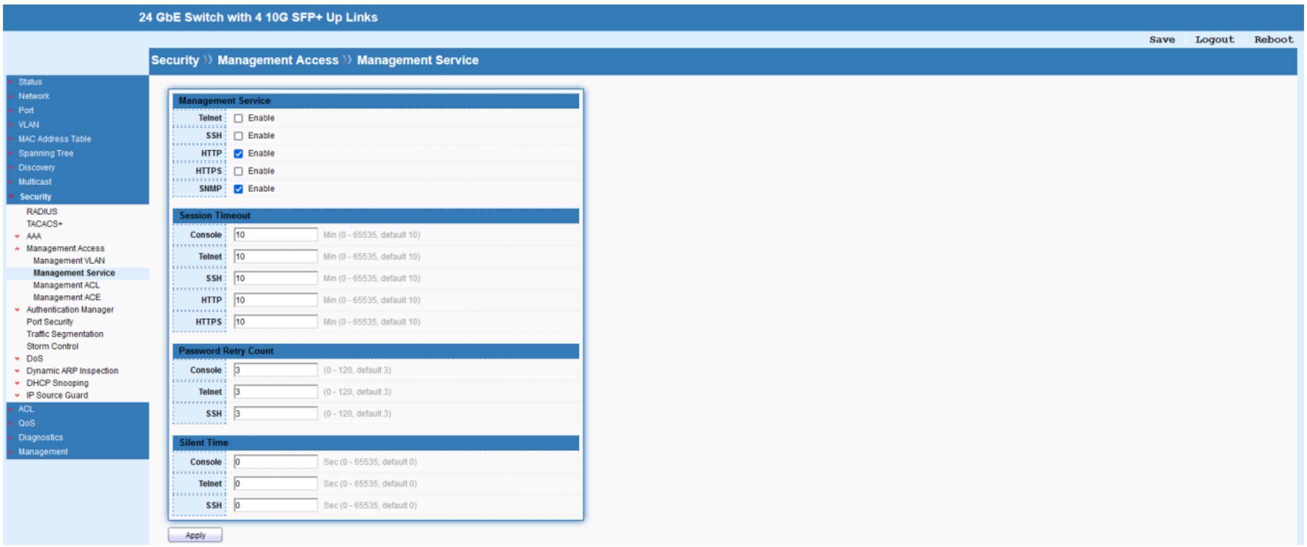
Management VLAN: 1 - default

Note: Change Management VLAN may cause connection interrupted

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

11.3.2 Management Service

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



Management Service

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

Session Timeout

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

Password Retry Count

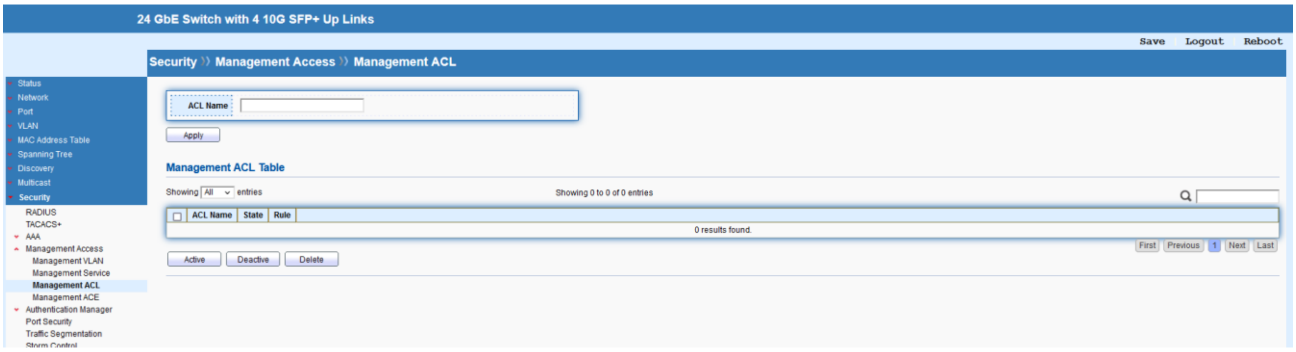
Console: 3 (0 - 120, default 3)
Telnet: 3 (0 - 120, default 3)
SSH: 3 (0 - 120, default 3)

Silent Time

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

11.3.3 Management ACL

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



ACL Name:

Management ACL Table

Showing All entries

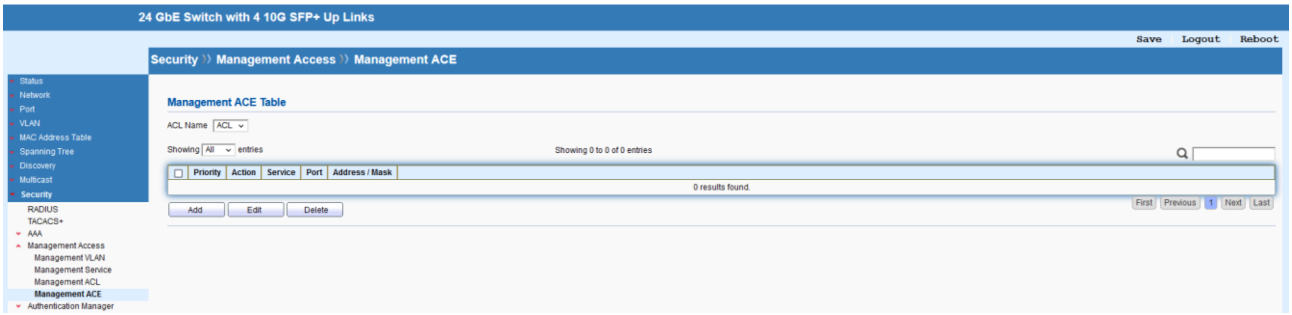
Showing 0 to 0 of 0 entries

□	ACL Name	State	Rule
0 results found.			

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.

11.3.4 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.



24 GbE Switch with 4 10G SFP+ Up Links

Security » Management Access » Management ACE

Management ACE Table

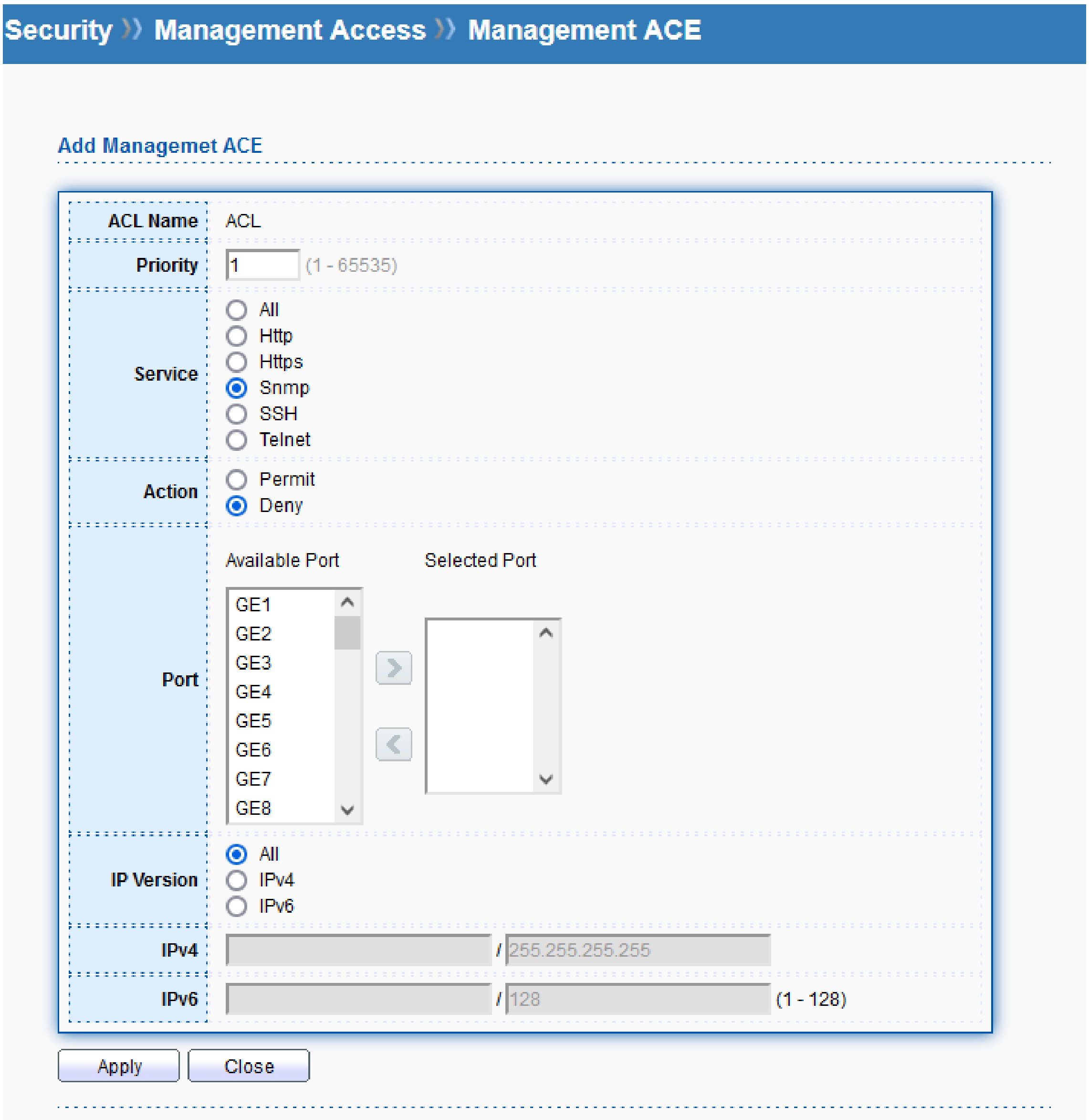
ACL Name: ACL

Showing All entries

Showing 0 to 0 of 0 entries

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

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.



Security » Management Access » Management ACE

Add Managemet ACE

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

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.

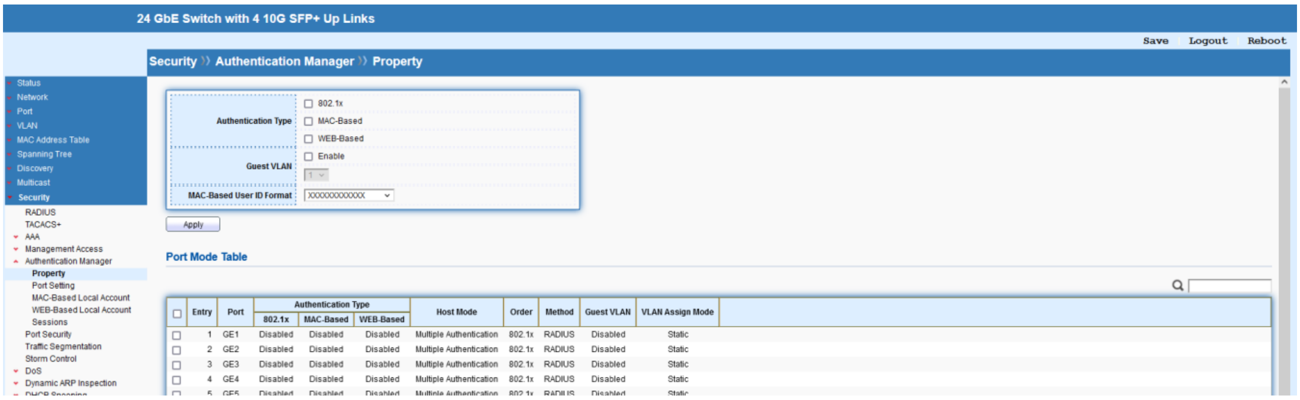
	IPv6: Specify the IPv6 address / subnet.
IPv4	Enter the IPv4 address / subnet to which the ACE rule should apply.
IPv6	Enter the IPv6 address / subnet to which the ACE rule should apply.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

11.4 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.

11.4.1 Property

The 850X-28 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.



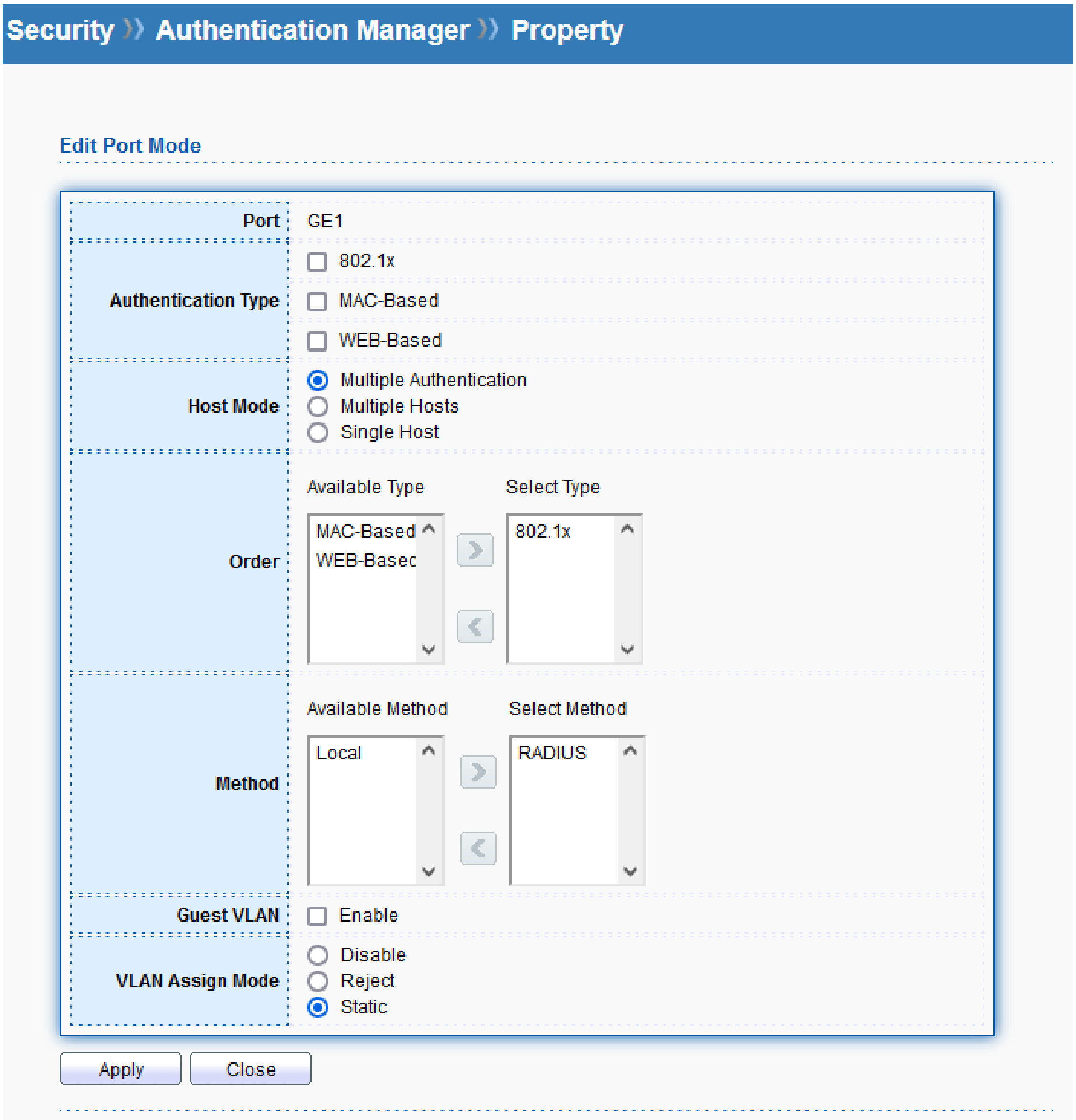
Authentication Type: □ 802.1x □ MAC-Based □ WEB-Based

Guest VLAN: □ Enable 1

MAC-Based User ID Format: XXXXXXXXXXXX

□	Entry	Port	Authentication Type			Host Mode	Order	Method	Guest VLAN	VLAN Assign Mode
			802.1x	MAC-Based	WEB-Based					
□	1	GE1	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
□	2	GE2	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
□	3	GE3	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
□	4	GE4	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
□	5	GE5	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static

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).



Security » Authentication Manager » Property

Edit Port Mode

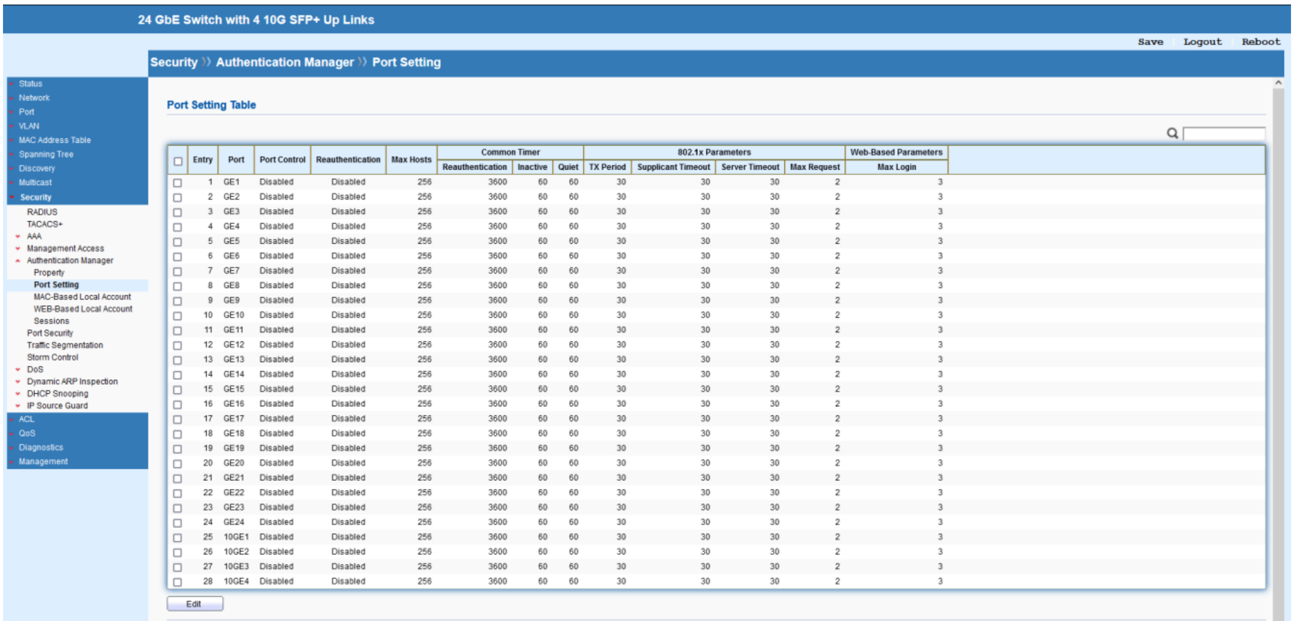
Port	GE1
Authentication Type	□ 802.1x □ MAC-Based □ WEB-Based
Host Mode	● Multiple Authentication ○ Multiple Hosts ○ Single Host
Order	Available Type: MAC-Based, WEB-Based Select Type: 802.1x
Method	Available Method: Local Select Method: RADIUS
Guest VLAN	□ Enable
VLAN Assign Mode	○ Disable ○ Reject ● Static

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.

11.4.2 Port Setting

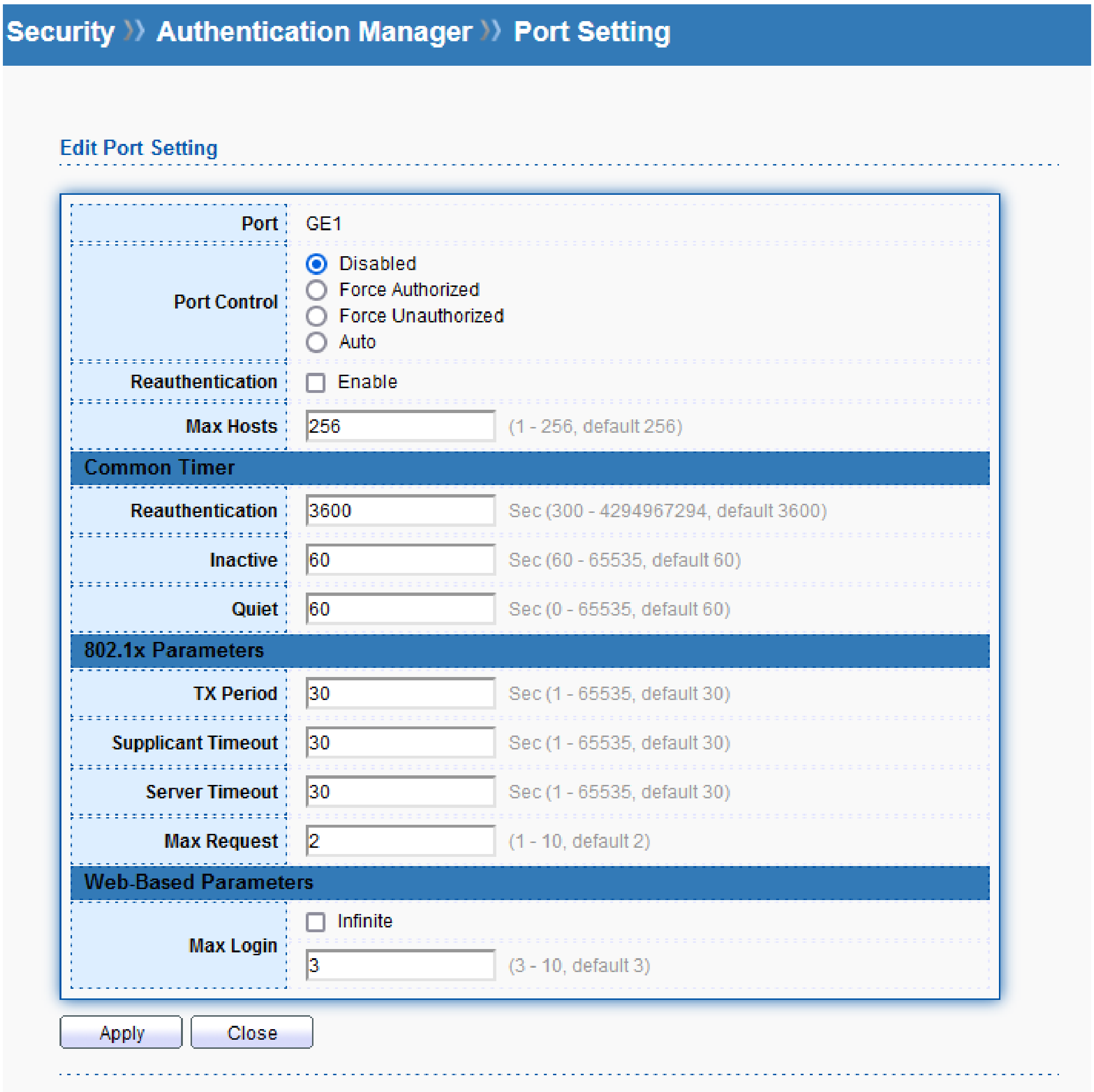
This page allows to controls port setting, based on 802.1X, for Ethernet port authentication.



Port Setting Table

☐	Entry	Port	Port Control	Reauthentication	Max Hosts	Common Timer			802.1x Parameters				Web-Based Parameters
						Reauthentication	Inactive	Quiet	TX Period	Supplicant Timeout	Server Timeout	Max Request	Max Login
☐	1	GE1	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	2	GE2	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	3	GE3	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	4	GE4	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	5	GE5	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	6	GE6	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	7	GE7	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	8	GE8	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	9	GE9	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	10	GE10	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	11	GE11	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	12	GE12	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	13	GE13	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	14	GE14	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	15	GE15	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	16	GE16	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	17	GE17	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	18	GE18	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	19	GE19	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	20	GE20	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	21	GE21	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	22	GE22	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	23	GE23	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	24	GE24	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	25	10GE1	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	26	10GE2	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	27	10GE3	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
☐	28	10GE4	Disabled	Disabled	256	3600	60	60	30	30	30	2	3

Item	Description
Edit	Edit the selected port(s).



Security ›› Authentication Manager ›› Port Setting

Edit Port Setting

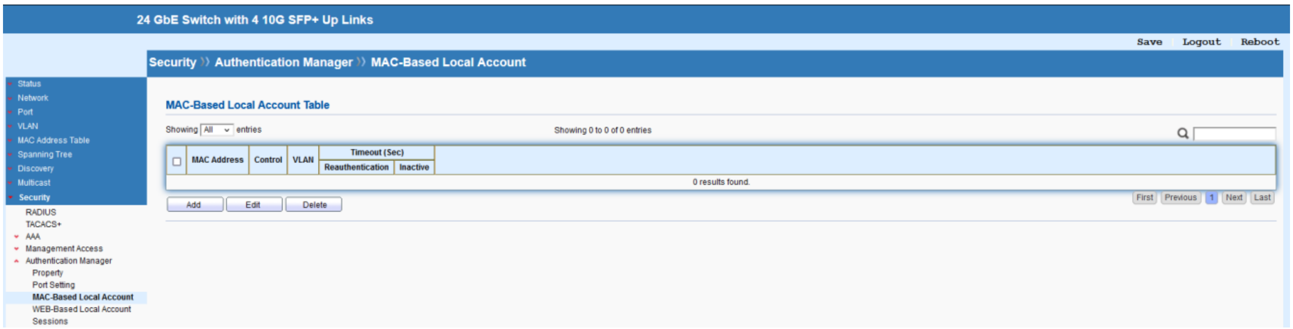
Port	GE1
Port Control	● Disabled ○ Force Authorized ○ Force Unauthorized ○ Auto
Reauthentication	□ Enable
Max Hosts	256 (1 - 256, default 256)
Common Timer	
Reauthentication	3600 Sec (300 - 4294967294, default 3600)
Inactive	60 Sec (60 - 65535, default 60)
Quiet	60 Sec (0 - 65535, default 60)
802.1x Parameters	
TX Period	30 Sec (1 - 65535, default 30)
Supplicant Timeout	30 Sec (1 - 65535, default 30)
Server Timeout	30 Sec (1 - 65535, default 30)
Max Request	2 (1 - 10, default 2)
Web-Based Parameters	
Max Login	□ Infinite 3 (3 - 10, default 3)

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.

11.4.3 MAC-Based Local Account

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



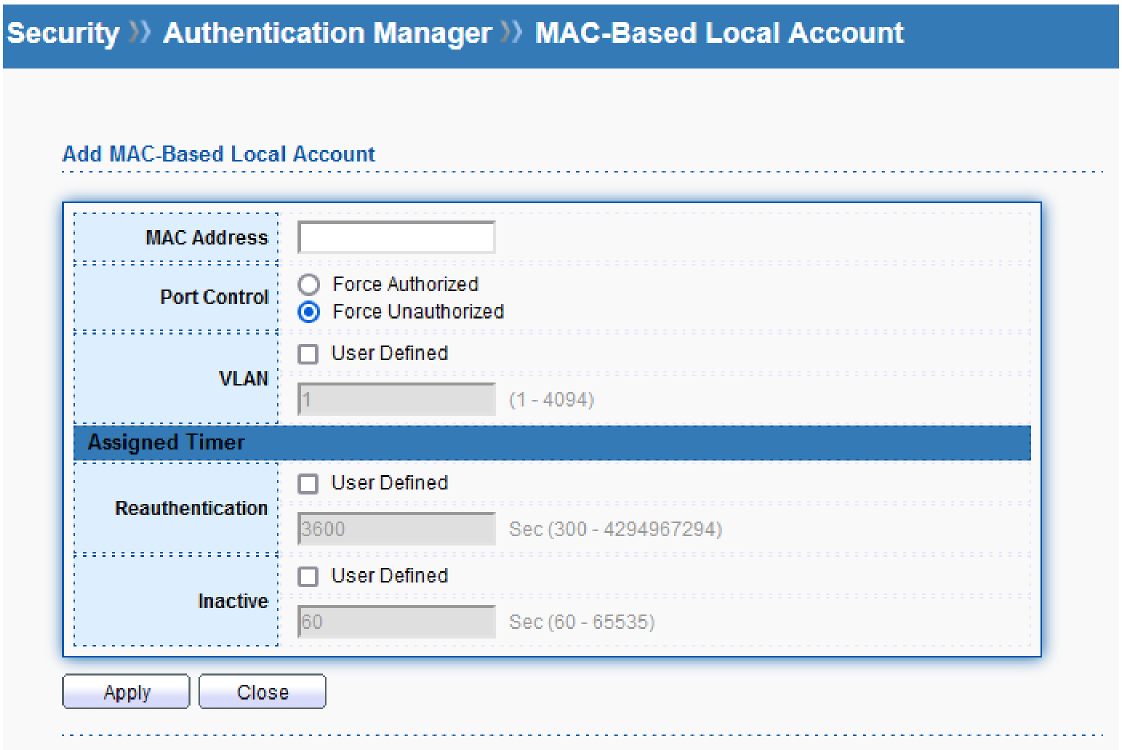
MAC-Based Local Account Table

Showing All entries   Showing 0 to 0 of 0 entries

□	MAC Address	Control	VLAN	Timeout (Sec)	
				Reauthentication	Inactive

0 results found.

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



Add MAC-Based Local Account

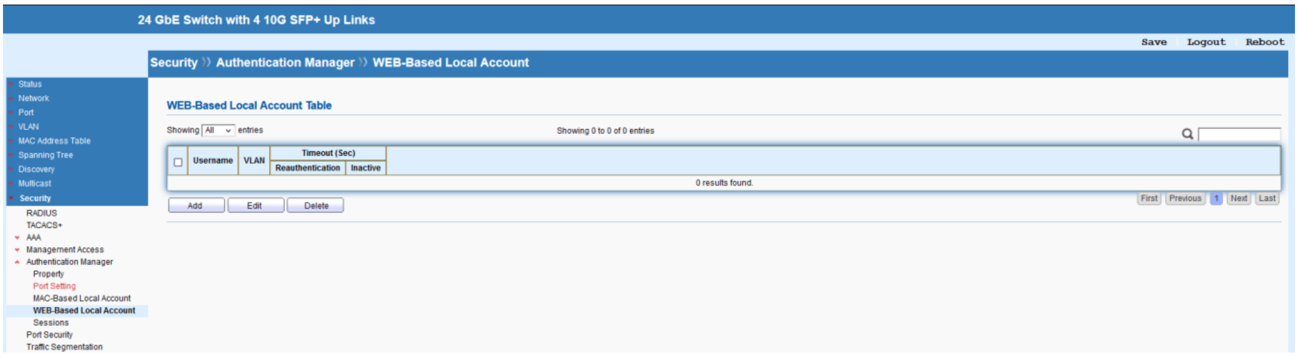
MAC Address	
Port Control	○ Force Authorized ● Force Unauthorized
VLAN	□ User Defined 1 (1 - 4094)
Assigned Timer	
Reauthentication	□ User Defined 3600 Sec (300 - 4294967294)
Inactive	□ User Defined 60 Sec (60 - 65535)

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.
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.

11.4.4 WEB-Based Local Account

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



WEB-Based Local Account Table

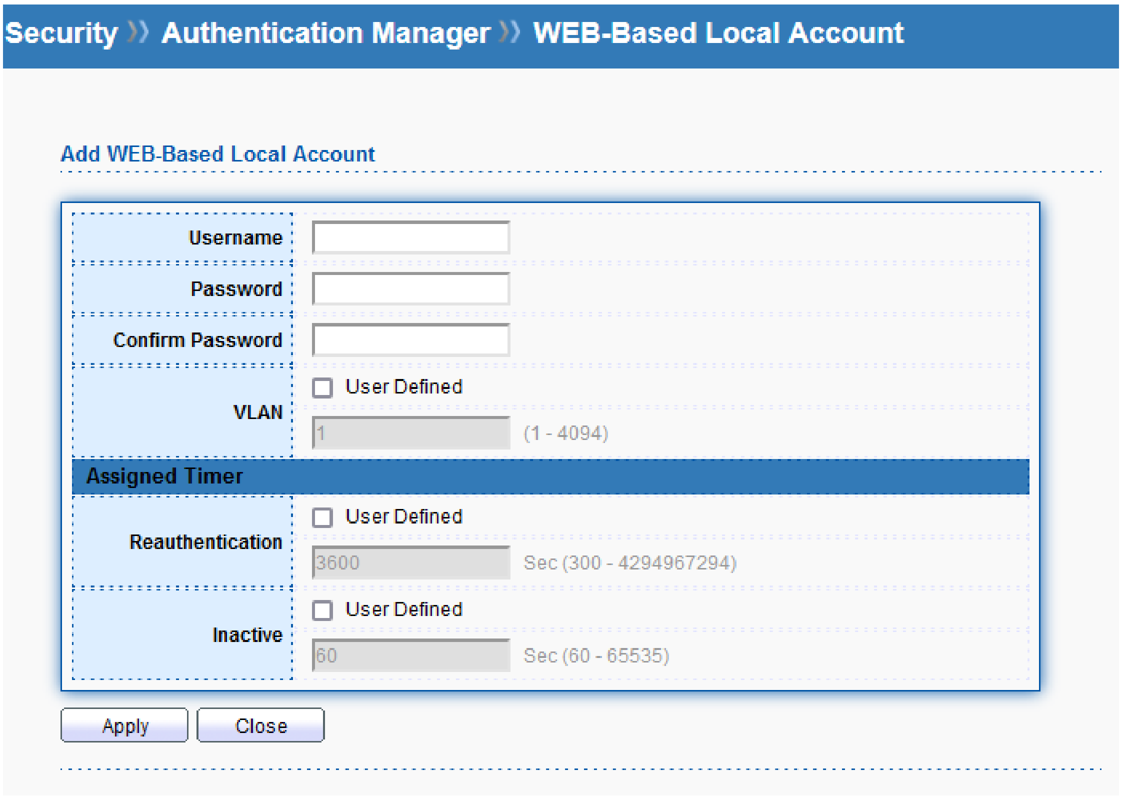
Showing All entries

Showing 0 to 0 of 0 entries

□	Username	VLAN	Timeout (Sec)	
			Reauthentication	Inactive

0 results found.

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



Security » Authentication Manager » WEB-Based Local Account

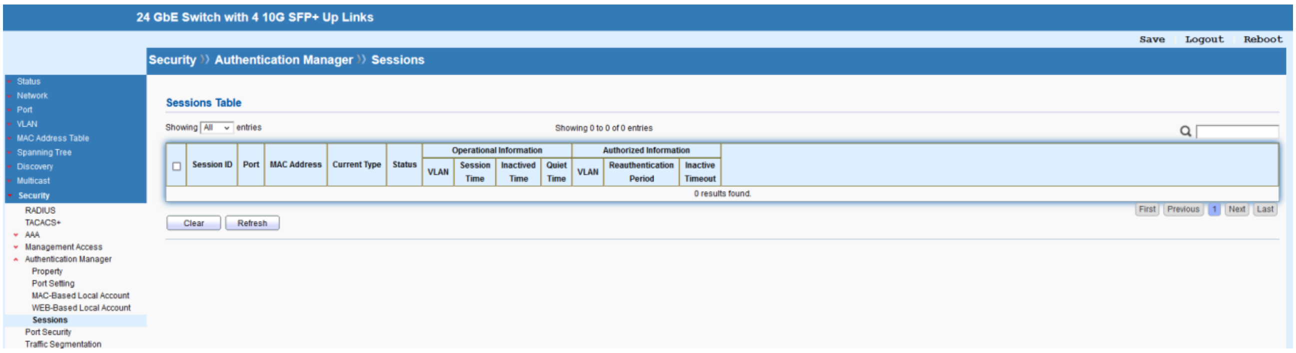
Add WEB-Based Local Account

Username	
Password	
Confirm Password	
VLAN	□ User Defined 1 (1 - 4094)
Assigned Timer	
Reauthentication	□ User Defined 3600 Sec (300 - 4294967294)
Inactive	□ User Defined 60 Sec (60 - 65535)

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.

11.4.5 Sessions

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



Sessions Table

Showing All entries

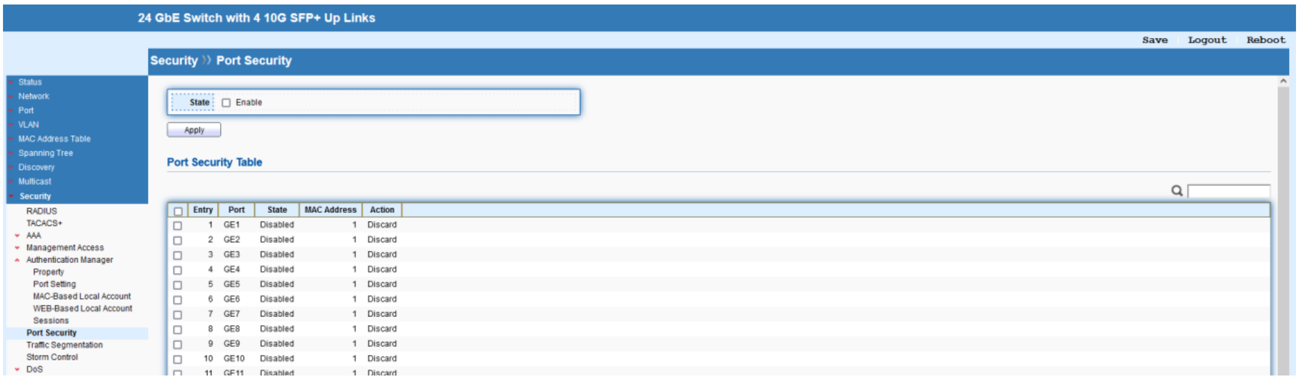
Showing 0 to 0 of 0 entries

□	Session ID	Port	MAC Address	Current Type	Status	Operational Information				Authorized Information		
						VLAN	Session Time	Inactived Time	Quiet Time	VLAN	Reauthentication Period	Inactive Timeout

0 results found.

11.5 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, releated action will be performed once detecting that the number of MAC address exceeds the limit.

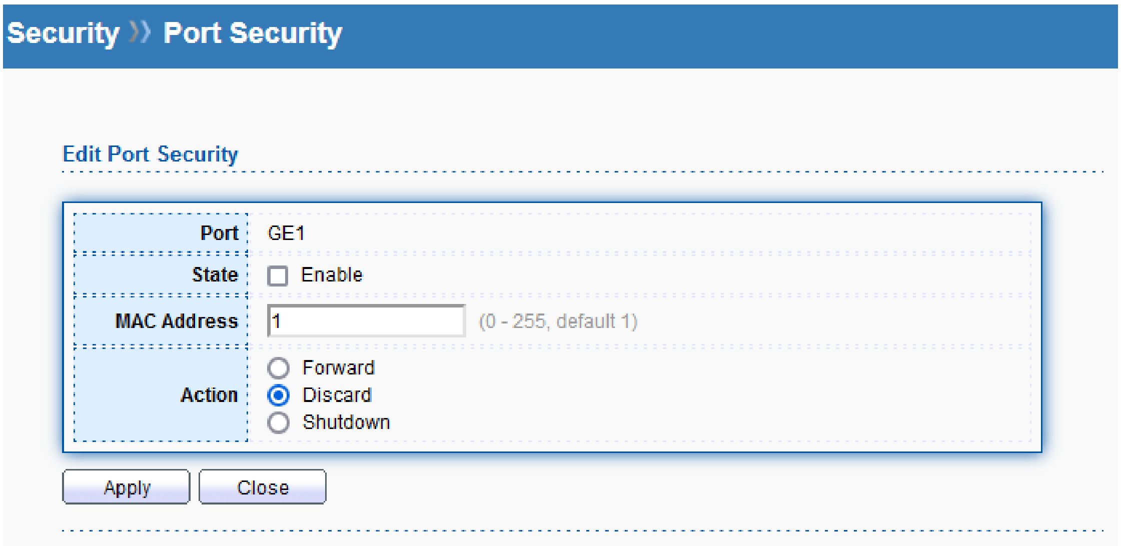


State □ Enable

Port Security Table

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

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

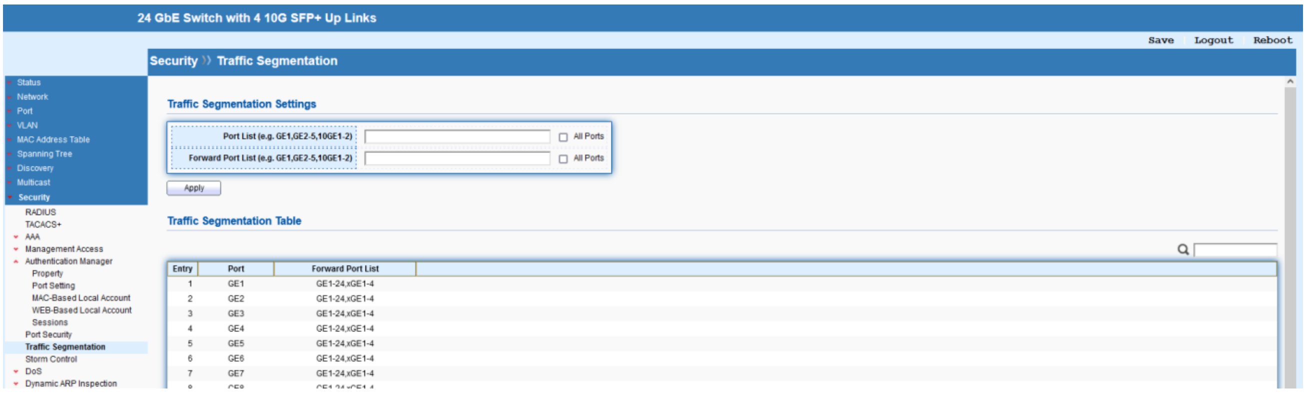


Port	GE1
State	□ Enable
MAC Address	1 (0 - 255, default 1)
Action	○ Forward ● Discard ○ Shutdown

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.

11.6 Traffic Segmentation

This page allows to enable traffic segmentation on specified port(s).



Traffic Segmentation Settings

Port List (e.g. GE1,GE2-5,10GE1-2) □ All Ports

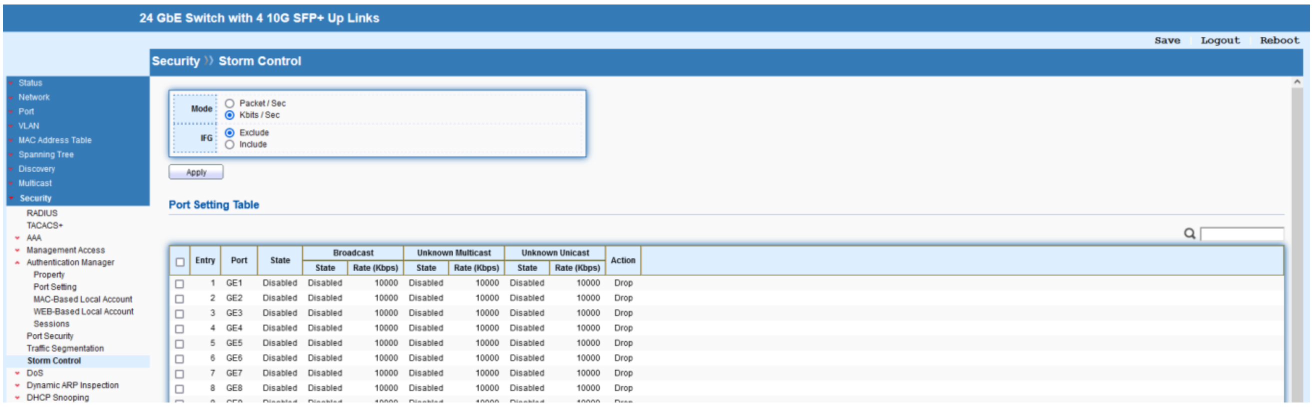
Forward Port List (e.g. GE1,GE2-5,10GE1-2) □ All Ports

Traffic Segmentation Table

Entry	Port	Forward Port List
1	GE1	GE1-24,xGE1-4
2	GE2	GE1-24,xGE1-4
3	GE3	GE1-24,xGE1-4
4	GE4	GE1-24,xGE1-4
5	GE5	GE1-24,xGE1-4
6	GE6	GE1-24,xGE1-4
7	GE7	GE1-24,xGE1-4

11.7 Storm Control

This page allows to configure general settings for Storm Control.



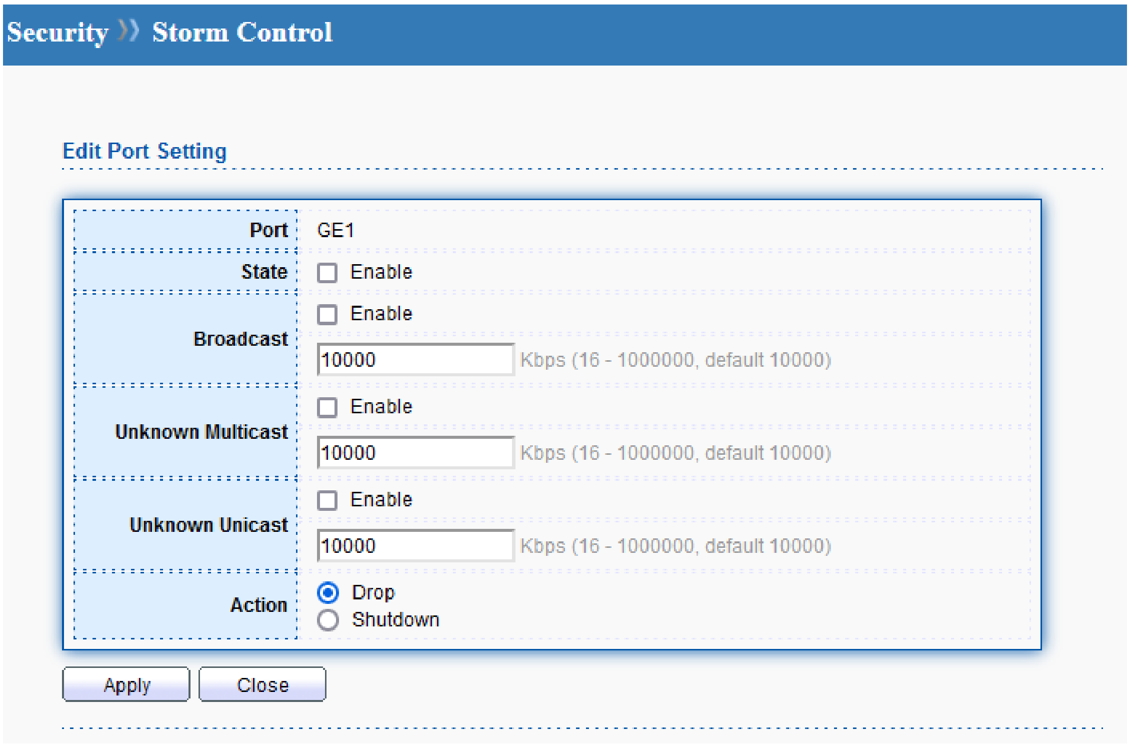
Mode ○ Packet / Sec ● Kbits / Sec

IFG ● Exclude ○ Include

Port Setting Table

□	Entry	Port	State	Broadcast		Unknown Multicast		Unknown Unicast		Action
				State	Rate (Kbps)	State	Rate (Kbps)	State	Rate (Kbps)	
□	1	GE1	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
□	2	GE2	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
□	3	GE3	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
□	4	GE4	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
□	5	GE5	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
□	6	GE6	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
□	7	GE7	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop
□	8	GE8	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop

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.



Security » Storm Control

Edit Port Setting

Port	GE1
State	□ Enable
Broadcast	□ Enable 10000 Kbps (16 - 1000000, default 10000)
Unknown Multicast	□ Enable 10000 Kbps (16 - 1000000, default 10000)
Unknown Unicast	□ Enable 10000 Kbps (16 - 1000000, default 10000)
Action	● Drop ○ Shutdown

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.

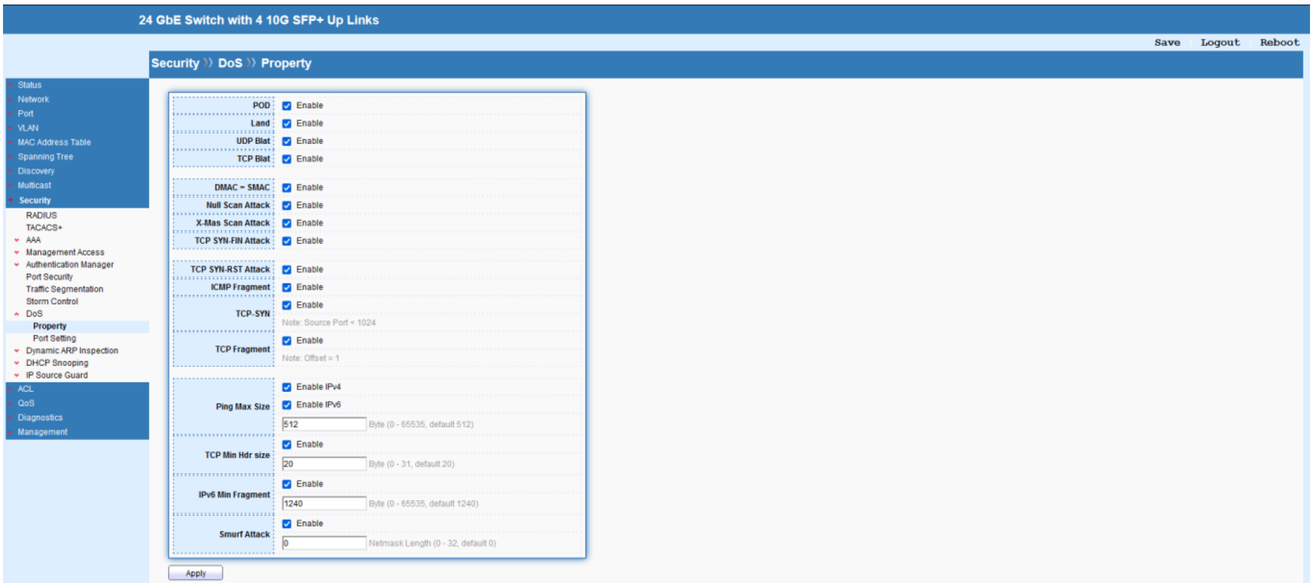
11.8 DoS

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.

11.8.1 Property

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



POD ☑ Enable

Land ☑ Enable

UDP Blat ☑ Enable

TCP Blat ☑ Enable

DMAC = SMAC ☑ Enable

Null Scan Attack ☑ Enable

X-Mas Scan Attack ☑ Enable

TCP SYN-FIN Attack ☑ Enable

TCP SYN-RST Attack ☑ Enable

ICMP Fragment ☑ Enable

TCP-SYN ☑ Enable
Note: Source Port < 1024

TCP Fragment ☑ Enable
Note: Offset = 1

Ping Max Size ☑ Enable IPv4 ☑ Enable IPv6
512 Byte (0 - 65535, default 512)

TCP Min Hdr size ☑ Enable
20 Byte (0 - 31, default 20)

IPv6 Min Fragment ☑ Enable
1240 Byte (0 - 65535, default 1240)

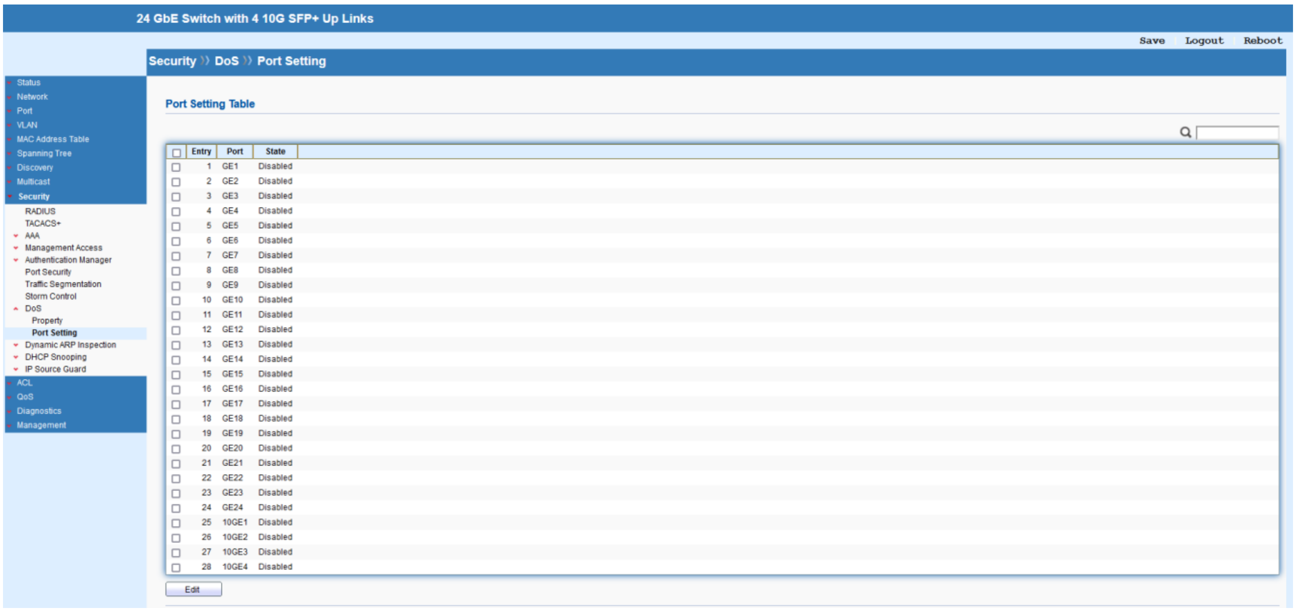
Smurf Attack ☑ Enable
0 Netmask Length (0 - 32, default 0)

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.

11.8.2 Port Setting

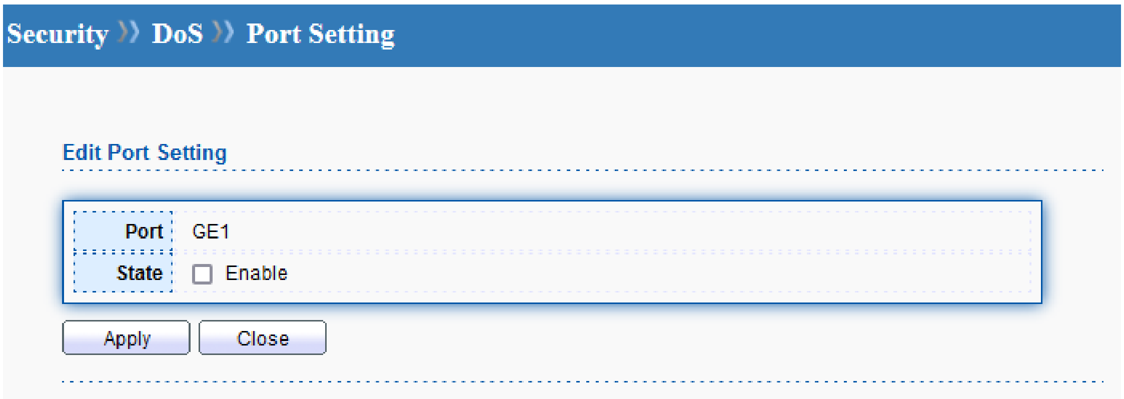
This page allows to configure and display the state of DoS protection for interfaces.



Port Setting Table

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

Item	Description
Edit	Edit the settings of selected port.



Port: GE1

State: □ Enable

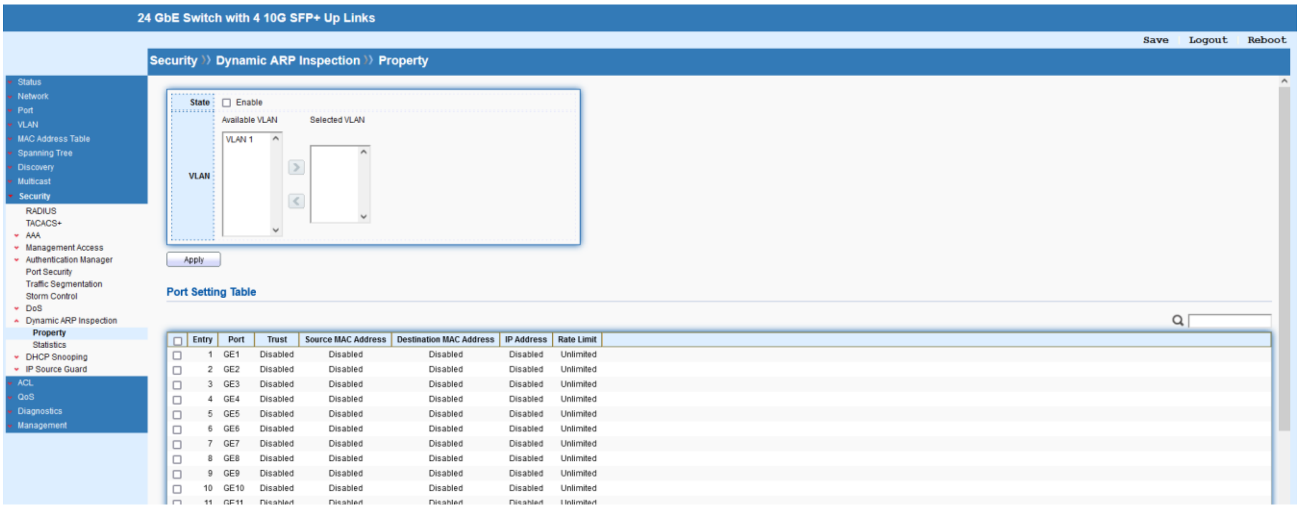
Item	Description
Port	The index number of selected port.
State	Enable or disable the DoS protection on the selected port(s)
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

11.9 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.

11.9.1 Property

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



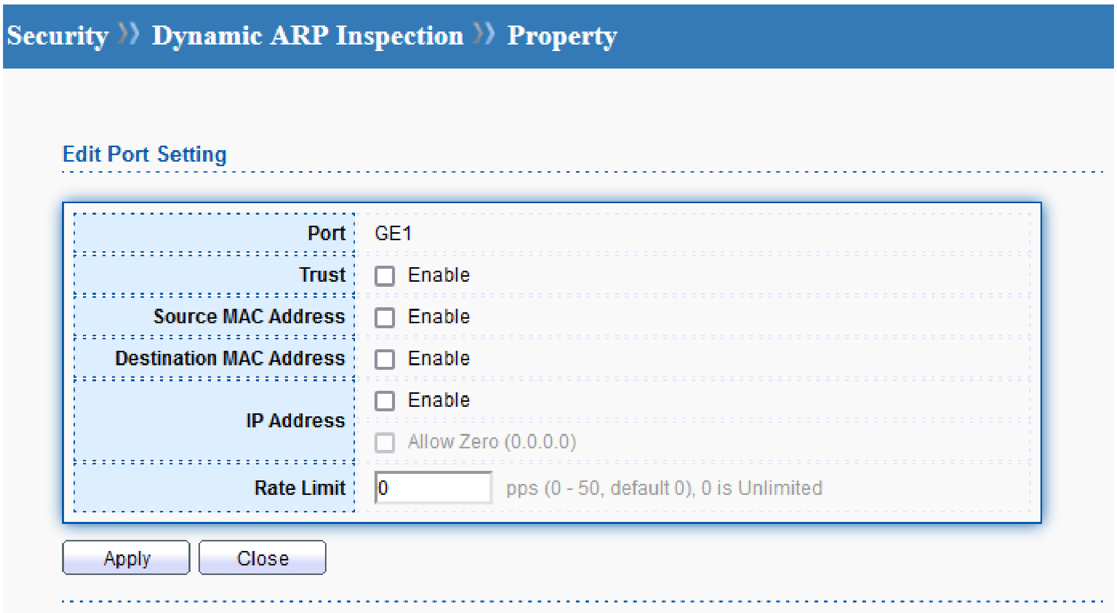
State: □ Enable

VLAN: Available VLAN: VLAN 1 / Selected VLAN:

□	Entry	Port	Trust	Source MAC Address	Destination MAC Address	IP Address	Rate Limit
□	1	GE1	Disabled	Disabled	Disabled	Disabled	Unlimited
□	2	GE2	Disabled	Disabled	Disabled	Disabled	Unlimited
□	3	GE3	Disabled	Disabled	Disabled	Disabled	Unlimited
□	4	GE4	Disabled	Disabled	Disabled	Disabled	Unlimited
□	5	GE5	Disabled	Disabled	Disabled	Disabled	Unlimited
□	6	GE6	Disabled	Disabled	Disabled	Disabled	Unlimited
□	7	GE7	Disabled	Disabled	Disabled	Disabled	Unlimited
□	8	GE8	Disabled	Disabled	Disabled	Disabled	Unlimited
□	9	GE9	Disabled	Disabled	Disabled	Disabled	Unlimited
□	10	GE10	Disabled	Disabled	Disabled	Disabled	Unlimited
□	11	GE11	Disabled	Disabled	Disabled	Disabled	Unlimited

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.



Security » Dynamic ARP Inspection » Property

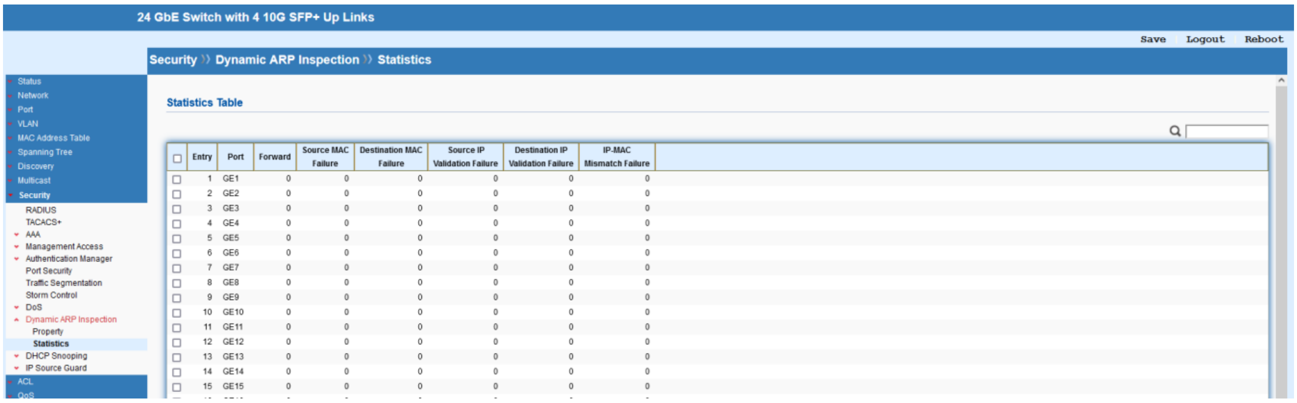
Edit Port Setting

Port	GE1
Trust	□ Enable
Source MAC Address	□ Enable
Destination MAC Address	□ Enable
IP Address	□ Enable □ Allow Zero (0.0.0.0)
Rate Limit	0 pps (0 - 50, default 0), 0 is Unlimited

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.

11.9.2 Statistics

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



Statistics Table

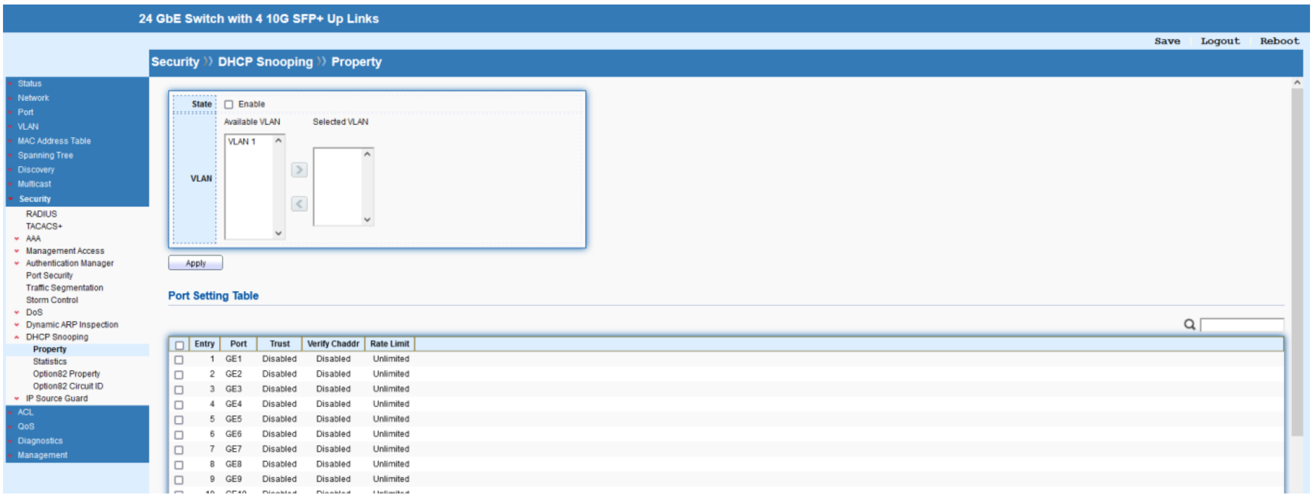
□	Entry	Port	Forward	Source MAC Failure	Destination MAC Failure	Source IP Validation Failure	Destination IP Validation Failure	IP-MAC Mismatch Failure
□	1	GE1	0	0	0	0	0	0
□	2	GE2	0	0	0	0	0	0
□	3	GE3	0	0	0	0	0	0
□	4	GE4	0	0	0	0	0	0
□	5	GE5	0	0	0	0	0	0
□	6	GE6	0	0	0	0	0	0
□	7	GE7	0	0	0	0	0	0
□	8	GE8	0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

11.10 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.

11.10.1 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.



State □ Enable

VLAN: Available VLAN: VLAN 1; Selected VLAN:

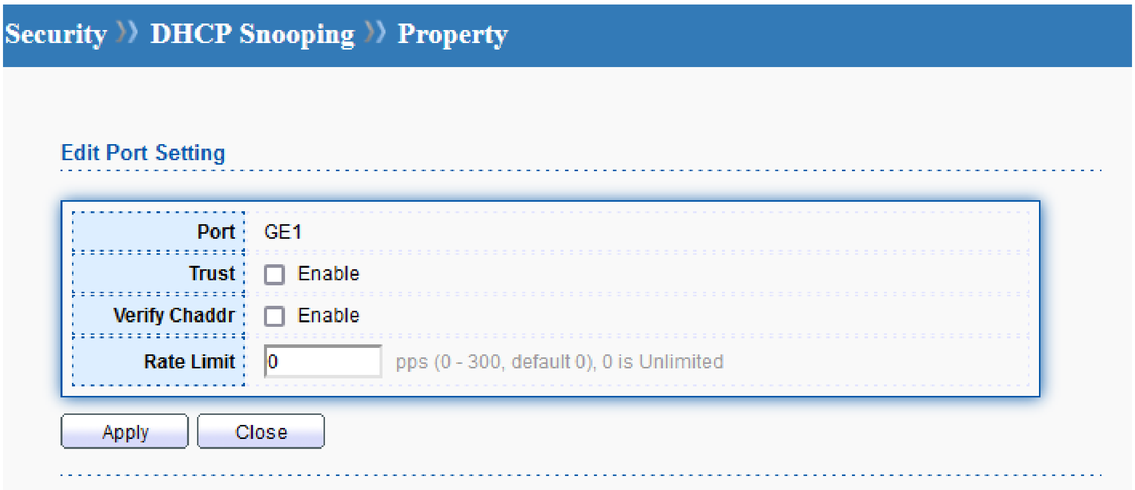
Apply

Port Setting Table

□	Entry	Port	Trust	Verify Chaddr	Rate Limit
□	1	GE1	Disabled	Disabled	Unlimited
□	2	GE2	Disabled	Disabled	Unlimited
□	3	GE3	Disabled	Disabled	Unlimited
□	4	GE4	Disabled	Disabled	Unlimited
□	5	GE5	Disabled	Disabled	Unlimited
□	6	GE6	Disabled	Disabled	Unlimited
□	7	GE7	Disabled	Disabled	Unlimited
□	8	GE8	Disabled	Disabled	Unlimited
□	9	GE9	Disabled	Disabled	Unlimited

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.



Security » DHCP Snooping » Property

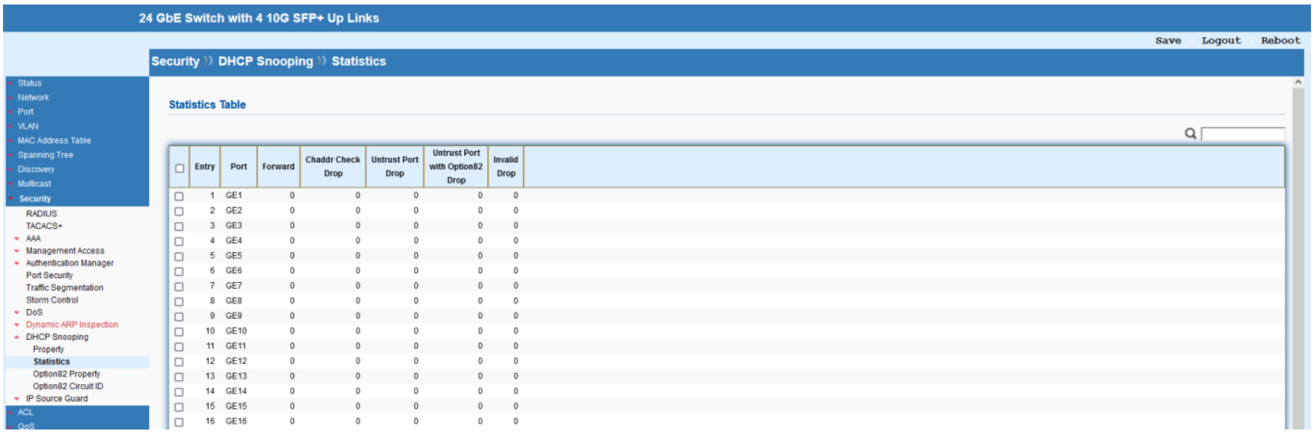
Edit Port Setting

Port	GE1
Trust	□ Enable
Verify Chaddr	□ Enable
Rate Limit	0 pps (0 - 300, default 0), 0 is Unlimited

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.

11.10.2 Statistics

This page displays all statistics recorded by DHCP snooping function.

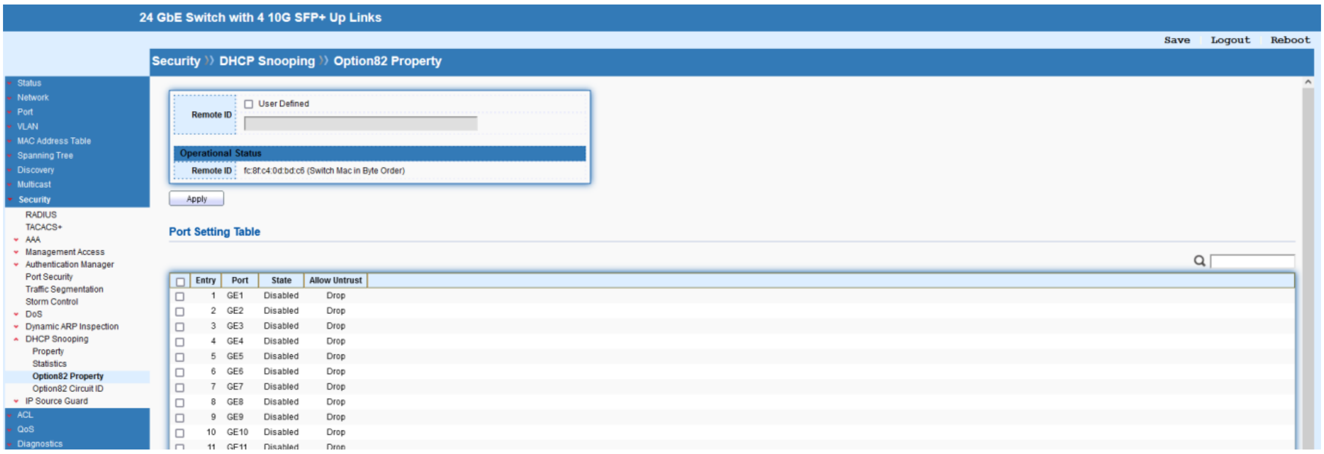


Statistics Table

☐	Entry	Port	Forward	Chaddr Check Drop	Untrust Port Drop	Untrust Port with Option82 Drop	Invalid Drop
☐	1	GE1	0	0	0	0	0
☐	2	GE2	0	0	0	0	0
☐	3	GE3	0	0	0	0	0
☐	4	GE4	0	0	0	0	0
☐	5	GE5	0	0	0	0	0
☐	6	GE6	0	0	0	0	0
☐	7	GE7	0	0	0	0	0
☐	8	GE8	0	0	0	0	0
☐	9	GE9	0	0	0	0	0
☐	10	GE10	0	0	0	0	0
☐	11	GE11	0	0	0	0	0
☐	12	GE12	0	0	0	0	0
☐	13	GE13	0	0	0	0	0
☐	14	GE14	0	0	0	0	0
☐	15	GE15	0	0	0	0	0
☐	16	GE16	0	0	0	0	0

11.10.3 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



Remote ID: ☐ User Defined

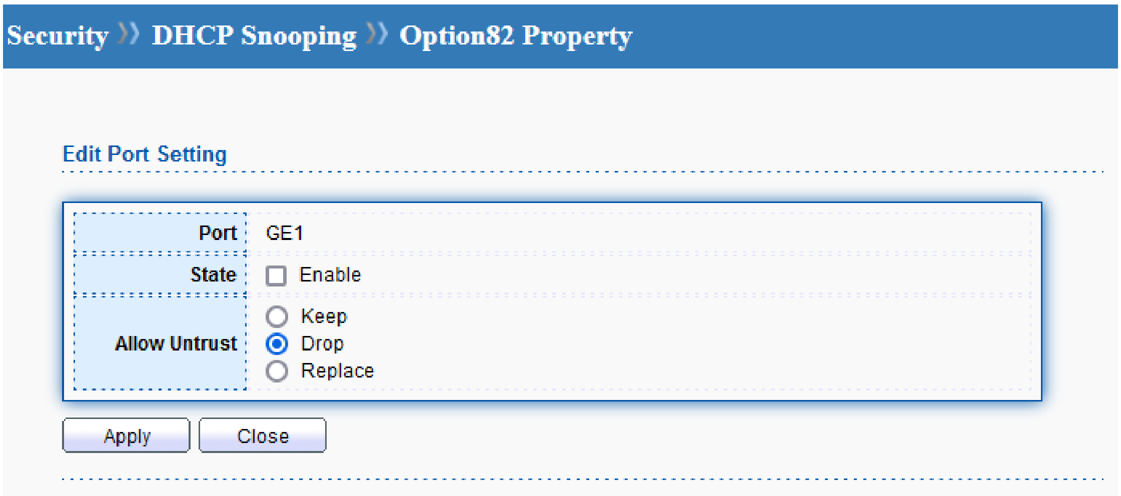
Operational Status

Remote ID: fc:8f:c4:0d:bd:c6 (Switch Mac in Byte Order)

Port Setting Table

☐	Entry	Port	State	Allow Untrust
☐	1	GE1	Disabled	Drop
☐	2	GE2	Disabled	Drop
☐	3	GE3	Disabled	Drop
☐	4	GE4	Disabled	Drop
☐	5	GE5	Disabled	Drop
☐	6	GE6	Disabled	Drop
☐	7	GE7	Disabled	Drop
☐	8	GE8	Disabled	Drop
☐	9	GE9	Disabled	Drop
☐	10	GE10	Disabled	Drop
☐	11	GE11	Disabled	Drop

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.



Security » DHCP Snooping » Option82 Property

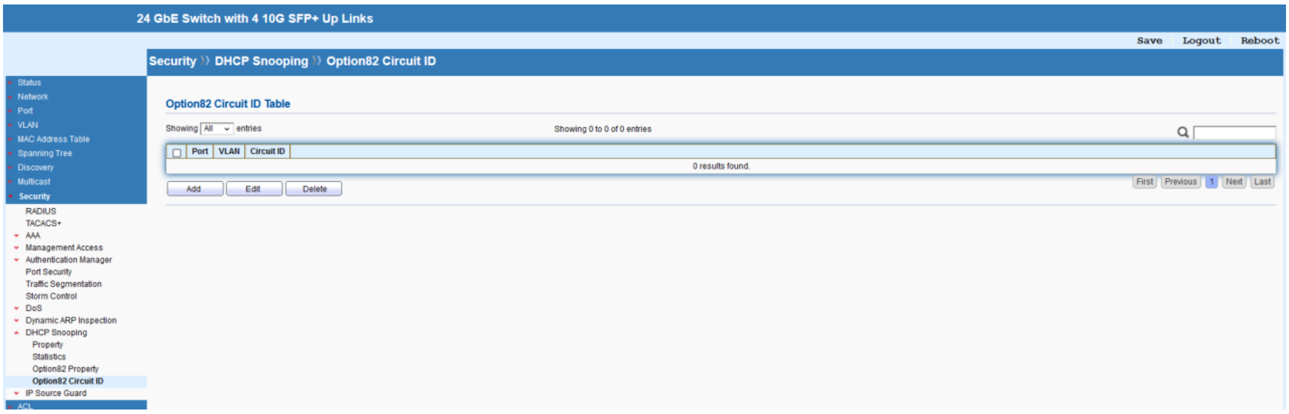
Edit Port Setting

Port	GE1
State	□ Enable
Allow Untrust	○ Keep ● Drop ○ Replace

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. **Replace**: Packets will be replaced.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

11.10.4 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).



24 GbE Switch with 4 10G SFP+ Up Links

Security » DHCP Snooping » Option82 Circuit ID

Option82 Circuit ID Table

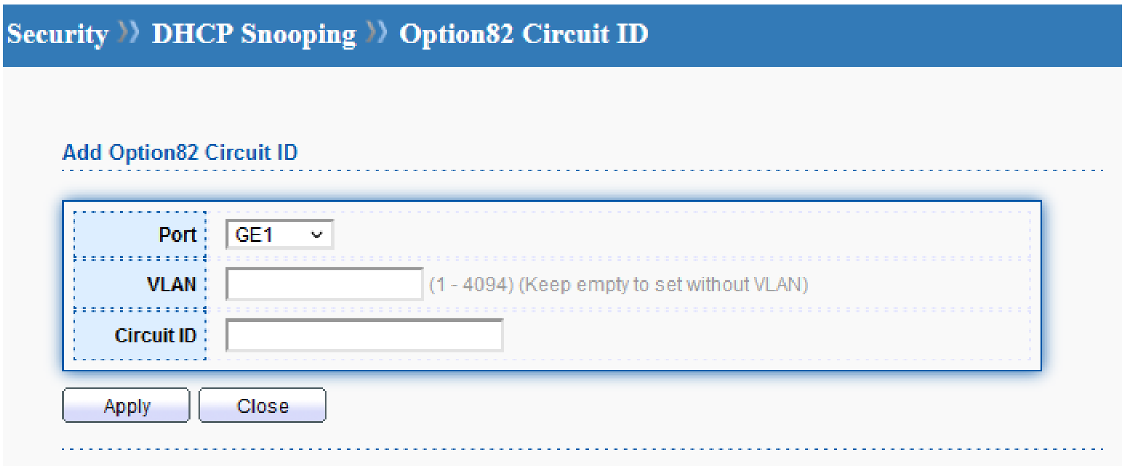
Showing All entries

Showing 0 to 0 of 0 entries

□	Port	VLAN	Circuit ID

0 results found.

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



Security >> DHCP Snooping >> Option82 Circuit ID

Add Option82 Circuit ID

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

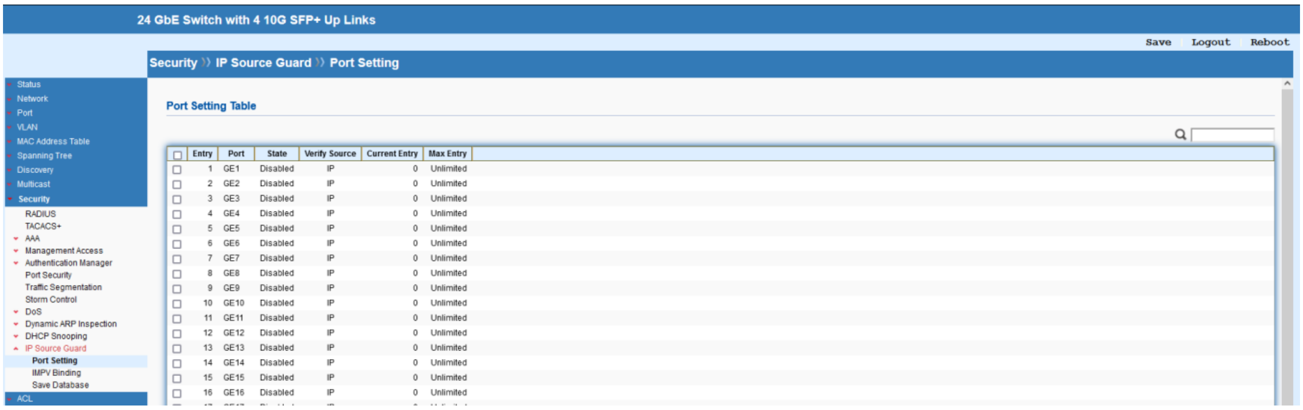
Item	Description
Port	Use the drop down list to select the port for applying DHCP snooping, Option82 Property function.
VLAN	Choose a number as VLAN ID which is easy to be identified for a packet containing with it. It is optional setting.
Circuit ID	Enter ASCII text string in the entry box. Later, any 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.

11.11 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.

11.11.1 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.

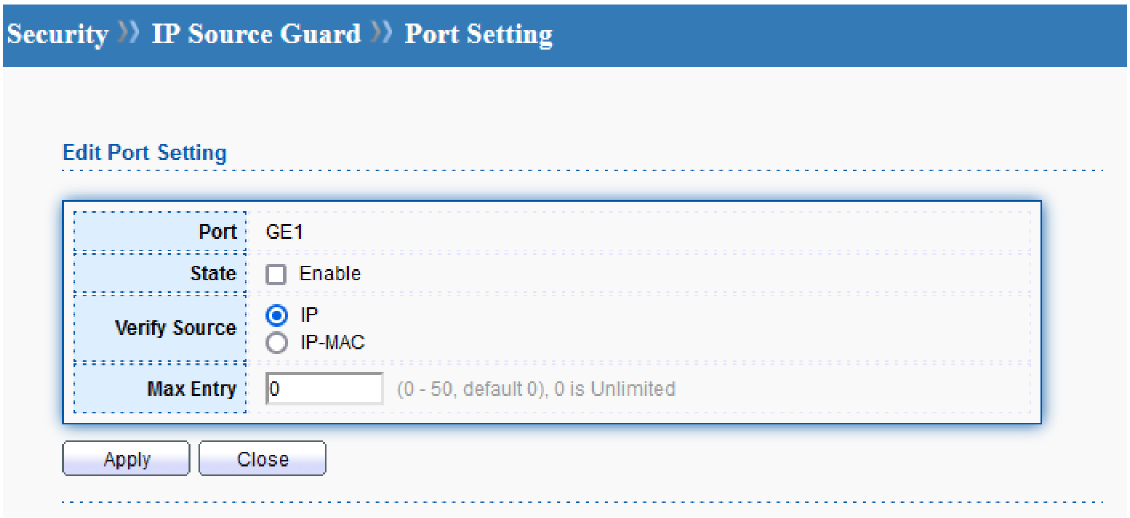


Security 》 IP Source Guard 》 Port Setting

Port Setting Table

□	Entry	Port	State	Verify Source	Current Entry	Max Entry
□	1	GE1	Disabled	IP	0	Unlimited
□	2	GE2	Disabled	IP	0	Unlimited
□	3	GE3	Disabled	IP	0	Unlimited
□	4	GE4	Disabled	IP	0	Unlimited
□	5	GE5	Disabled	IP	0	Unlimited
□	6	GE6	Disabled	IP	0	Unlimited
□	7	GE7	Disabled	IP	0	Unlimited
□	8	GE8	Disabled	IP	0	Unlimited
□	9	GE9	Disabled	IP	0	Unlimited
□	10	GE10	Disabled	IP	0	Unlimited
□	11	GE11	Disabled	IP	0	Unlimited
□	12	GE12	Disabled	IP	0	Unlimited
□	13	GE13	Disabled	IP	0	Unlimited
□	14	GE14	Disabled	IP	0	Unlimited
□	15	GE15	Disabled	IP	0	Unlimited
□	16	GE16	Disabled	IP	0	Unlimited

Item	Description
Edit	Edit the settings of selected port.



Security 》 IP Source Guard 》 Port Setting

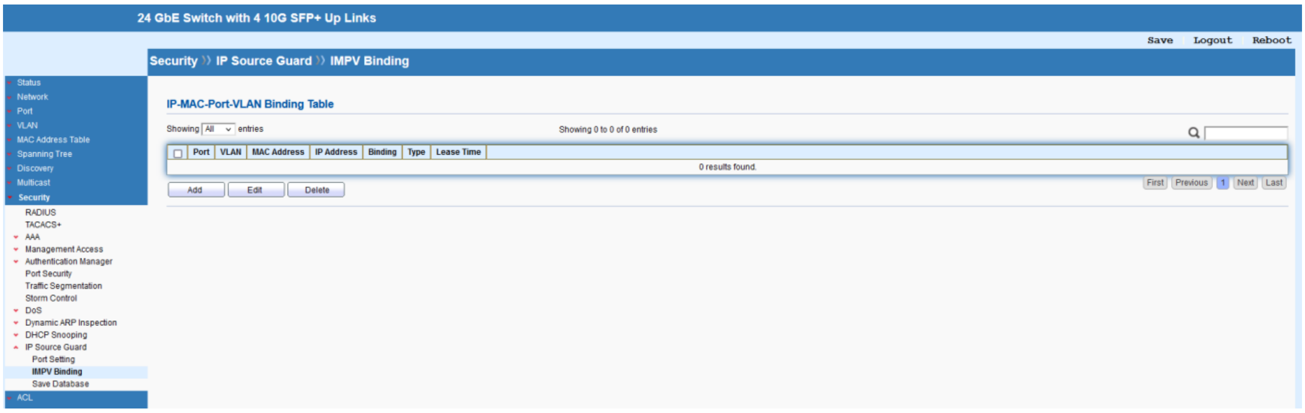
Edit Port Setting

Port	GE1
State	□ Enable
Verify Source	● IP ○ IP-MAC
Max Entry	0 (0 - 50, default 0), 0 is Unlimited

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.

11.11.2 IMPV Binding

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



Security » IP Source Guard » IMPV Binding

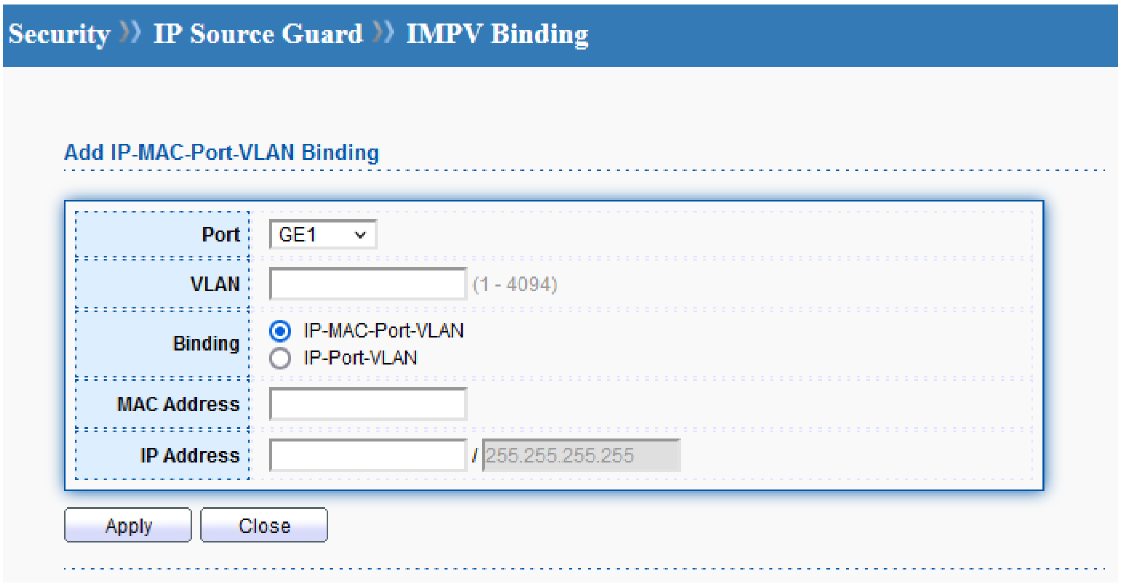
IP-MAC-Port-VLAN Binding Table

Showing All entries

Showing 0 to 0 of 0 entries

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

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



Security » IP Source Guard » IMPV Binding

Add IP-MAC-Port-VLAN Binding

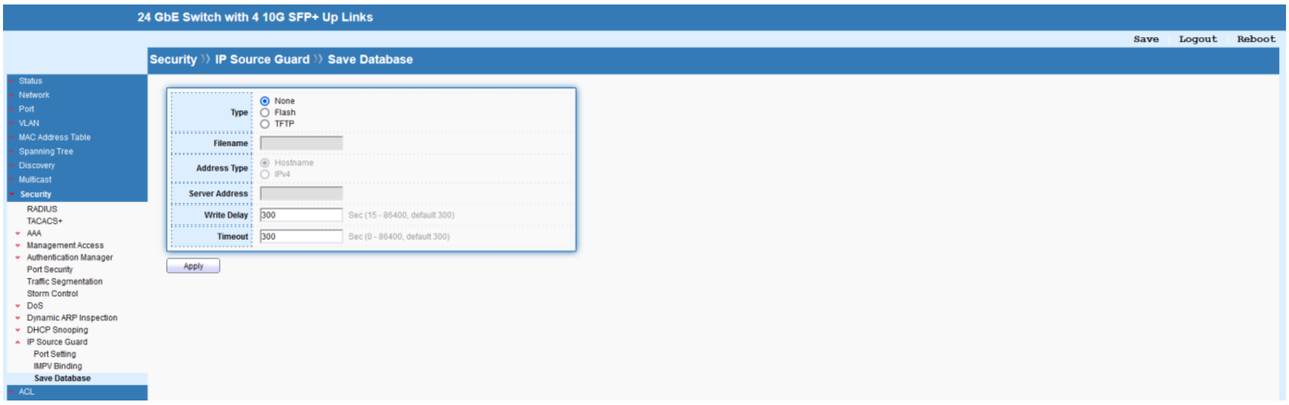
Port	GE1
VLAN	(1 - 4094)
Binding	● IP-MAC-Port-VLAN ○ IP-Port-VLAN
MAC Address	
IP Address	/ 255.255.255.255

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.

11.11.3 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.



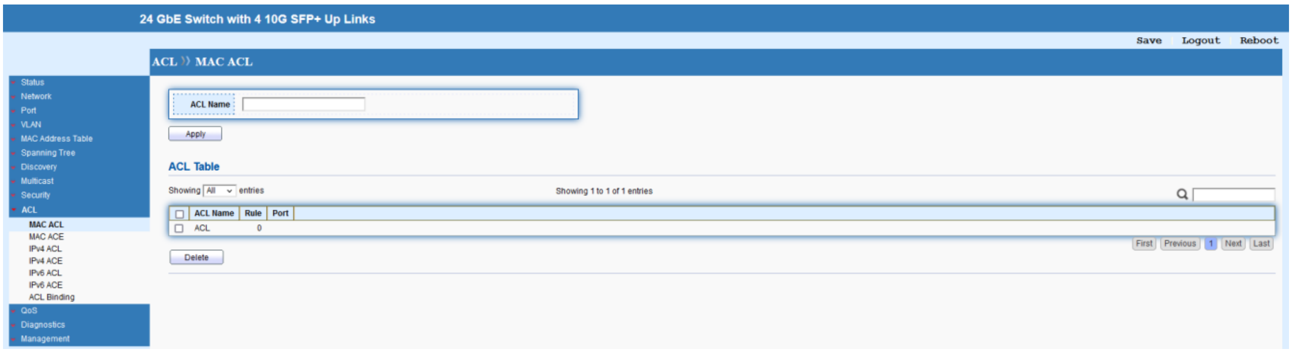
Type	● None ○ Flash ○ TFTP
Filename	
Address Type	● Hostname ○ IPv4
Server Address	
Write Delay	300 Sec (15 - 86400, default 300)
Timeout	300 Sec (0 - 86400, default 300)

12 ACL

The Access Control List (ACL) is a sequential list of permit 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 rules match, the frame is accepted.

12.1 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.



ACL Name

ACL Table

Showing All entries

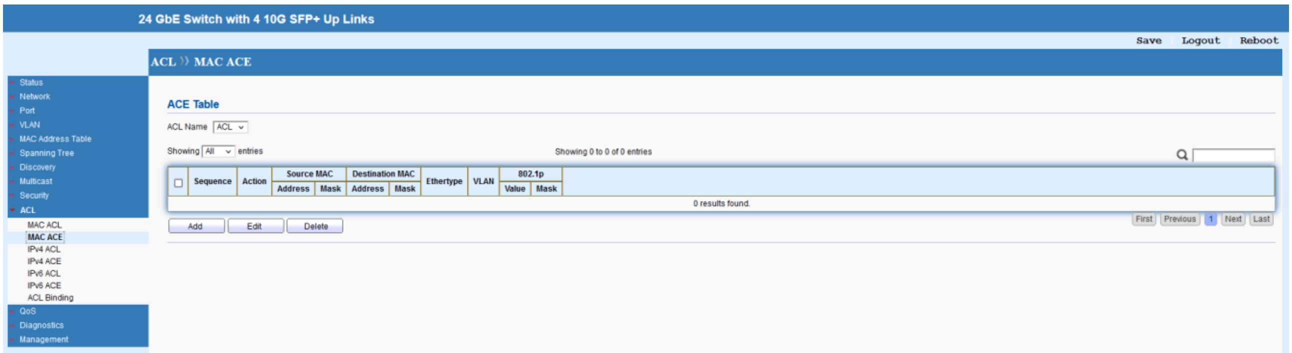
Showing 1 to 1 of 1 entries

□	ACL Name	Rule	Port
□	ACL	0	

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

12.2 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.



ACE Table

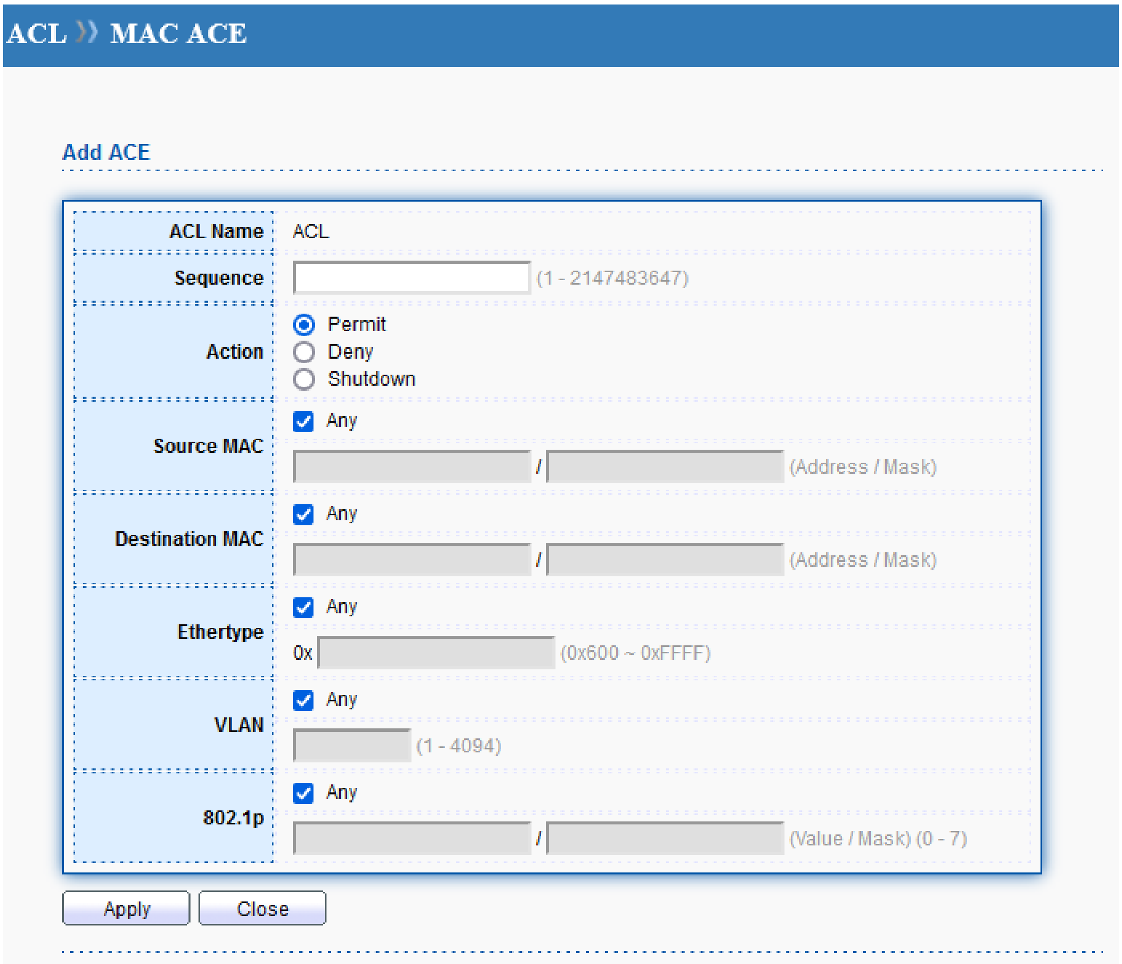
ACL Name ACL

Showing All entries

Showing 0 to 0 of 0 entries

□	Sequence	Action	Source MAC		Destination MAC		Ethertype	VLAN	802.1p	
			Address	Mask	Address	Mask			Value	Mask
0 results found.										

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


ACL » MAC ACE

Add ACE

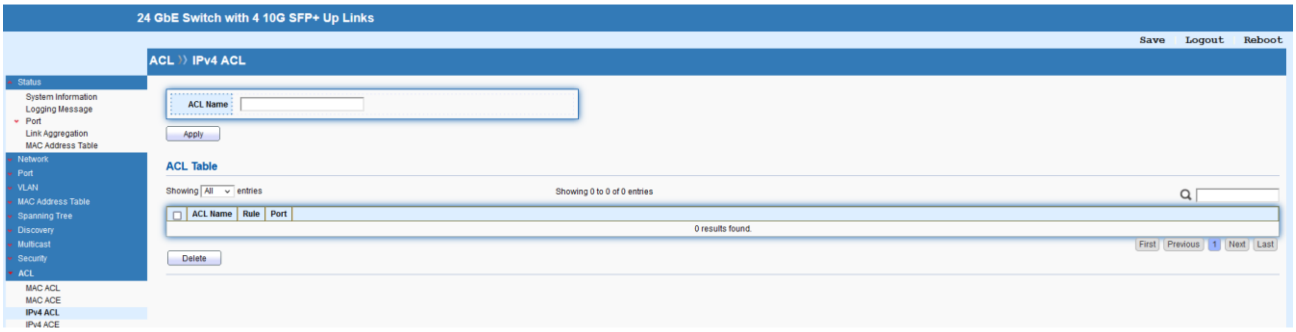
ACL Name	ACL
Sequence	(1 - 2147483647)
Action	● Permit ○ Deny ○ Shutdown
Source MAC	☑ Any / (Address / Mask)
Destination MAC	☑ Any / (Address / Mask)
Ethertype	☑ Any 0x (0x600 ~ 0xFFFF)
VLAN	☑ Any (1 - 4094)
802.1p	☑ Any / (Value / Mask) (0 - 7)

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.

12.3 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.



ACL Name

ACL Table

Showing All entries

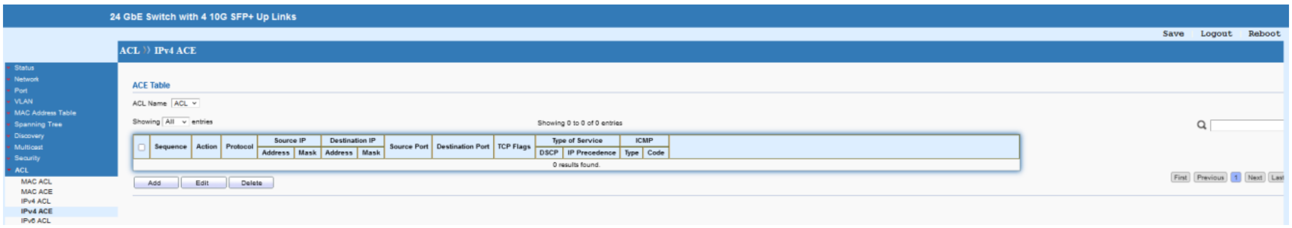
Showing 0 to 0 of 0 entries

□	ACL Name	Rule	Port
0 results found.			

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

12.4 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.



ACL 》 IPv4 ACE

ACE Table

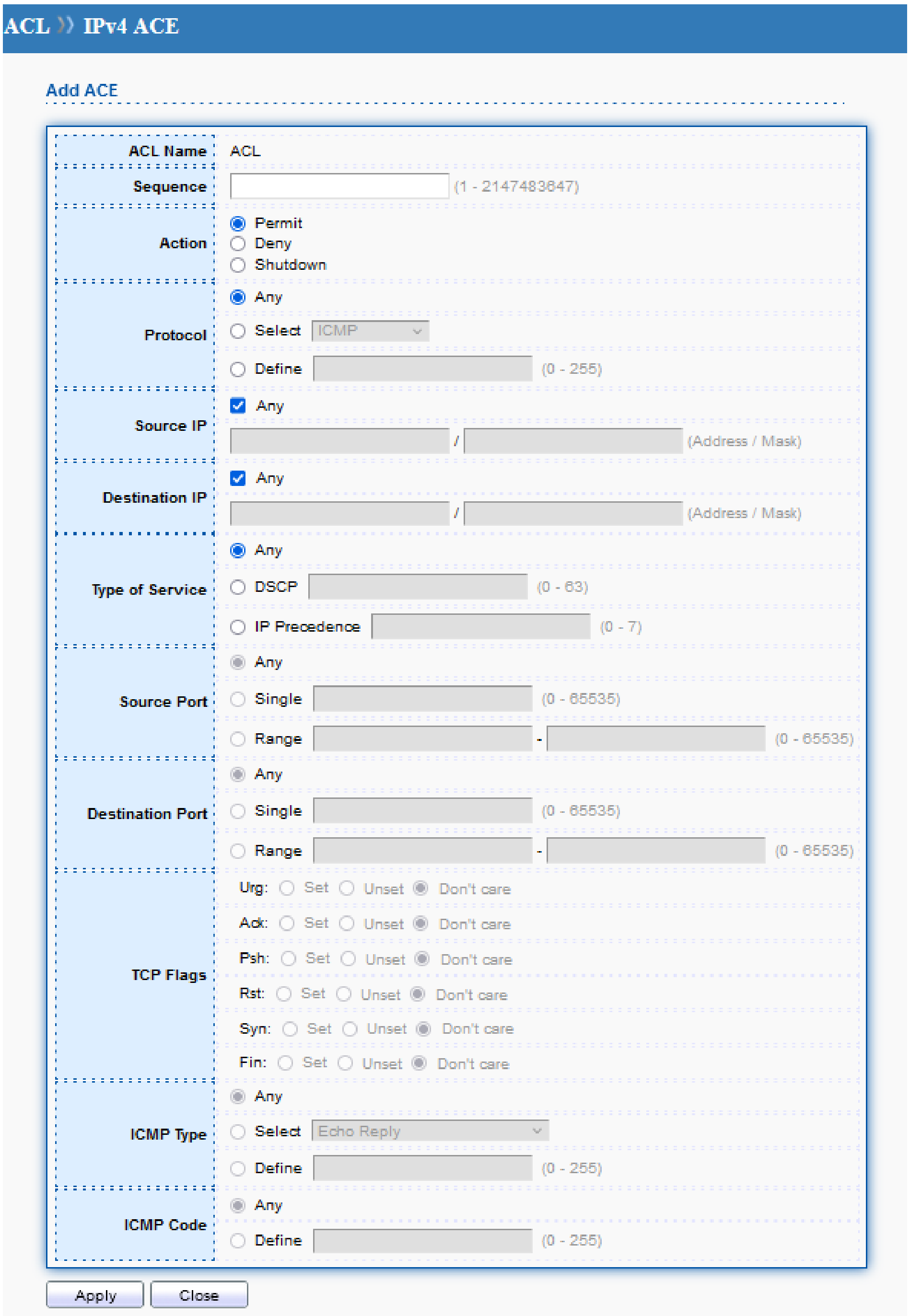
ACL Name: ACL

Showing All entries

Showing 0 to 0 of 0 entries

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

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



ACL » IPv4 ACE

Add ACE

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

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.

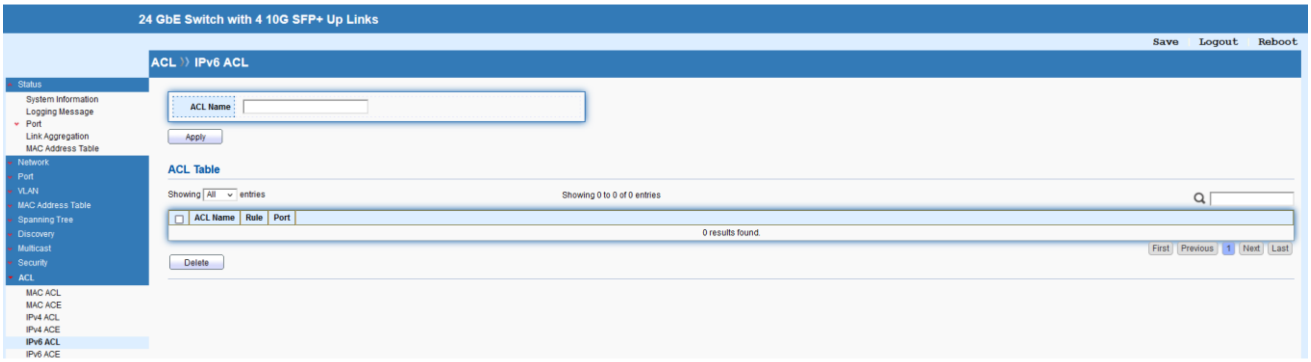
	Permit or deny the packets into switch core, or shutdown the port for stopping further transmission.
Protocol	Specify the protocol for filtering. **Any**: All packets will be filtered. **Select**: Choose one of the protocol (e.g., ICMP, IP in IP, TCP, EGP, IGP…) from the drop down list. Packets passing 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.

12.5 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.



ACL Name

ACL Table

Showing All entries   Showing 0 to 0 of 0 entries

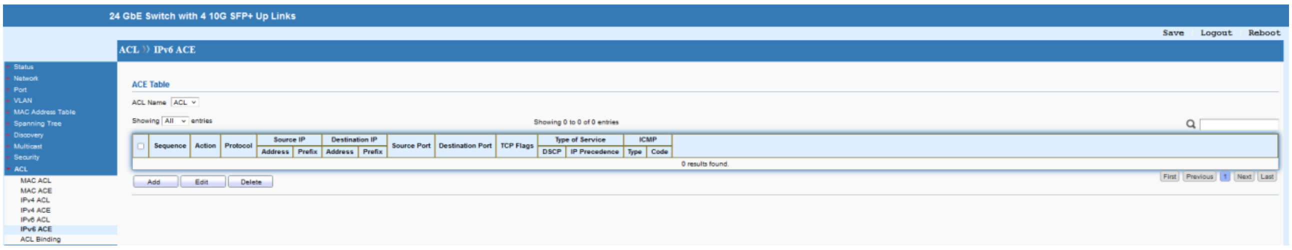
□	ACL Name	Rule	Port

0 results found.

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

12.6 IPv6 ACE

This page allows to create ACE based on IPv6 address.



ACE Table

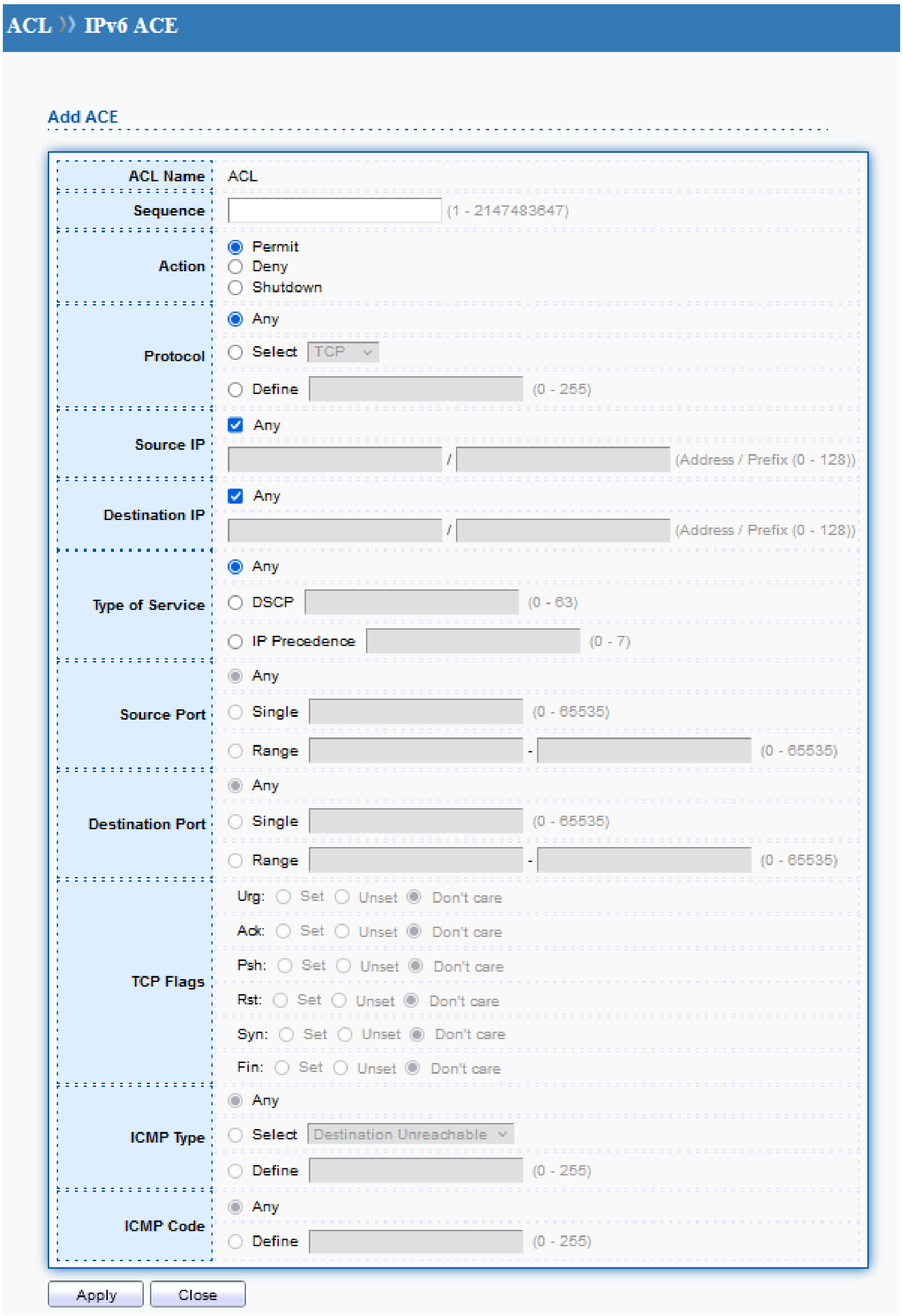
ACL Name: ACL

Showing All entries

Showing 0 to 0 of 0 entries

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

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



ACL » IPv6 ACE

Add ACE

ACL Name	ACL
Sequence	(1 - 2147483647)
Action	● Permit ○ Deny ○ Shutdown
Protocol	● Any ○ Select TCP ○ Define (0 - 255)
Source IP	☑ Any / (Address / Prefix (0 - 128))
Destination IP	☑ Any / (Address / Prefix (0 - 128))
Type of Service	● Any ○ DSCP (0 - 63) ○ IP Precedence (0 - 7)
Source Port	● Any ○ Single (0 - 65535) ○ Range - (0 - 65535)
Destination Port	● Any ○ Single (0 - 65535) ○ Range - (0 - 65535)
TCP Flags	Urg: ○ Set ○ Unset ● Don't care Ack: ○ Set ○ Unset ● Don't care Psh: ○ Set ○ Unset ● Don't care Rst: ○ Set ○ Unset ● Don't care Syn: ○ Set ○ Unset ● Don't care Fin: ○ Set ○ Unset ● Don't care
ICMP Type	● Any ○ Select Destination Unreachable ○ Define (0 - 255)
ICMP Code	● Any ○ Define (0 - 255)

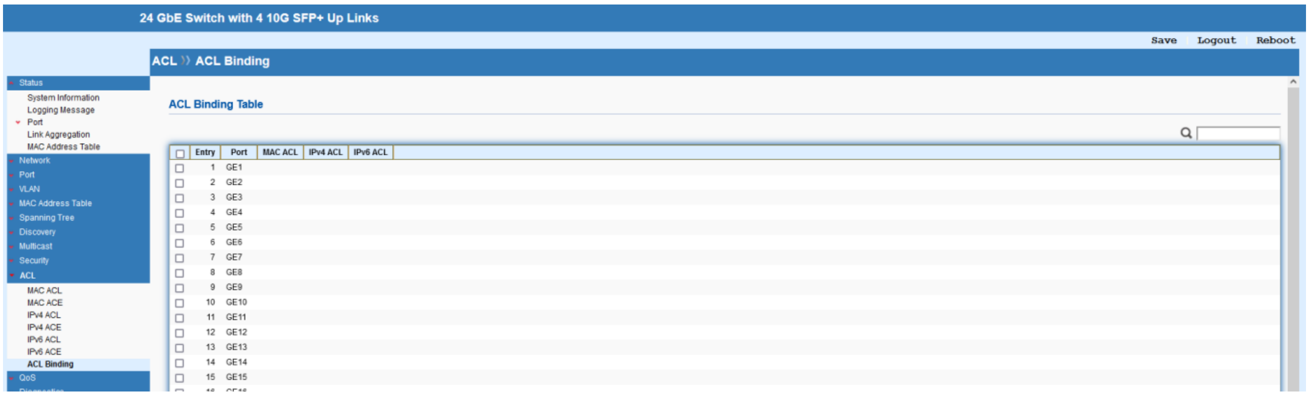
Item	Description
ACL Name	The name of selected ACL profile.
Sequence	Assign a sequence number to this ACE. The sequence is used to identify which one of ACEs in an ACL is firstly used to match ingress packets. The switch port bound with an ACL use the contained ACE rules, start with the one with lower 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.

12.7 ACL Binding

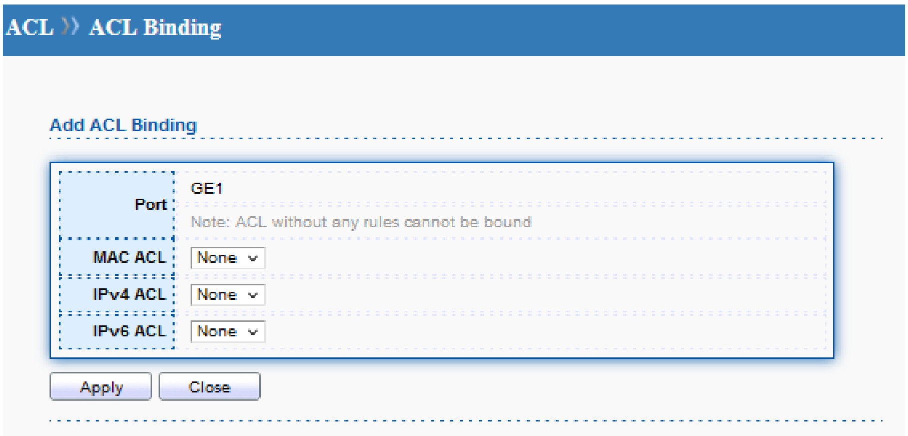
This section allows to bind Access Control Lists created in previous section to an interface (physical port or aggregation). A physical port can only be bound with one of the IPv4 and IPv6 ACL, not both.



ACL Binding Table

□	Entry	Port	MAC ACL	IPv4 ACL	IPv6 ACL
□	1	GE1			
□	2	GE2			
□	3	GE3			
□	4	GE4			
□	5	GE5			
□	6	GE6			
□	7	GE7			
□	8	GE8			
□	9	GE9			
□	10	GE10			
□	11	GE11			
□	12	GE12			
□	13	GE13			
□	14	GE14			
□	15	GE15			

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.



ACL » ACL Binding

Add ACL Binding

Port	GE1 Note: ACL without any rules cannot be bound
MAC ACL	None
IPv4 ACL	None
IPv6 ACL	None

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.

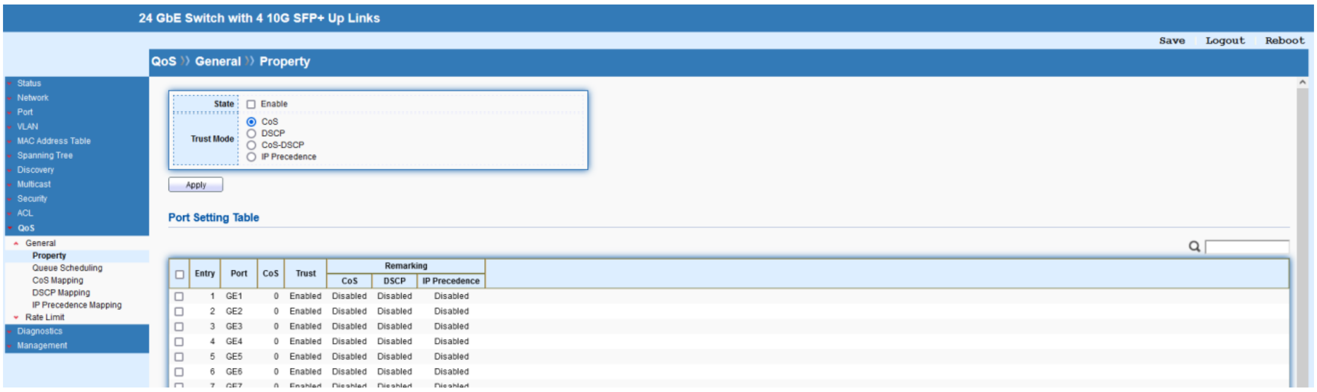
13 QoS

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.

13.1 General

13.1.1 Property

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



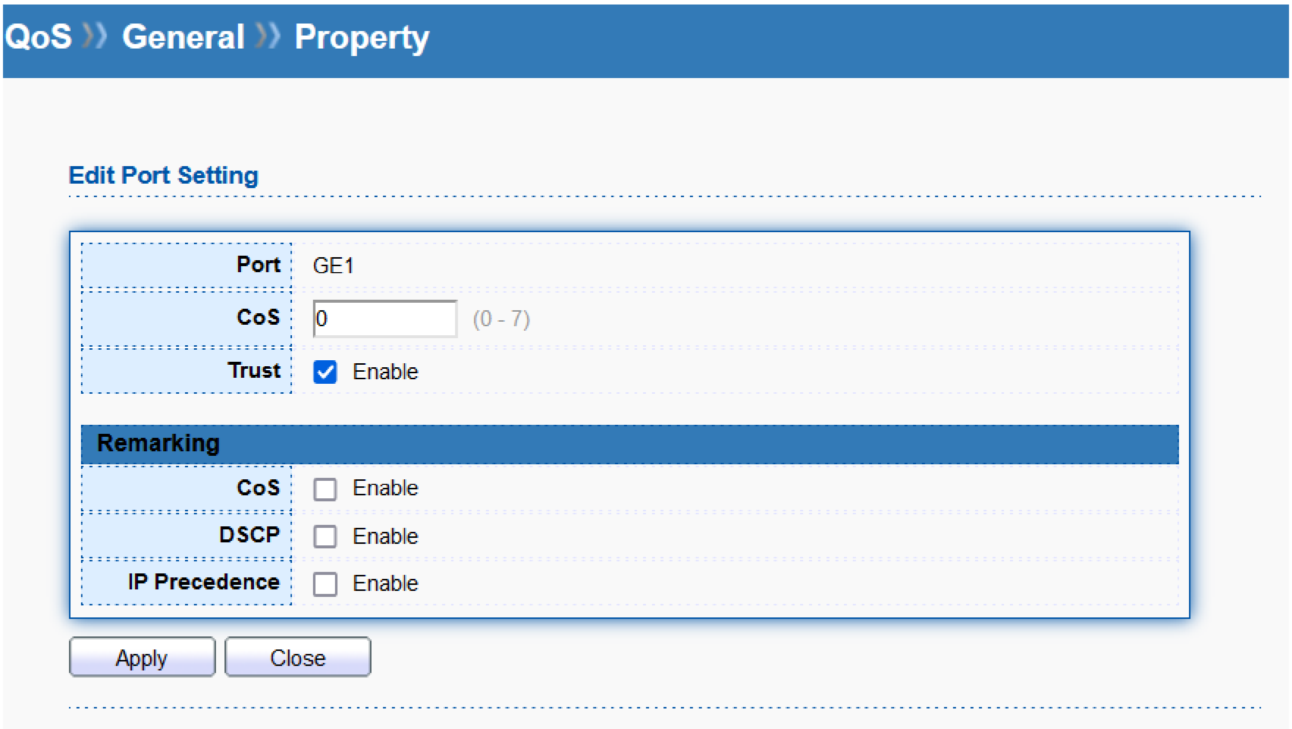
QoS » General » Property

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

Port Setting Table

□	Entry	Port	CoS	Trust	Remarking		
					CoS	DSCP	IP Precedence
□	1	GE1	0	Enabled	Disabled	Disabled	Disabled
□	2	GE2	0	Enabled	Disabled	Disabled	Disabled
□	3	GE3	0	Enabled	Disabled	Disabled	Disabled
□	4	GE4	0	Enabled	Disabled	Disabled	Disabled
□	5	GE5	0	Enabled	Disabled	Disabled	Disabled
□	6	GE6	0	Enabled	Disabled	Disabled	Disabled
□	7	GE7	0	Enabled	Disabled	Disabled	Disabled

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).



QoS » General » Property

Edit Port Setting

Port	GE1
CoS	0 (0 - 7)
Trust	☑ Enable

Remarking

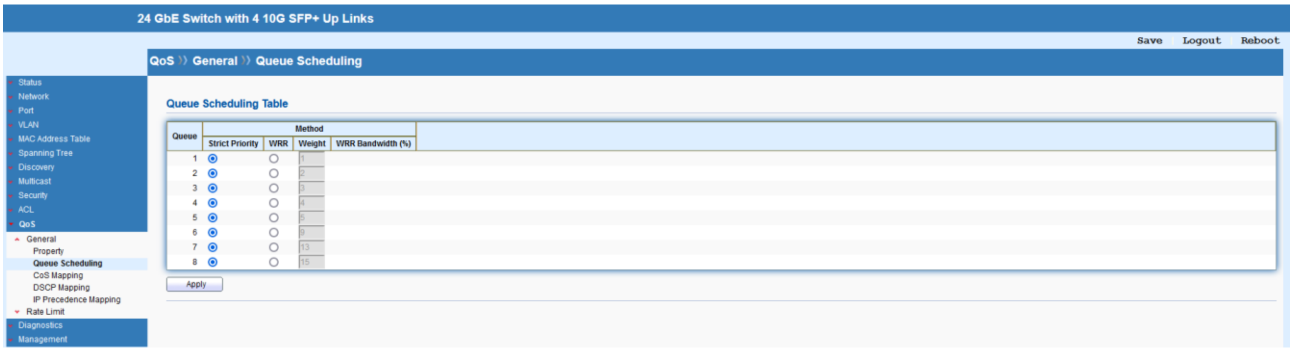
CoS	□ Enable
DSCP	□ Enable
IP Precedence	□ Enable

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.

13.1.2 Queue Scheduling

The Switch 850X-28 supports multiple queues for each interface. The higher numbered queue represents the higher priority.



QoS » General » Queue Scheduling

Queue Scheduling Table

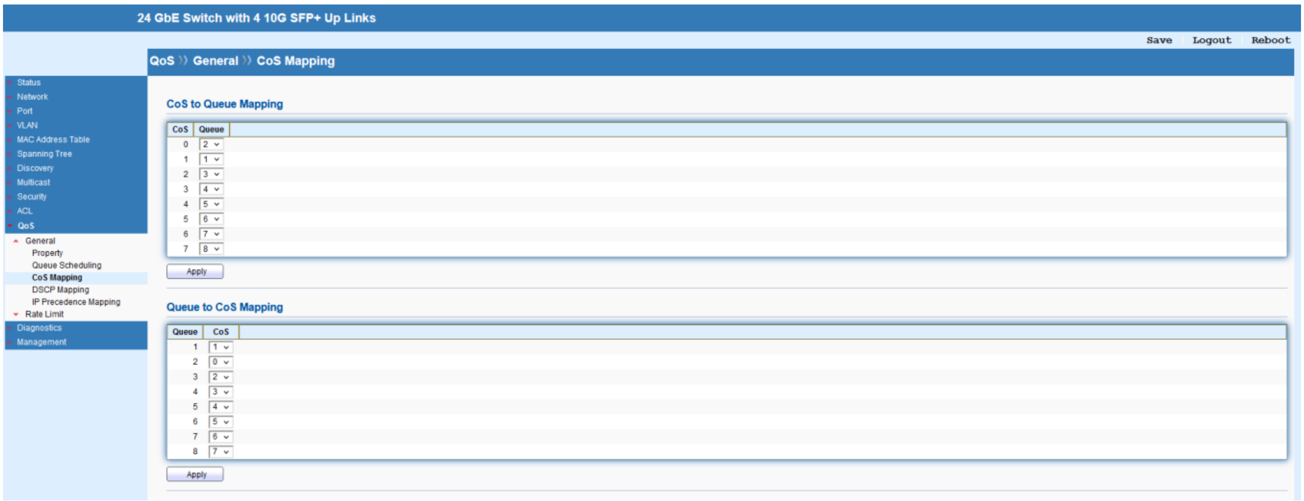
Queue	Method			
	Strict Priority	WRR	Weight	WRR Bandwidth (%)
1	●	○	1	
2	●	○	2	
3	●	○	3	
4	●	○	4	
5	●	○	5	
6	●	○	9	
7	●	○	13	
8	●	○	15	

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.

13.1.3 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.



CoS to Queue Mapping

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

Apply

Queue to CoS Mapping

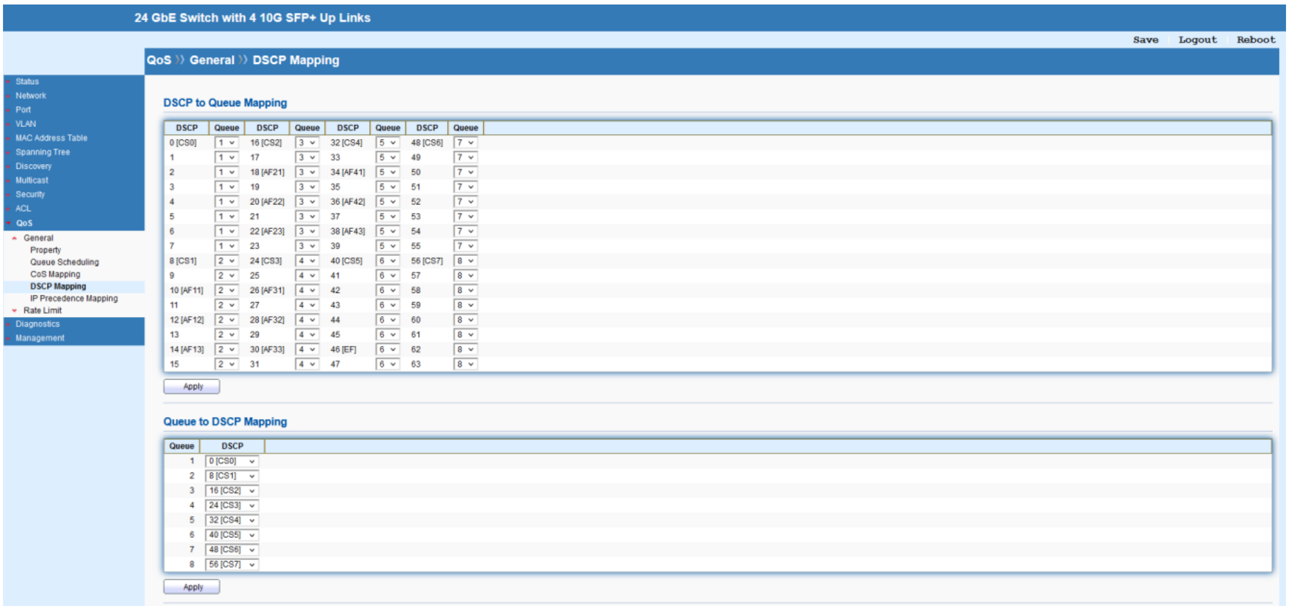
Queue	CoS
1	1
2	0
3	2
4	3
5	4
6	5
7	6
8	7

Apply

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.

13.1.4 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.



DSCP to Queue Mapping

DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
0 [CS0]	1	16 [CS2]	3	32 [CS4]	5	48 [CS6]	7
1	1	17	3	33	5	49	7
2	1	18 [AF21]	3	34 [AF41]	5	50	7
3	1	19	3	35	5	51	7
4	1	20 [AF22]	3	36 [AF42]	5	52	7
5	1	21	3	37	5	53	7
6	1	22 [AF23]	3	38 [AF43]	5	54	7
7	1	23	3	39	5	55	7
8 [CS1]	2	24 [CS3]	4	40 [CS5]	6	56 [CS7]	8
9	2	25	4	41	6	57	8
10 [AF11]	2	26 [AF31]	4	42	6	58	8
11	2	27	4	43	6	59	8
12 [AF12]	2	28 [AF32]	4	44	6	60	8
13	2	29	4	45	6	61	8
14 [AF13]	2	30 [AF33]	4	46 [EF]	6	62	8
15	2	31	4	47	6	63	8

Apply

Queue to DSCP Mapping

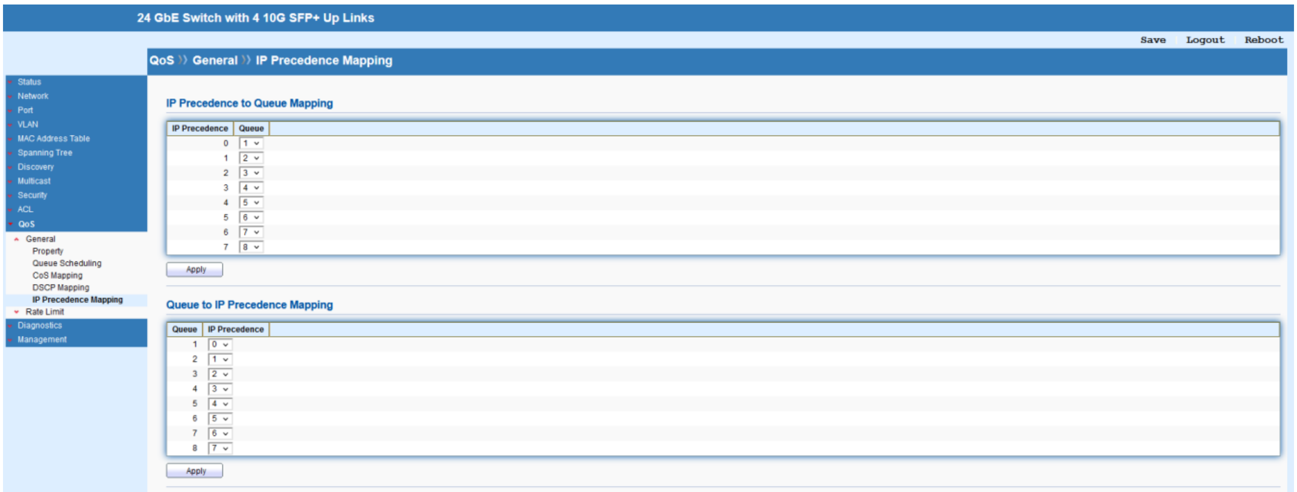
Queue	DSCP
1	0 [CS0]
2	8 [CS1]
3	16 [CS2]
4	24 [CS3]
5	32 [CS4]
6	40 [CS5]
7	48 [CS6]
8	56 [CS7]

Apply

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.

13.1.5 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.



IP Precedence to Queue Mapping

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

Queue to IP Precedence Mapping

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

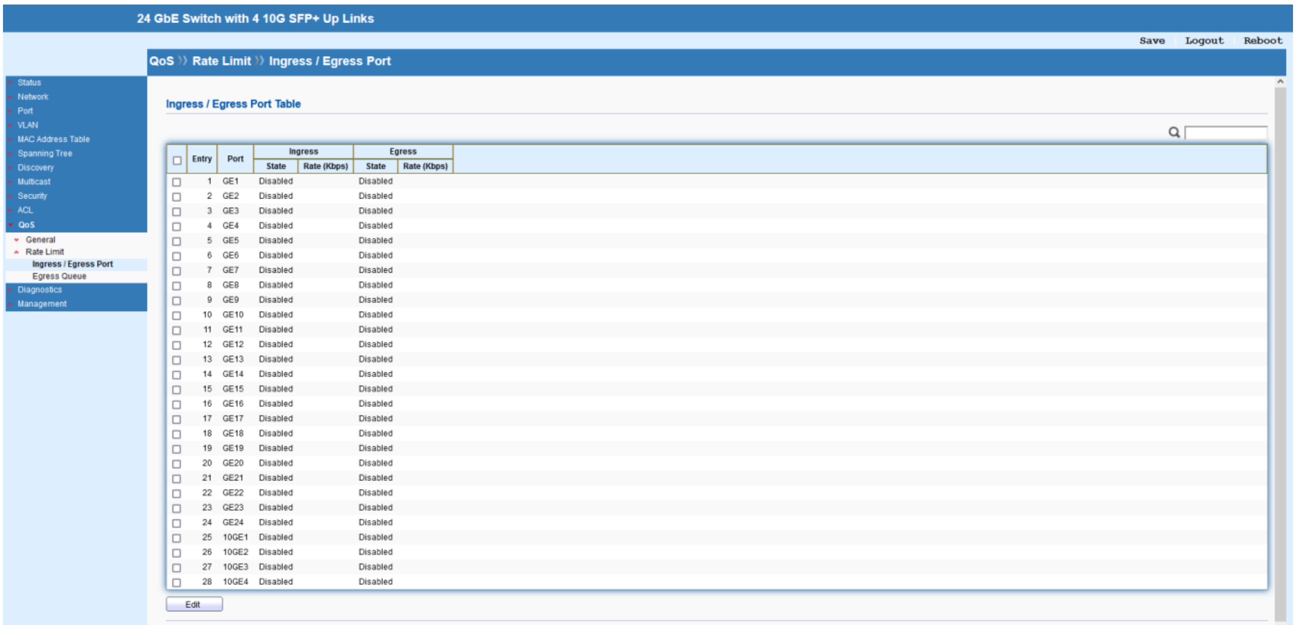
Item	Description
IP Precedence to Queue Mapping	
IP Precedence	Display the IP Precedence value (0 to 7).
Queue	Define the queue ID (level 1 to 8) for different IP Precedence values.
Apply	Apply the settings to the switch.
Queue to IP Precedence Mapping	
Queue	Display the queue ID (level 1 to 8) for different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

13.2 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.

13.2.1 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.

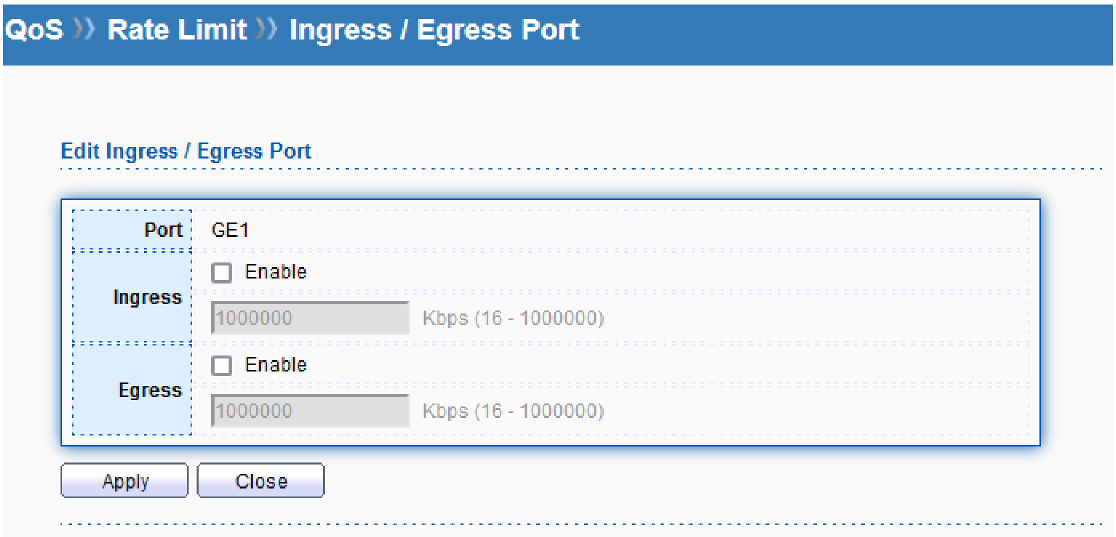


QoS » Rate Limit » Ingress / Egress Port

Ingress / Egress Port Table

□	Entry	Port	Ingress		Egress	
			State	Rate (Kbps)	State	Rate (Kbps)
□	1	GE1	Disabled		Disabled	
□	2	GE2	Disabled		Disabled	
□	3	GE3	Disabled		Disabled	
□	4	GE4	Disabled		Disabled	
□	5	GE5	Disabled		Disabled	
□	6	GE6	Disabled		Disabled	
□	7	GE7	Disabled		Disabled	
□	8	GE8	Disabled		Disabled	
□	9	GE9	Disabled		Disabled	
□	10	GE10	Disabled		Disabled	
□	11	GE11	Disabled		Disabled	
□	12	GE12	Disabled		Disabled	
□	13	GE13	Disabled		Disabled	
□	14	GE14	Disabled		Disabled	
□	15	GE15	Disabled		Disabled	
□	16	GE16	Disabled		Disabled	
□	17	GE17	Disabled		Disabled	
□	18	GE18	Disabled		Disabled	
□	19	GE19	Disabled		Disabled	
□	20	GE20	Disabled		Disabled	
□	21	GE21	Disabled		Disabled	
□	22	GE22	Disabled		Disabled	
□	23	GE23	Disabled		Disabled	
□	24	GE24	Disabled		Disabled	
□	25	10GE1	Disabled		Disabled	
□	26	10GE2	Disabled		Disabled	
□	27	10GE3	Disabled		Disabled	
□	28	10GE4	Disabled		Disabled	

Item	Description
Edit	Edit the selected port(s).



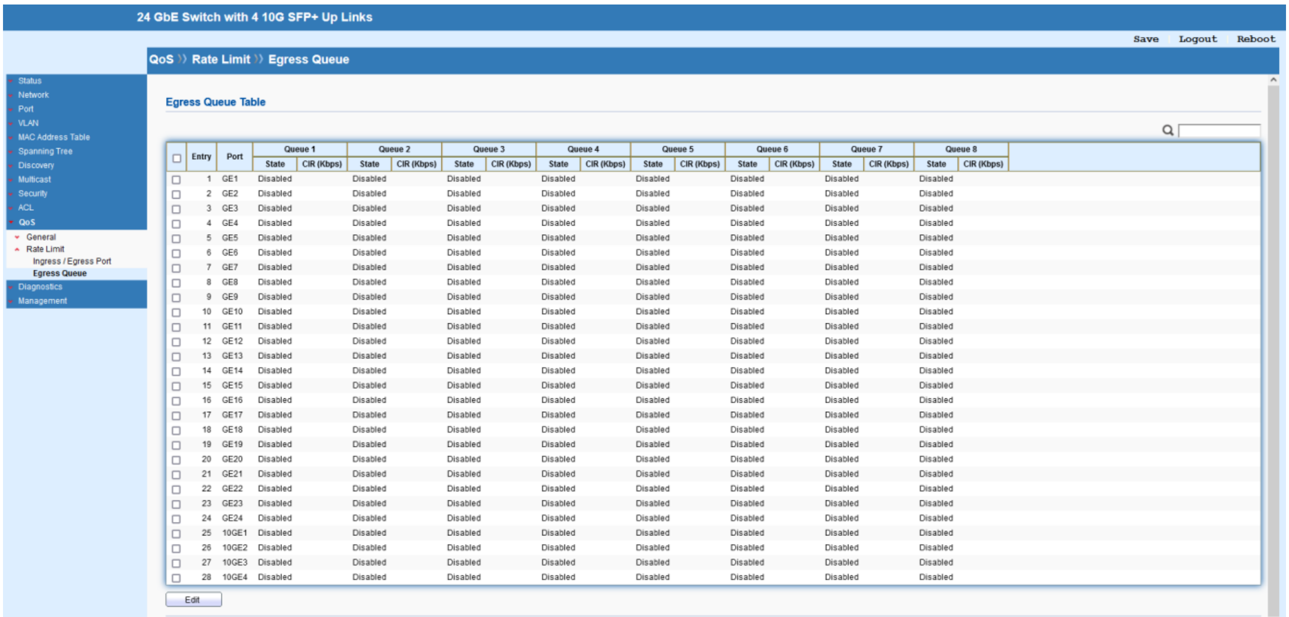
QoS » Rate Limit » Ingress / Egress Port

Edit Ingress / Egress Port

Port	GE1
Ingress	□ Enable 1000000 Kbps (16 - 1000000)
Egress	□ Enable 1000000 Kbps (16 - 1000000)

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.

13.2.2 Egress Queue

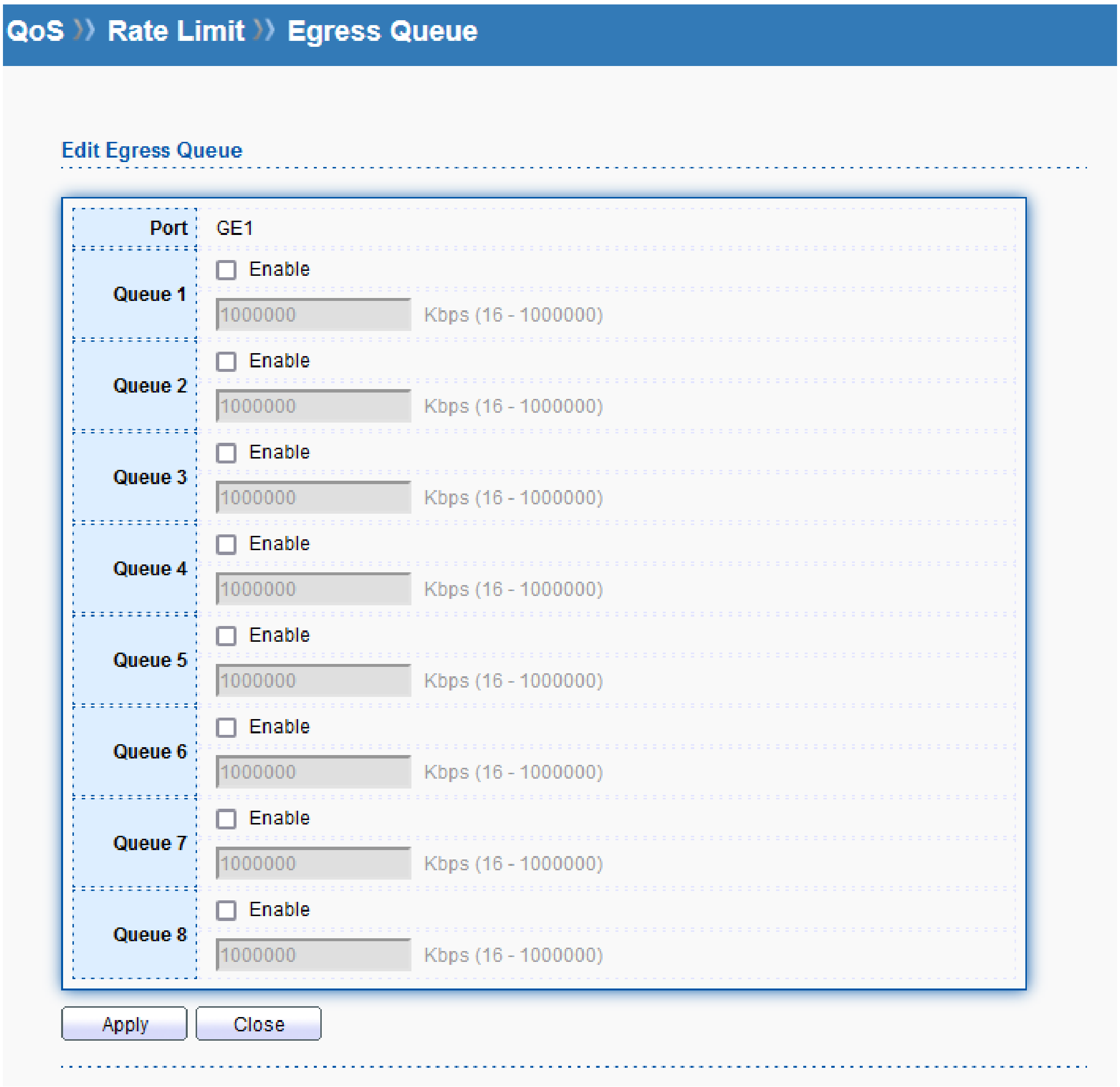


QoS 〉〉 Rate Limit 〉〉 Egress Queue

Egress Queue Table

□	Entry	Port	Queue 1		Queue 2		Queue 3		Queue 4		Queue 5		Queue 6		Queue 7		Queue 8	
			State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)	State	CIR (Kbps)
□	1	GE1	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	2	GE2	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	3	GE3	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	4	GE4	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	5	GE5	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	6	GE6	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	7	GE7	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	8	GE8	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	9	GE9	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	10	GE10	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	11	GE11	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	12	GE12	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	13	GE13	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	14	GE14	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	15	GE15	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	16	GE16	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	17	GE17	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	18	GE18	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	19	GE19	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	20	GE20	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	21	GE21	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	22	GE22	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	23	GE23	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	24	GE24	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	25	10GE1	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	26	10GE2	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	27	10GE3	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	
□	28	10GE4	Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled		Disabled	

Item	Description
Edit	Edit the selected port(s).



QoS >> Rate Limit >> Egress Queue

Edit Egress Queue

Port	GE1
Queue 1	□ Enable 1000000 Kbps (16 - 1000000)
Queue 2	□ Enable 1000000 Kbps (16 - 1000000)
Queue 3	□ Enable 1000000 Kbps (16 - 1000000)
Queue 4	□ Enable 1000000 Kbps (16 - 1000000)
Queue 5	□ Enable 1000000 Kbps (16 - 1000000)
Queue 6	□ Enable 1000000 Kbps (16 - 1000000)
Queue 7	□ Enable 1000000 Kbps (16 - 1000000)
Queue 8	□ Enable 1000000 Kbps (16 - 1000000)

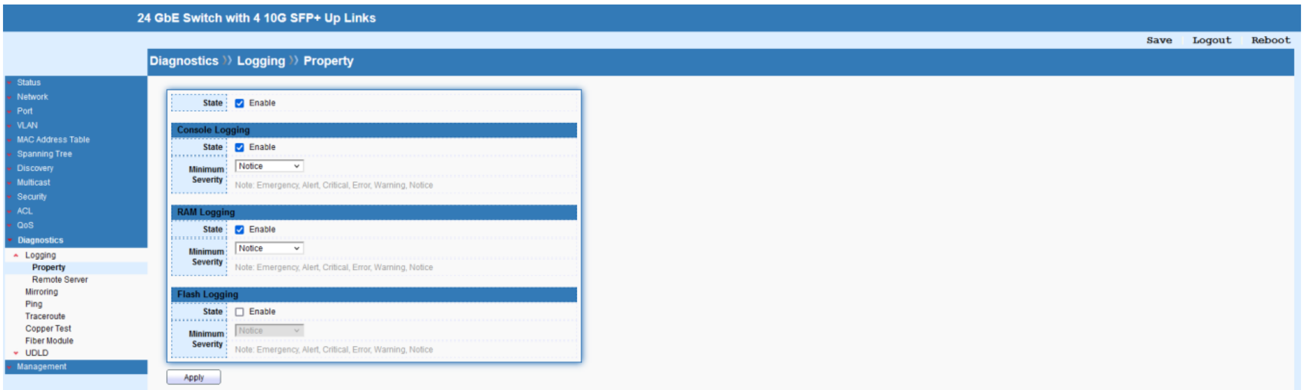
Item	Description
Port	The index number of selected port.
Queue (1~8)	Total eight queue rules. Enable or disable egress bandwidth control. Enter the rate value,<16-1000000>, unit:16 Kbps.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

14 Diagnostics

14.1 Logging

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

14.1.1 Property



State ☑ Enable

Console Logging

State ☑ Enable

Minimum Severity: Notice

Note: Emergency, Alert, Critical, Error, Warning, Notice

RAM Logging

State ☑ Enable

Minimum Severity: Notice

Note: Emergency, Alert, Critical, Error, Warning, Notice

Flash Logging

State ☐ Enable

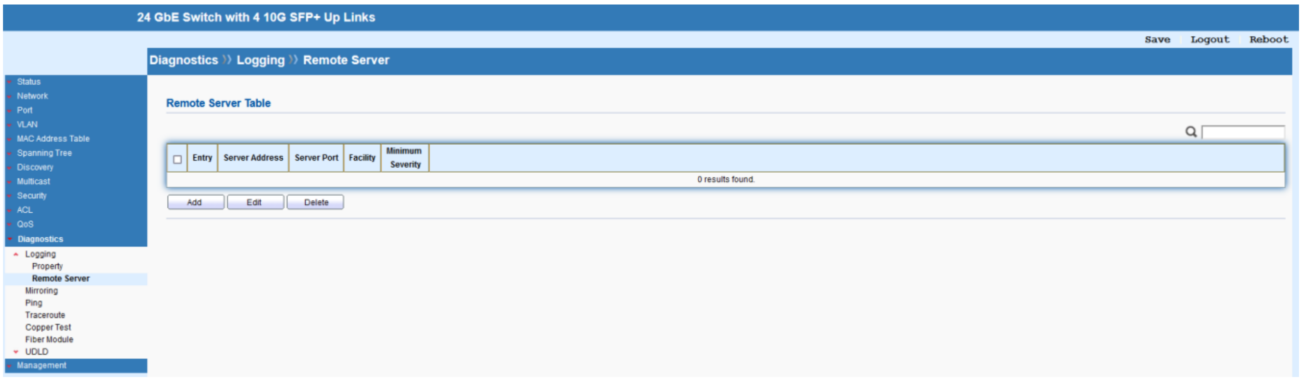
Minimum Severity: Notice

Note: Emergency, Alert, Critical, Error, Warning, Notice

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.

14.1.2 Remote Server

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



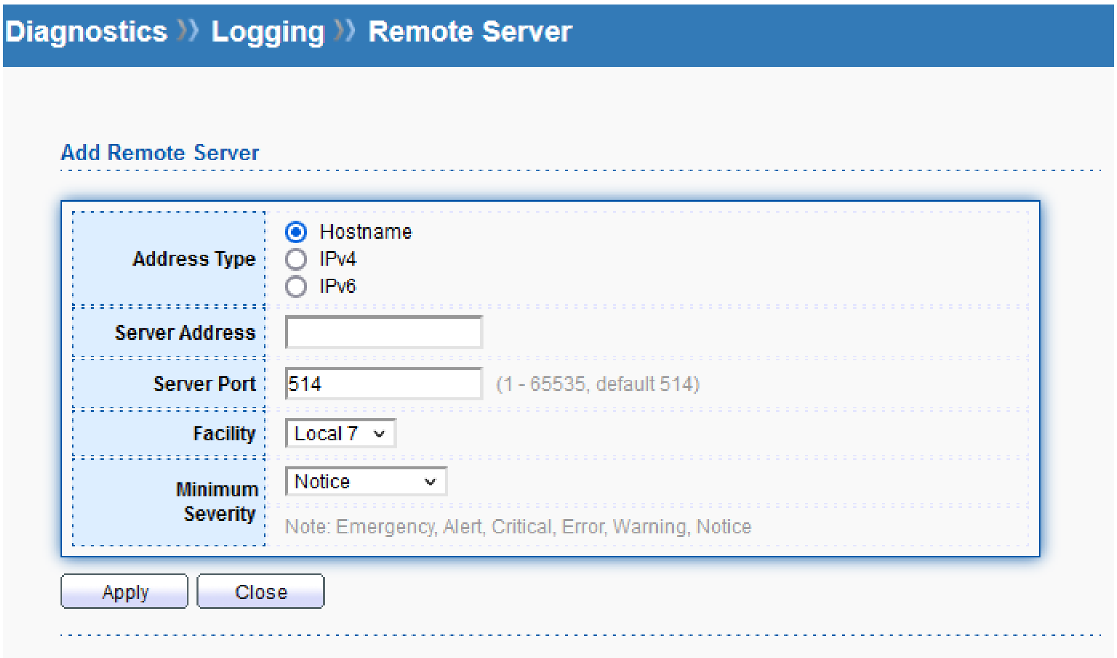
Diagnostics » Logging » Remote Server

Remote Server Table

□	Entry	Server Address	Server Port	Facility	Minimum Severity

0 results found.

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



Diagnostics » Logging » Remote Server

Add Remote Server

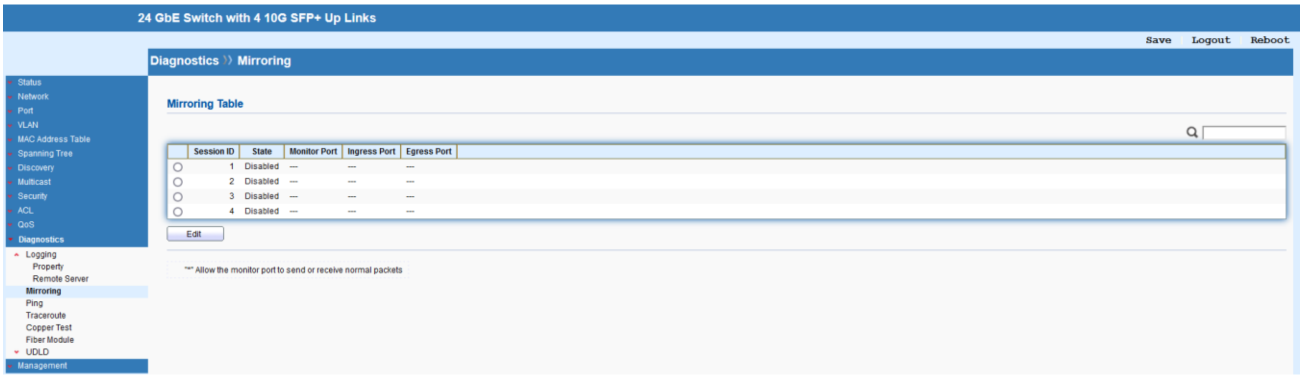
Address Type	● Hostname ○ IPv4 ○ IPv6
Server Address	
Server Port	514 (1 - 65535, default 514)
Facility	Local 7
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice

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.

14.2 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 convinent for system administrator to monitor / understand the traffic operation. Session ID 1 to 4 can be enabled simultaneously and operate independently.

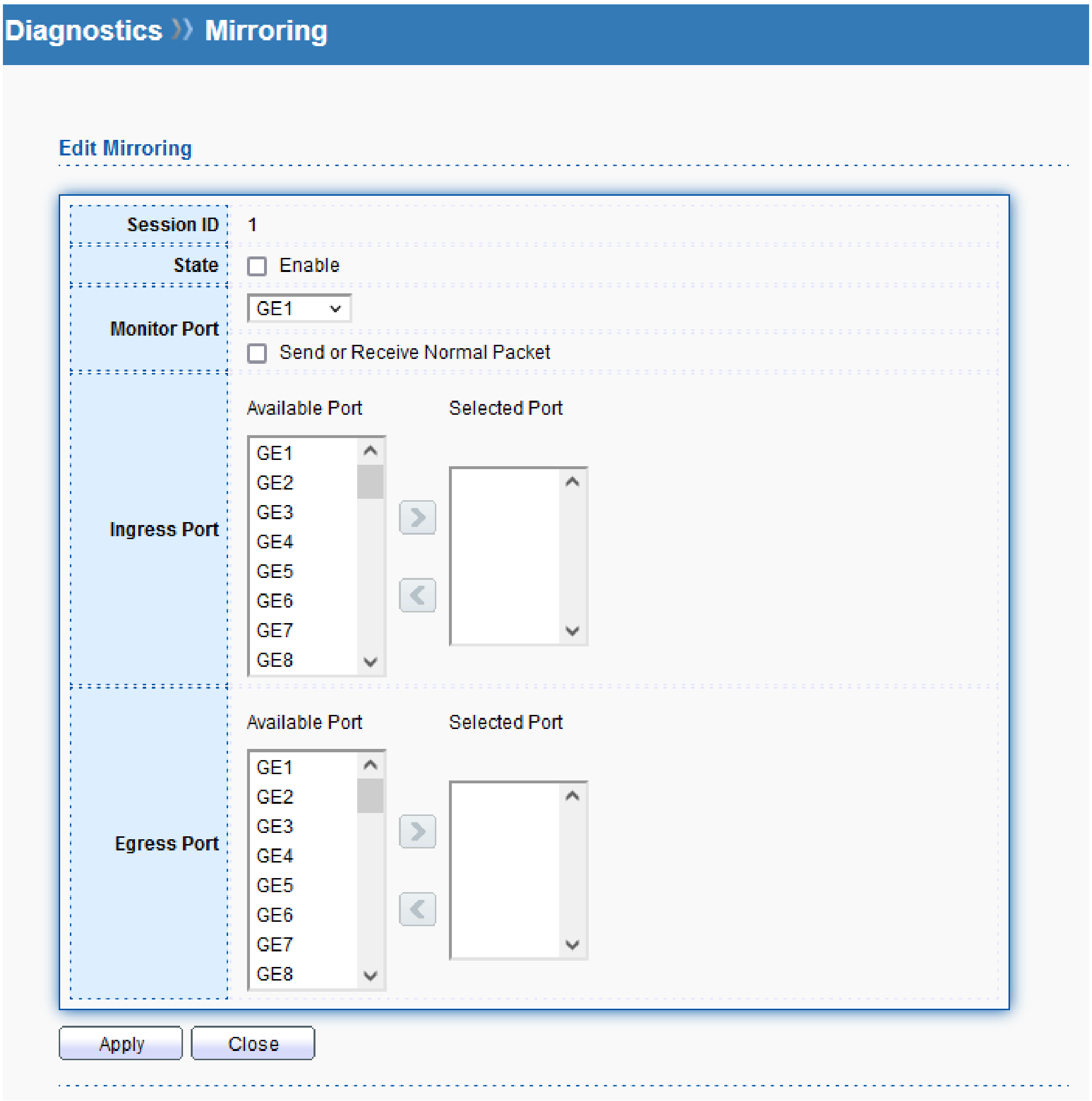


Mirroring Table

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

"*" Allow the monitor port to send or receive normal packets

Item	Description
Edit	Edit the selected port(s).


Diagnostics » Mirroring

Edit Mirroring

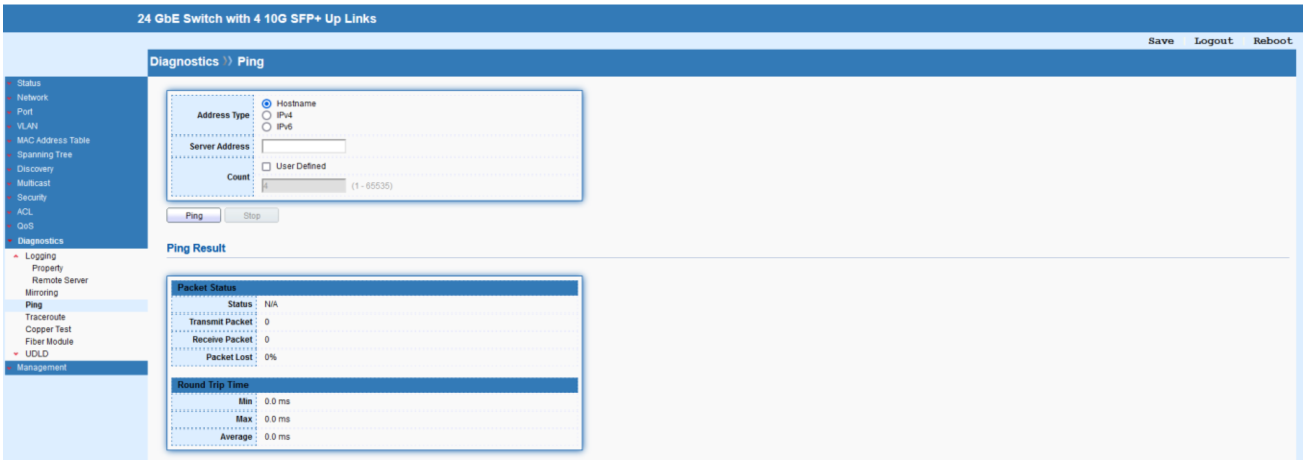
Session ID	1
State	□ Enable
Monitor Port	GE1 □ Send or Receive Normal Packet
Ingress Port	Available Port: GE1, GE2, GE3, GE4, GE5, GE6, GE7, GE8 Selected Port:
Egress Port	Available Port: GE1, GE2, GE3, GE4, GE5, GE6, GE7, GE8 Selected Port:

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.

14.3 Ping

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



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

Ping Result

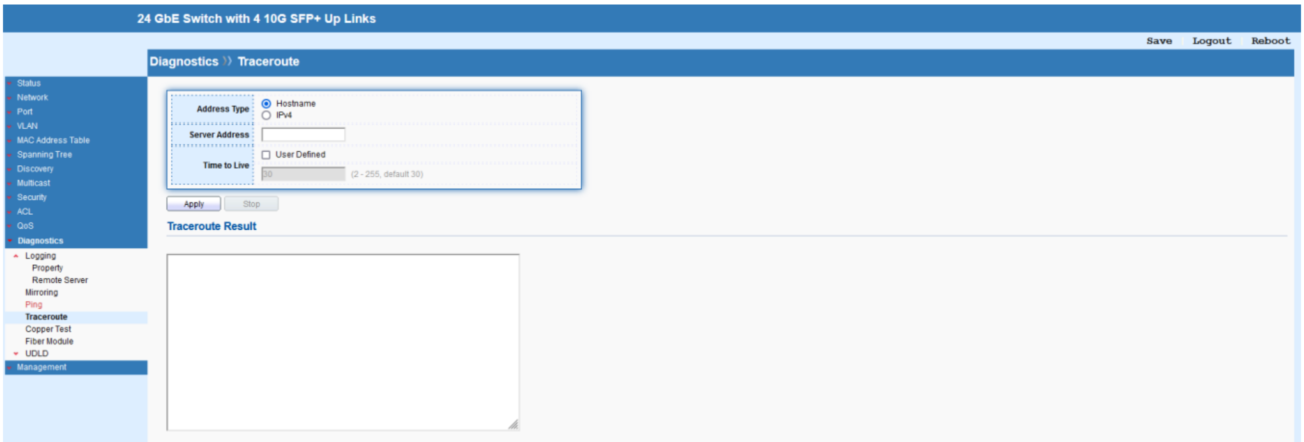
Packet Status	
Status	N/A
Transmit Packet	0
Receive Packet	0
Packet Lost	0%

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

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.

14.4 Traceroute

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



Address Type ● Hostname ○ IPv4

Server Address

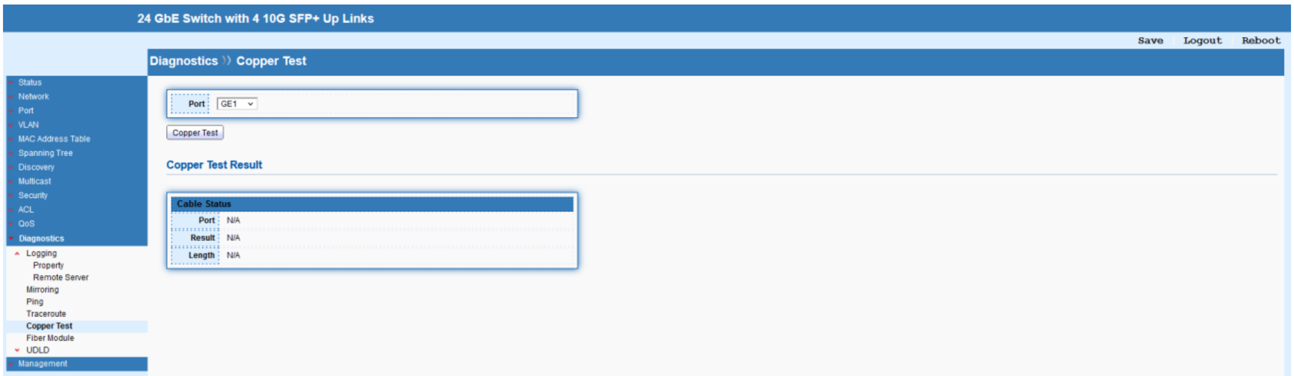
Time to Live □ User Defined 30 (2 - 255, default 30)

Traceroute Result

Item	Description
Address Type	Select the address type or remote server.
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.

14.5 Copper Test

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



Port GE1

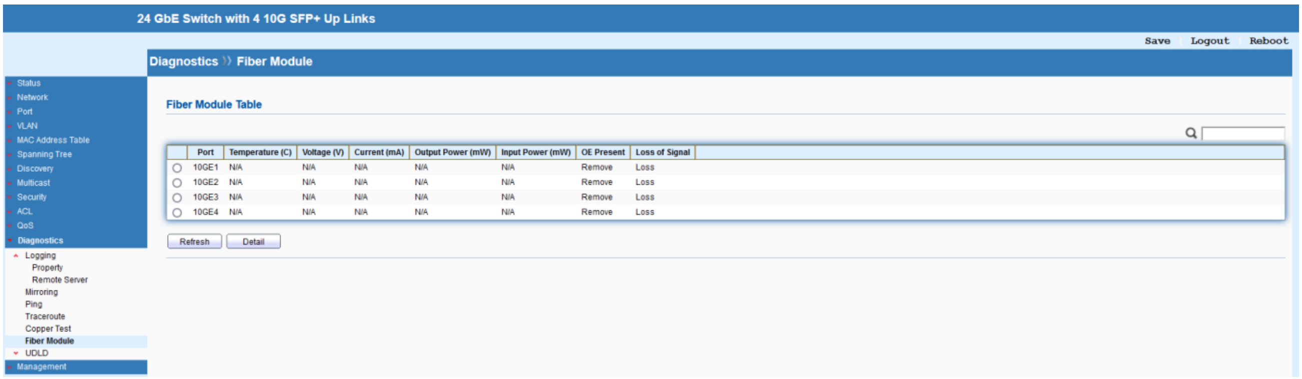
Copper Test Result

Cable Status	
Port	N/A
Result	N/A
Length	N/A

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

14.6 Fiber Module

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



Fiber Module Table

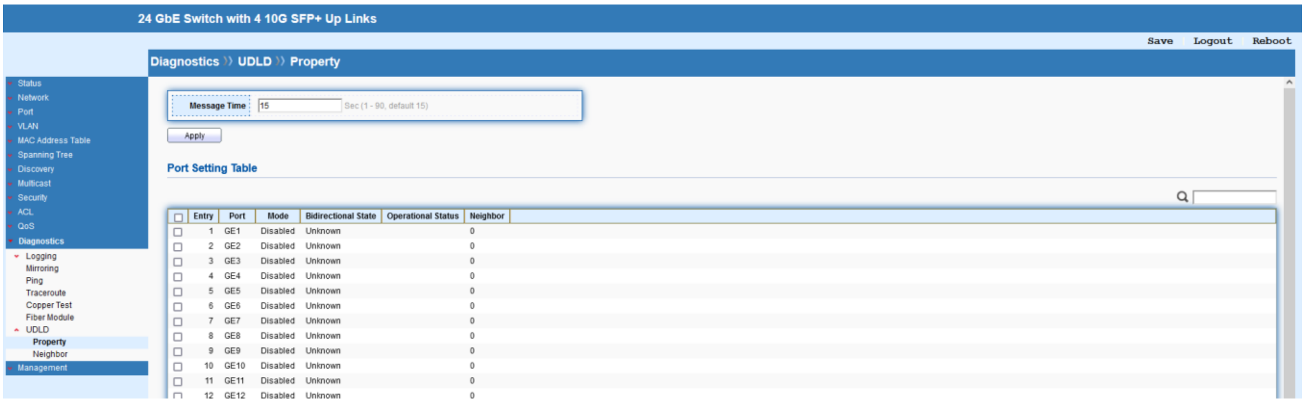
	Port	Temperature (C)	Voltage (V)	Current (mA)	Output Power (mW)	Input Power (mW)	OE Present	Loss of Signal
○	10GE1	N/A	N/A	N/A	N/A	N/A	Remove	Loss
○	10GE2	N/A	N/A	N/A	N/A	N/A	Remove	Loss
○	10GE3	N/A	N/A	N/A	N/A	N/A	Remove	Loss
○	10GE4	N/A	N/A	N/A	N/A	N/A	Remove	Loss

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

14.7 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.

14.7.1 Property



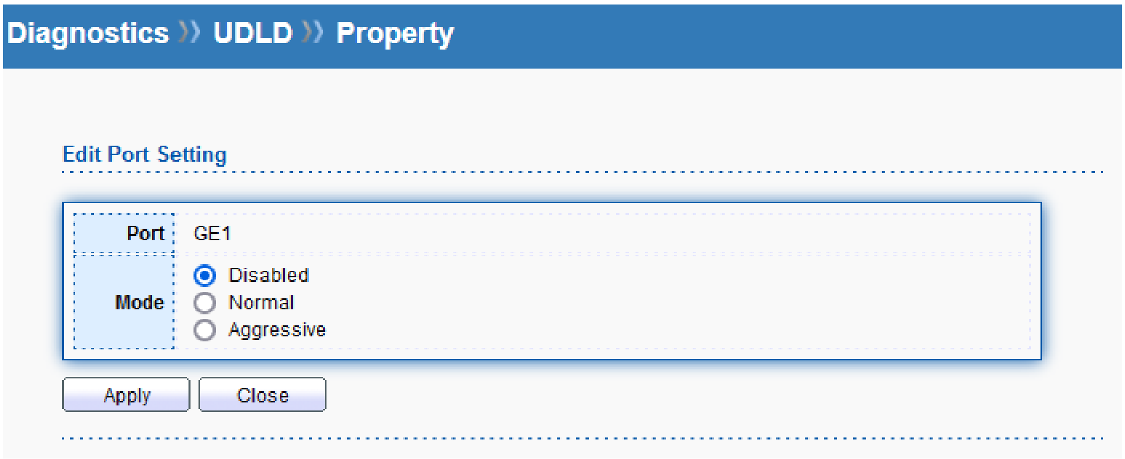
Message Time: 15 Sec (1 - 90, default 15)

Port Setting Table

□	Entry	Port	Mode	Bidirectional State	Operational Status	Neighbor
□	1	GE1	Disabled	Unknown		0
□	2	GE2	Disabled	Unknown		0
□	3	GE3	Disabled	Unknown		0
□	4	GE4	Disabled	Unknown		0
□	5	GE5	Disabled	Unknown		0
□	6	GE6	Disabled	Unknown		0
□	7	GE7	Disabled	Unknown		0
□	8	GE8	Disabled	Unknown		0
□	9	GE9	Disabled	Unknown		0
□	10	GE10	Disabled	Unknown		0
□	11	GE11	Disabled	Unknown		0
□	12	GE12	Disabled	Unknown		0

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.


Diagnostics » UDLD » Property

Edit Port Setting

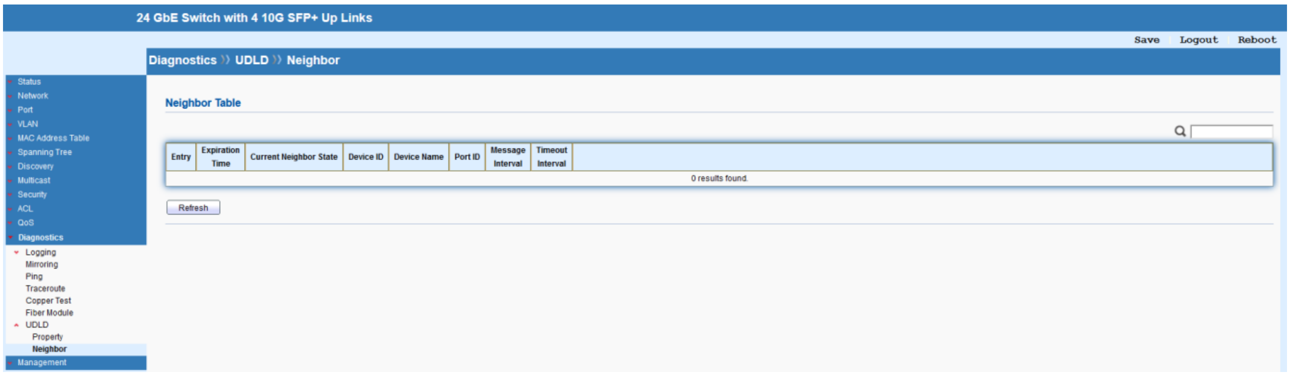
Port: GE1

Mode: ● Disabled ○ Normal ○ Aggressive

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.

14.7.2 Neighbor

This page displays information of the neighboring devices.


24 GbE Switch with 4 10G SFP+ Up Links

Diagnostics » UDLD » Neighbor

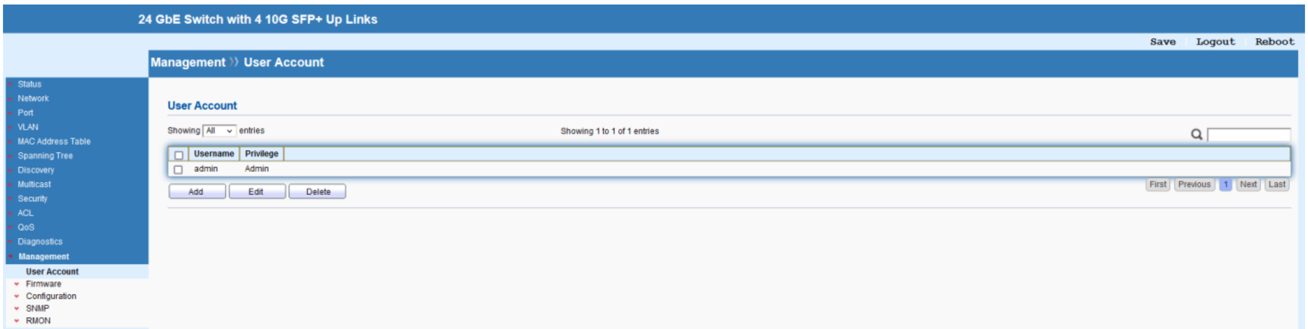
Neighbor Table

Entry	Expiration Time	Current Neighbor State	Device ID	Device Name	Port ID	Message Interval	Timeout Interval
0 results found.							

15 Management

15.1 User Account

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



User Account

Showing All entries

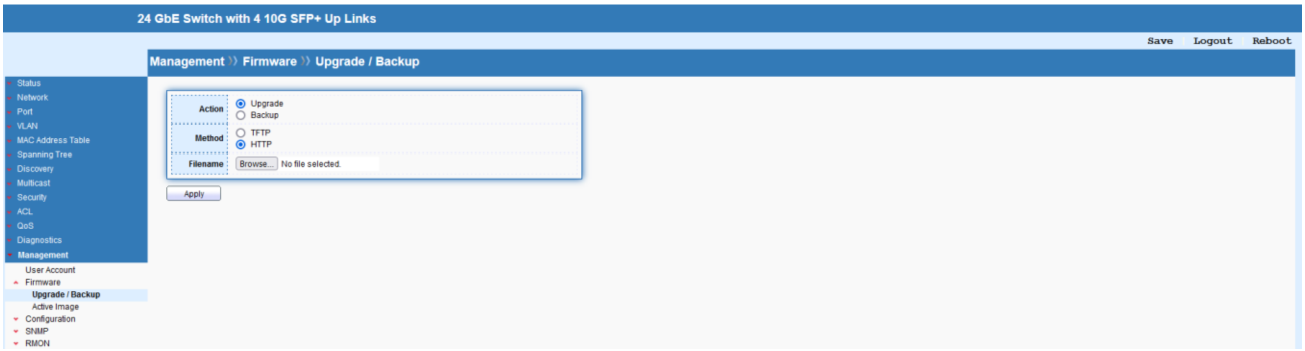
Showing 1 to 1 of 1 entries

□	Username	Privilege
□	admin	Admin

15.2 Firmware

15.2.1 Upgrade / Backup

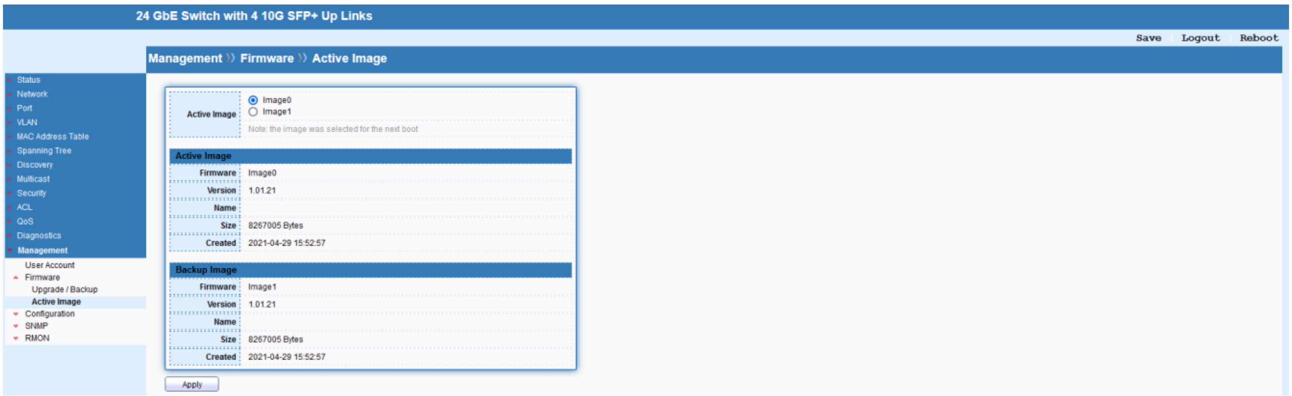
This page allows to upgrade the current image in the flash partition or backup the firmware from selected flash image partition 0 / 1.



Action	● Upgrade ○ Backup
Method	○ TFTP ● HTTP
Filename	Browse... No file selected.

15.2.2 Active Image

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

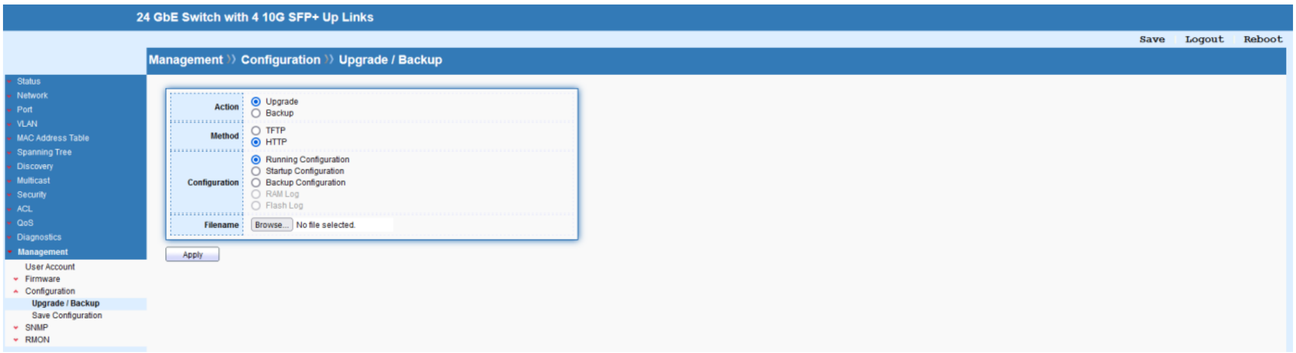


Active Image	● Image0 ○ Image1 Note: the image was selected for the next boot
Active Image	
Firmware	Image0
Version	1.01.21
Name	
Size	8267005 Bytes
Created	2021-04-29 15:52:57
Backup Image	
Firmware	Image1
Version	1.01.21
Name	
Size	8267005 Bytes
Created	2021-04-29 15:52:57

15.3 Configuration

15.3.1 Upgrade / Backup

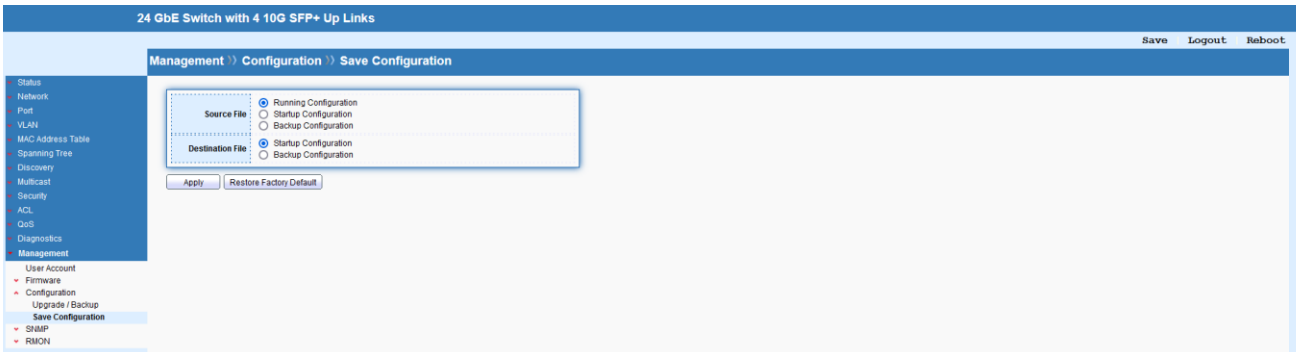
This page allows to upgrade the Running/Startup/Backup configuration or backup the Running/Startup/Backup configuration and RAM/Flash log via TFTP or HTTP.



Action	● Upgrade ○ Backup
Method	○ TFTP ● HTTP
Configuration	● Running Configuration ○ Startup Configuration ○ Backup Configuration ○ RAM Log ○ Flash Log
Filename	Browse... No file selected.

15.3.2 Save Configuration

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



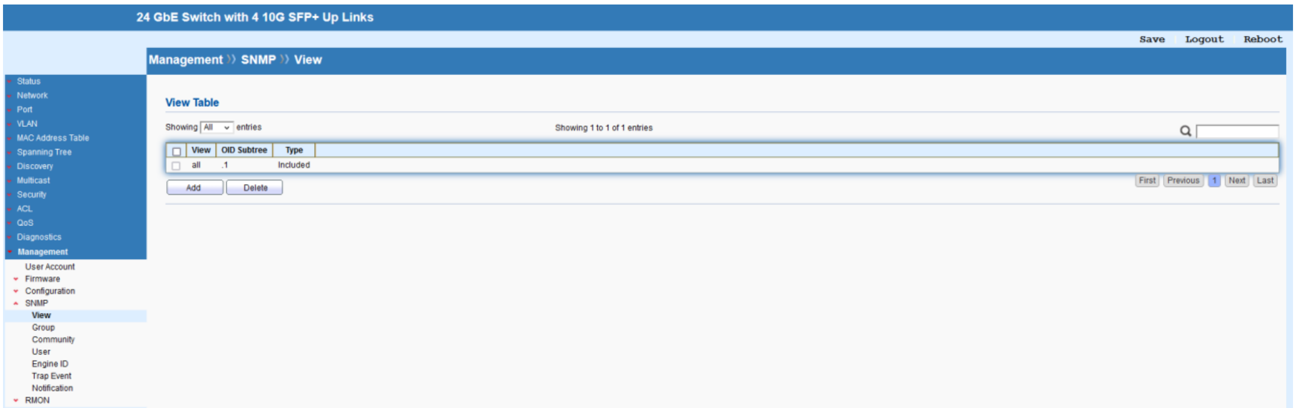
Source File	● Running Configuration ○ Startup Configuration ○ Backup Configuration
Destination File	● Startup Configuration ○ Backup Configuration

15.4 SNMP

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

15.4.1 View

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



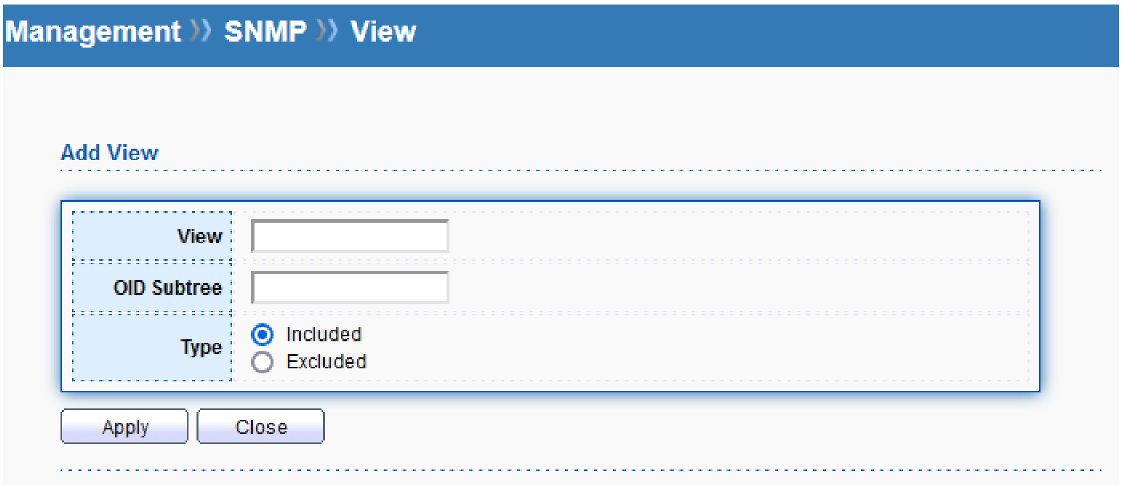
View Table

Showing All entries

Showing 1 to 1 of 1 entries

□	View	OID Subtree	Type
□	all	.1	Included

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



Add View

View

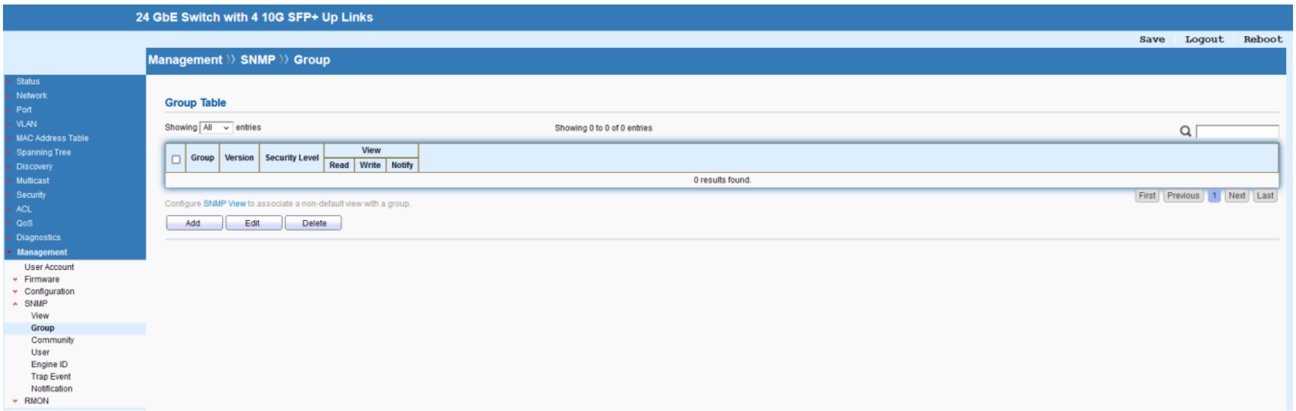
OID Subtree

Type ● Included ○ Excluded

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.

15.4.2 Group

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



Management » SNMP » Group

Group Table

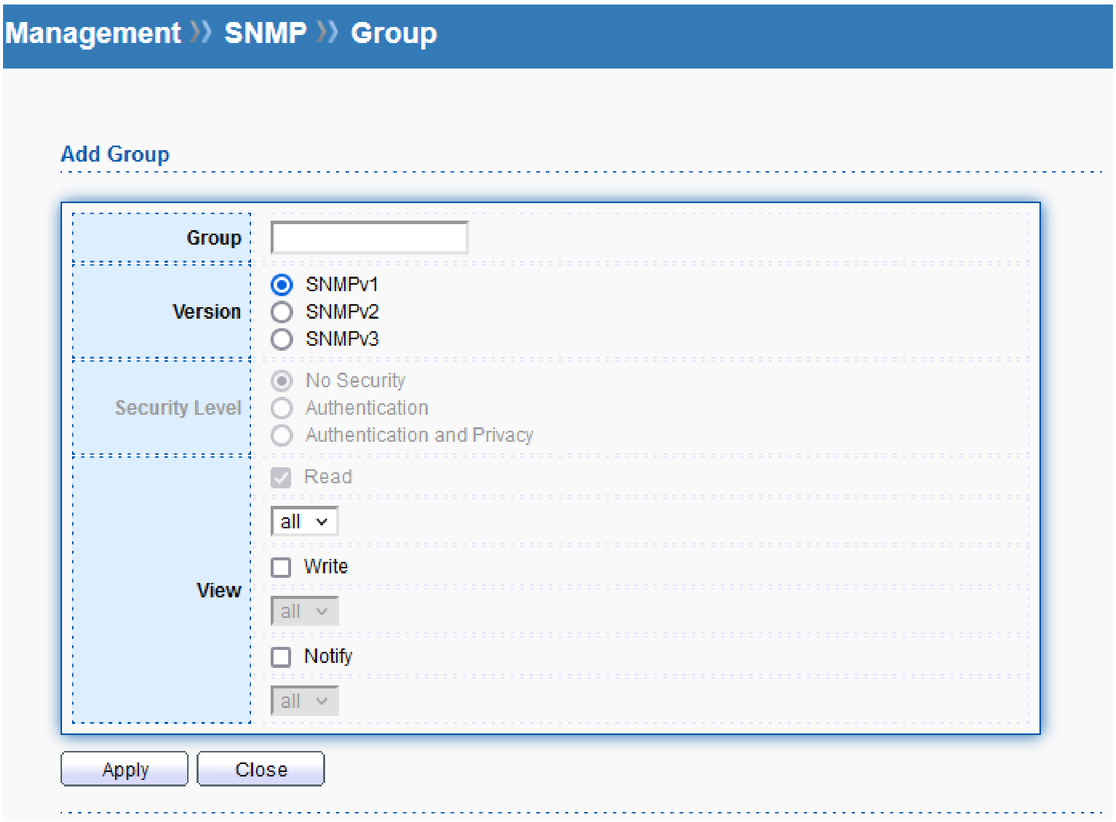
Showing All entries

Showing 0 to 0 of 0 entries

□	Group	Version	Security Level	View		
				Read	Write	Notify
0 results found.						

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

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



Management » SNMP » Group

Add Group

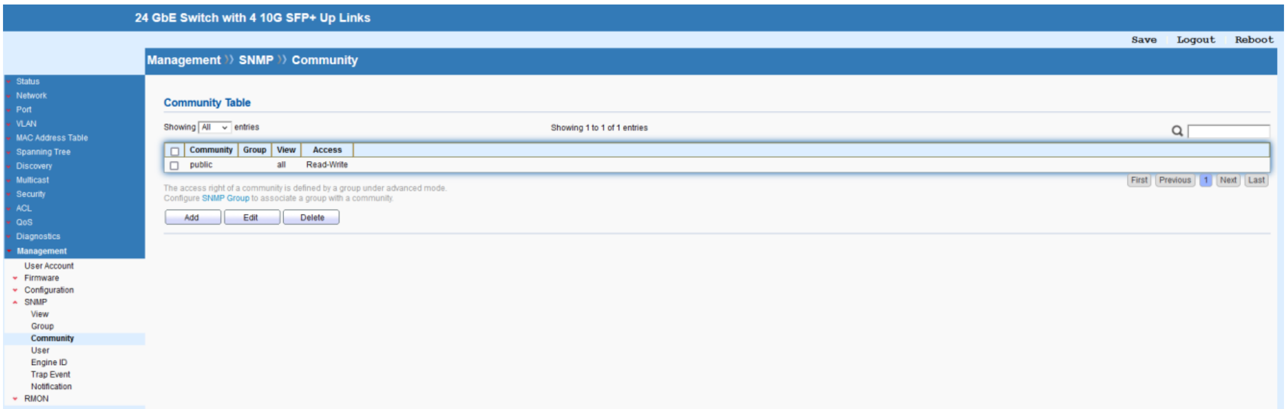
Group	
Version	● SNMPv1 ○ SNMPv2 ○ SNMPv3
Security Level	● No Security ○ Authentication ○ Authentication and Privacy
View	☑ Read all □ Write all □ Notify all

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.

15.4.3 Community

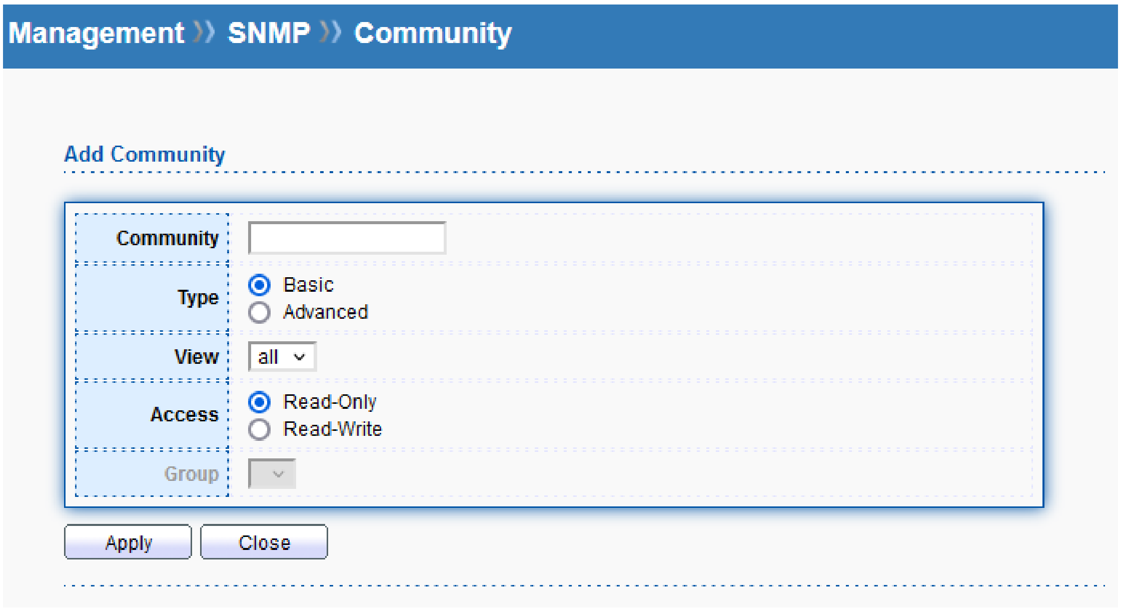
This page allows to add/remove multiple communities of SNMP.



□	Community	Group	View	Access
□	public		all	Read-Write

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

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



Management » SNMP » Community

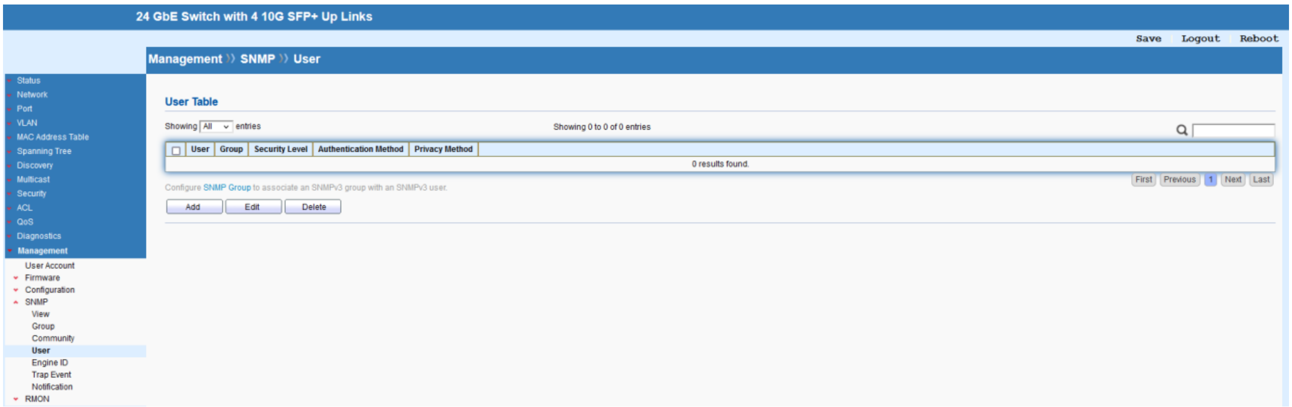
Add Community

Community	
Type	● Basic ○ Advanced
View	all
Access	● Read-Only ○ Read-Write
Group	

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.

15.4.4 User

This page allows to configure SNMP user profile.



Management » SNMP » User

User Table

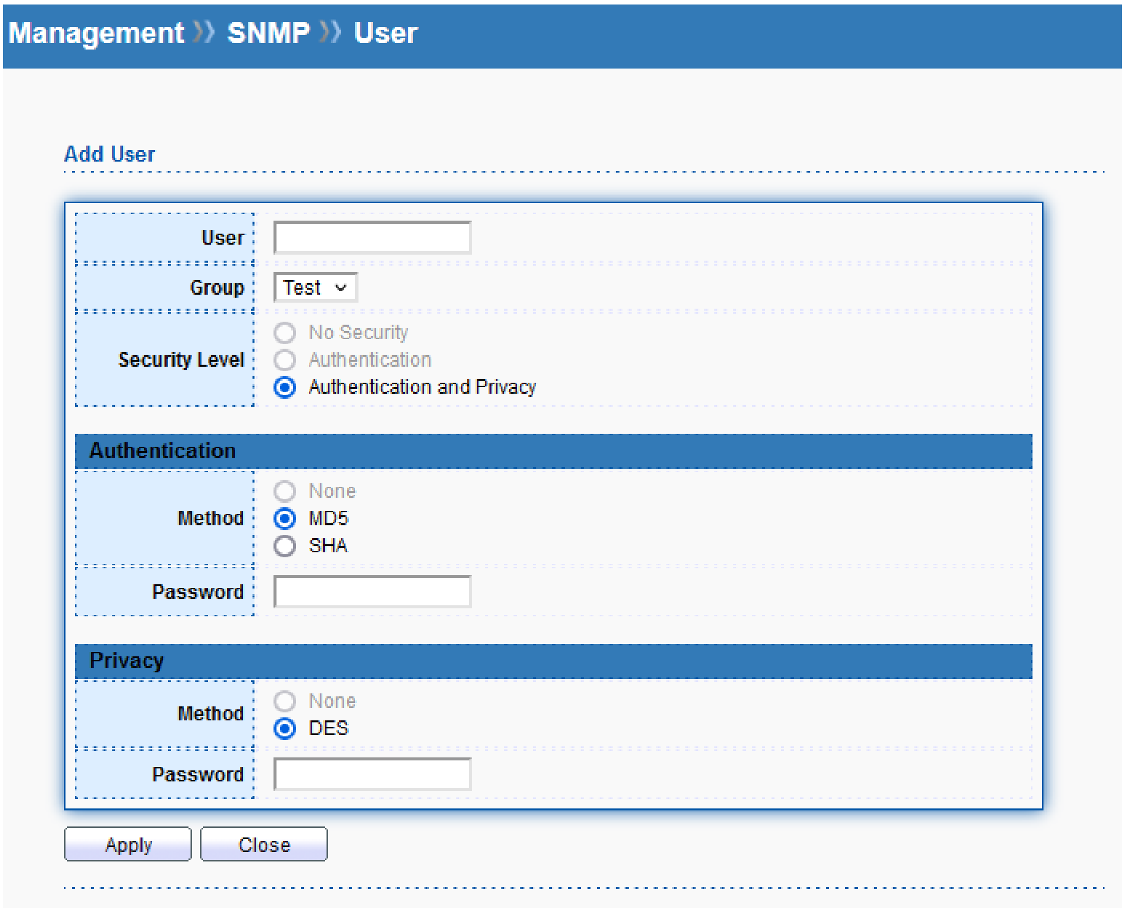
Showing All entries

Showing 0 to 0 of 0 entries

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

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

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



Management » SNMP » User

Add User

User

Group Test

Security Level ○ No Security ○ Authentication ● Authentication and Privacy

Authentication

Method ○ None ● MD5 ○ SHA

Password

Privacy

Method ○ None ● DES

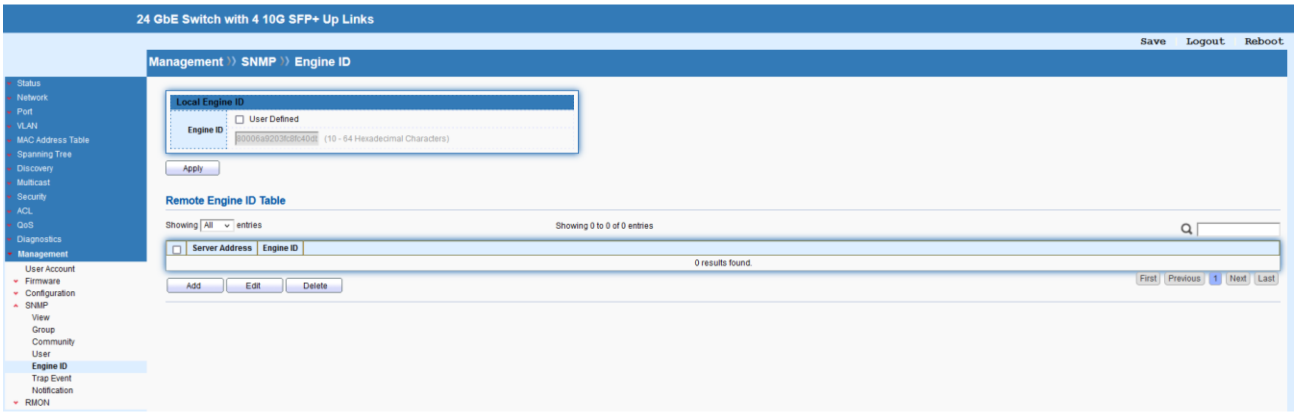
Password

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.
Privacy	
Method	At present, available methods include DES and None.
Password	Enter a password for the selected method.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.

15.4.5 Engine ID

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



Local Engine ID

Engine ID: ☐ User Defined

80006a9203fc8fc40dt (10 - 64 Hexadecimal Characters)

Remote Engine ID Table

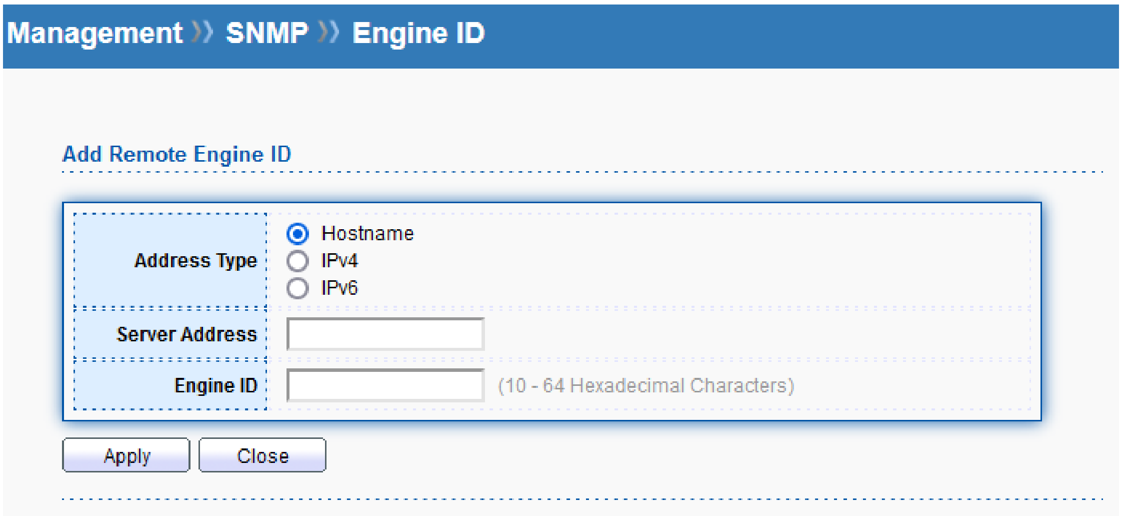
Showing All entries

Showing 0 to 0 of 0 entries

☐	Server Address	Engine ID
0 results found.		

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.



Management 〉〉 SNMP 〉〉 Engine ID

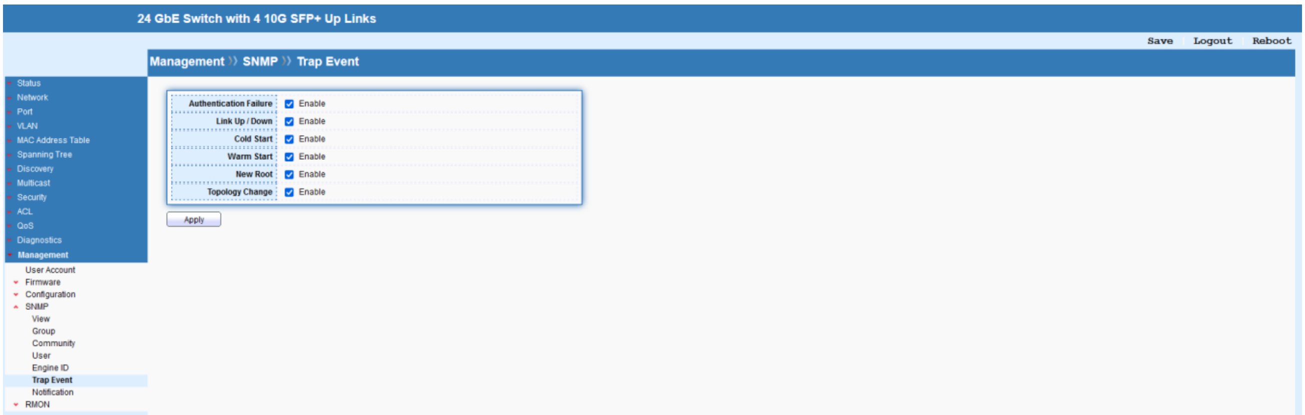
Add Remote Engine ID

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

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.

15.4.6 Trap Event

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



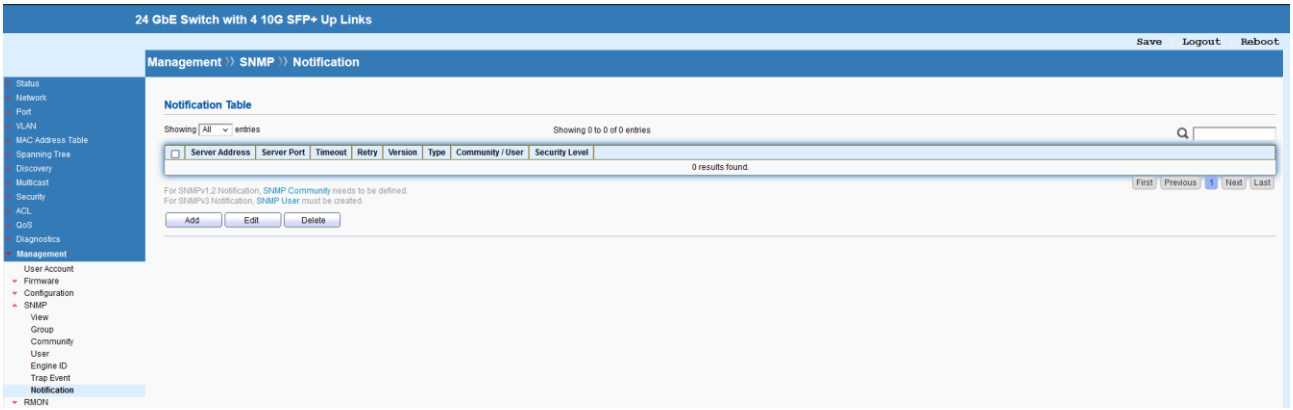
24 GbE Switch with 4 10G SFP+ Up Links

Management 〉〉 SNMP 〉〉 Trap Event

Authentication Failure	☑ Enable
Link Up / Down	☑ Enable
Cold Start	☑ Enable
Warm Start	☑ Enable
New Root	☑ Enable
Topology Change	☑ Enable

15.4.7 Notification

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



Notification Table

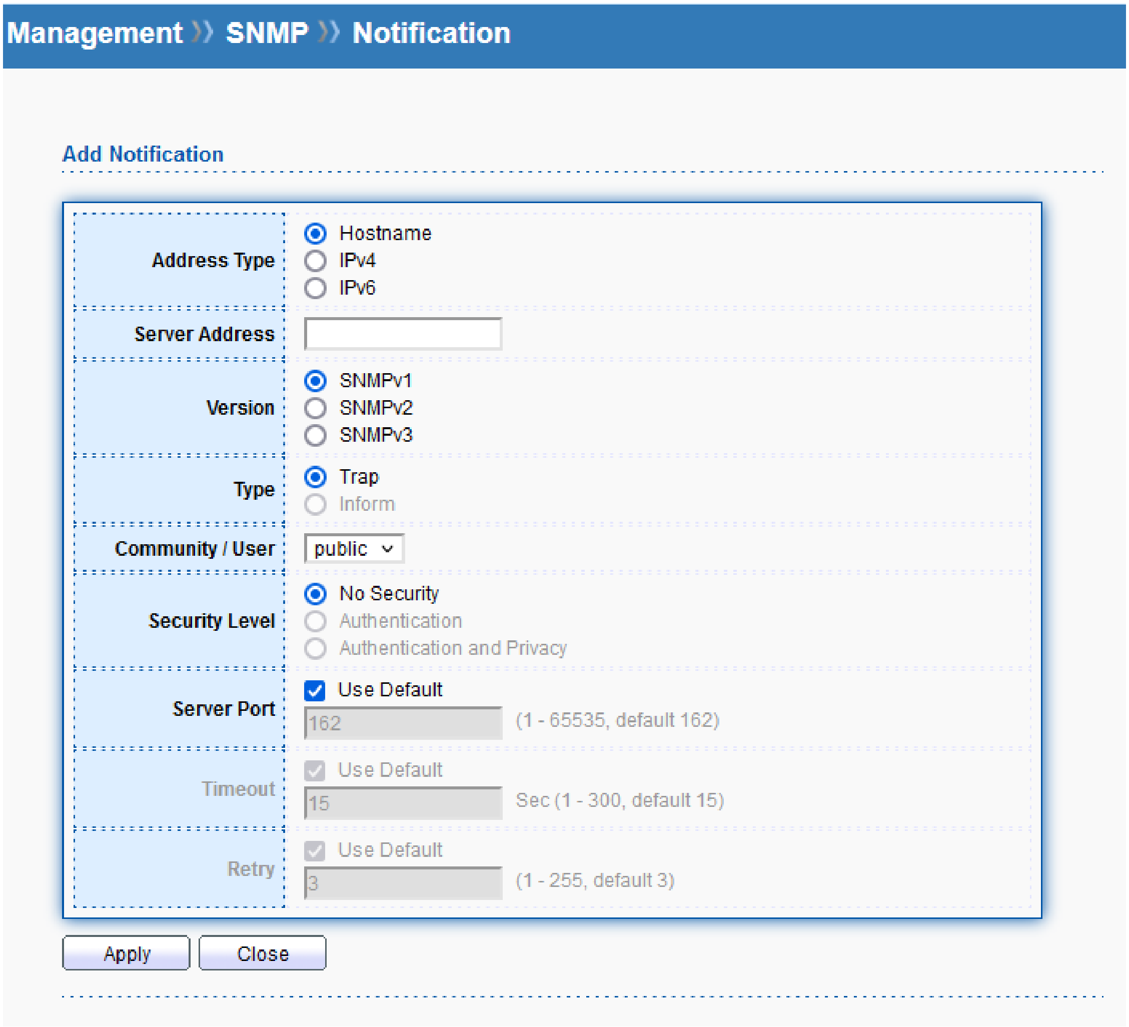
Showing All entries

Showing 0 to 0 of 0 entries

□	Server Address	Server Port	Timeout	Retry	Version	Type	Community / User	Security Level
0 results found.								

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

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



Management » SNMP » Notification

Add Notification

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

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.

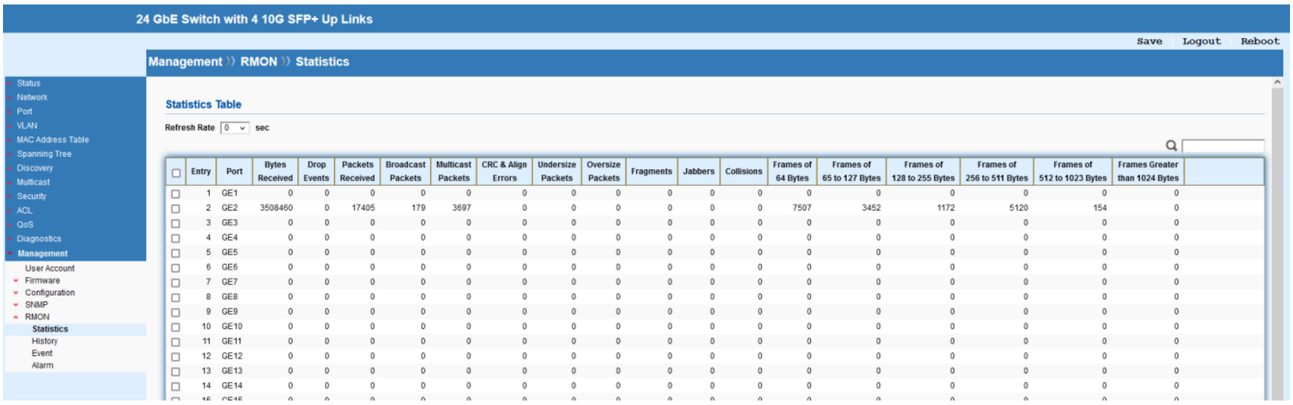
	Authentication and Privacy: Requires authentication and encryption.
Server Port	Specify the UDP port number for the recipient's server. **Use Default**: If it is checked, the default number (162) will be used automatically.
Timeout	Specify the SNMP informs timeout. It is available when Inform is selected 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.

15.5 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).

15.5.1 Statistics

This page shows the RMON statistics table.



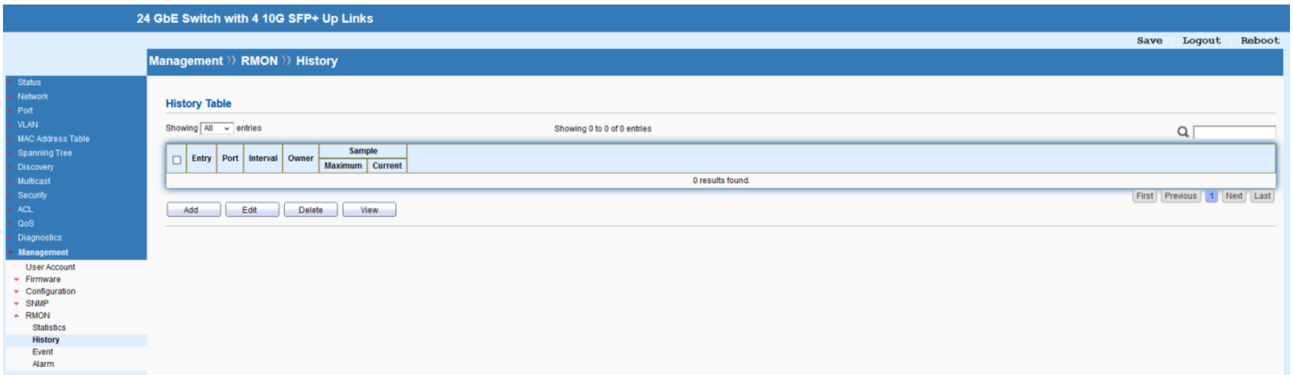
Statistics Table

Refresh Rate 0 sec

□	Entry	Port	Bytes Received	Drop Events	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Oversize Packets	Fragments	Jabbers	Collisions	Frames of 64 Bytes	Frames of 65 to 127 Bytes	Frames of 128 to 255 Bytes	Frames of 256 to 511 Bytes	Frames of 512 to 1023 Bytes	Frames Greater than 1024 Bytes
□	1	GE1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	2	GE2	3508460	0	17405	179	3697	0	0	0	0	0	0	7507	3452	1172	5120	154	0
□	3	GE3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	4	GE4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	5	GE5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	6	GE6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	7	GE7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	8	GE8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	9	GE9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	10	GE10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	11	GE11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	12	GE12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	13	GE13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
□	14	GE14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

15.5.2 History

This page allows to configure RMON history table.



History Table

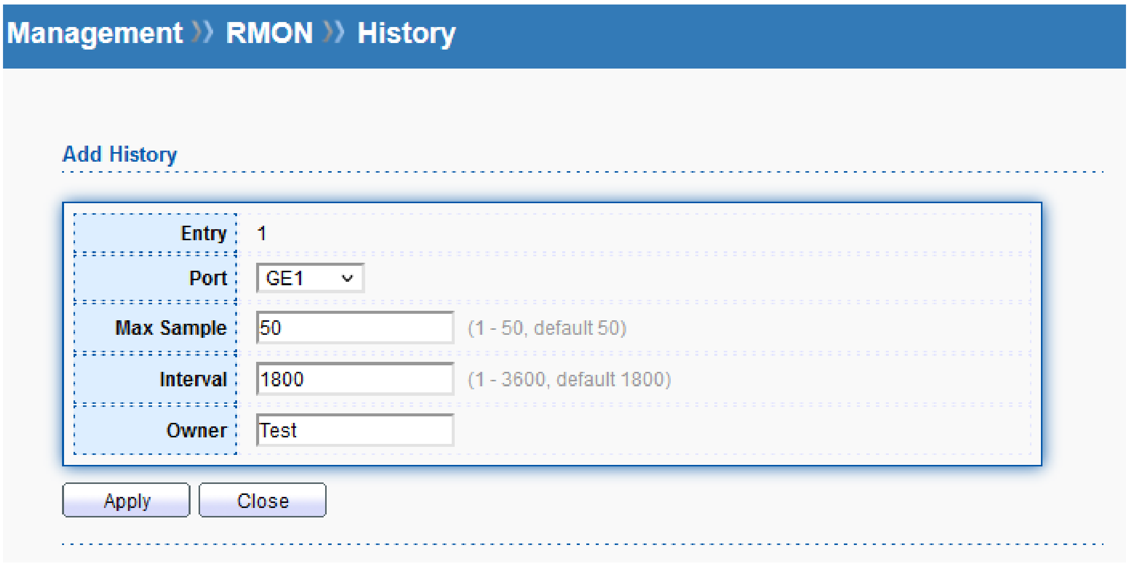
Showing All entries

Showing 0 to 0 of 0 entries

□	Entry	Port	Interval	Owner	Sample	
					Maximum	Current

0 results found.

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



Add History

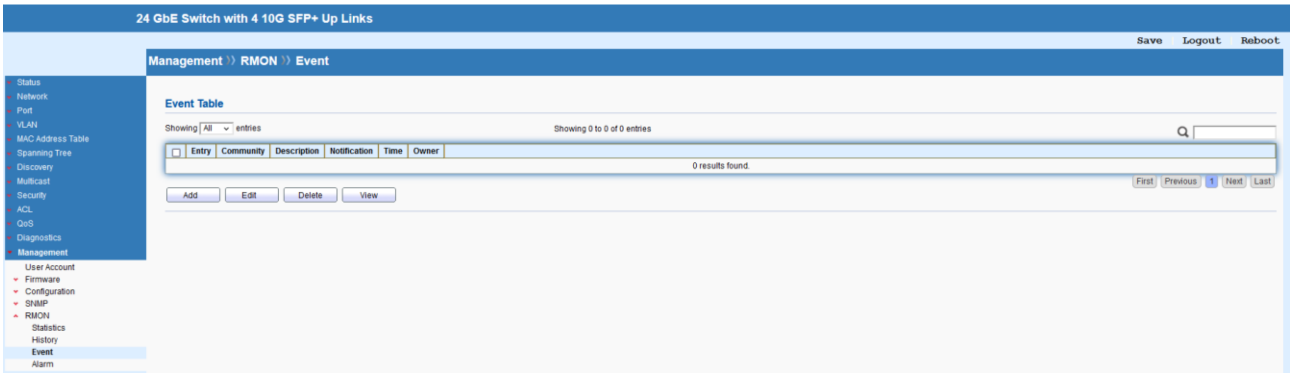
Entry	1
Port	GE1
Max Sample	50 (1 - 50, default 50)
Interval	1800 (1 - 3600, default 1800)
Owner	Test

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.

15.5.3 Event

This page allows to configure RMON Event table.



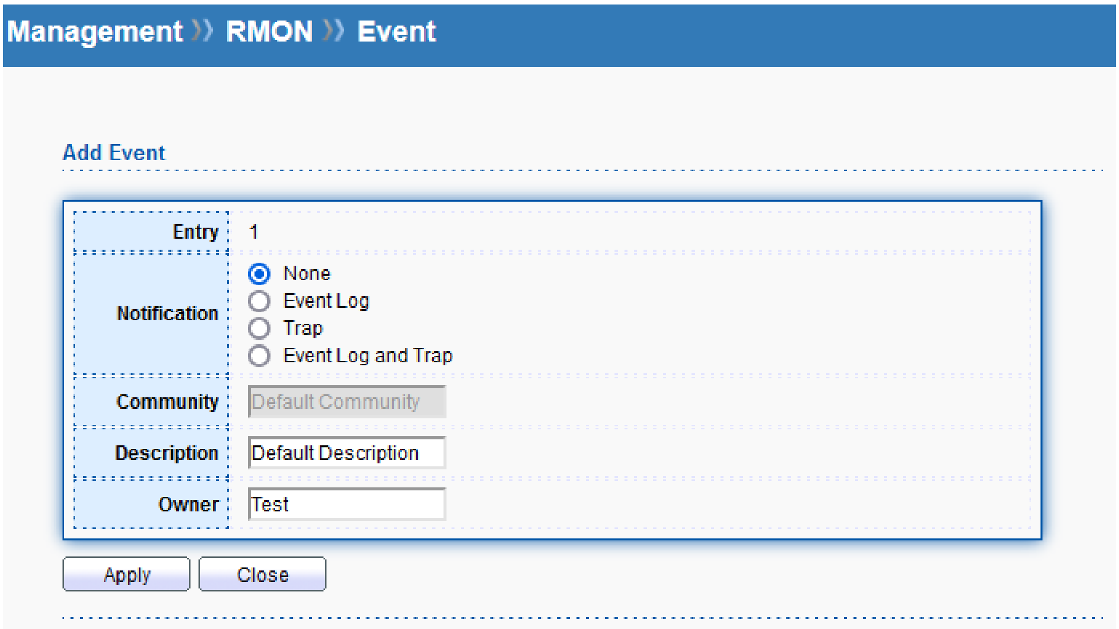
Event Table

Showing All entries

Showing 0 to 0 of 0 entries

□	Entry	Community	Description	Notification	Time	Owner
0 results found.						

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



Add Event

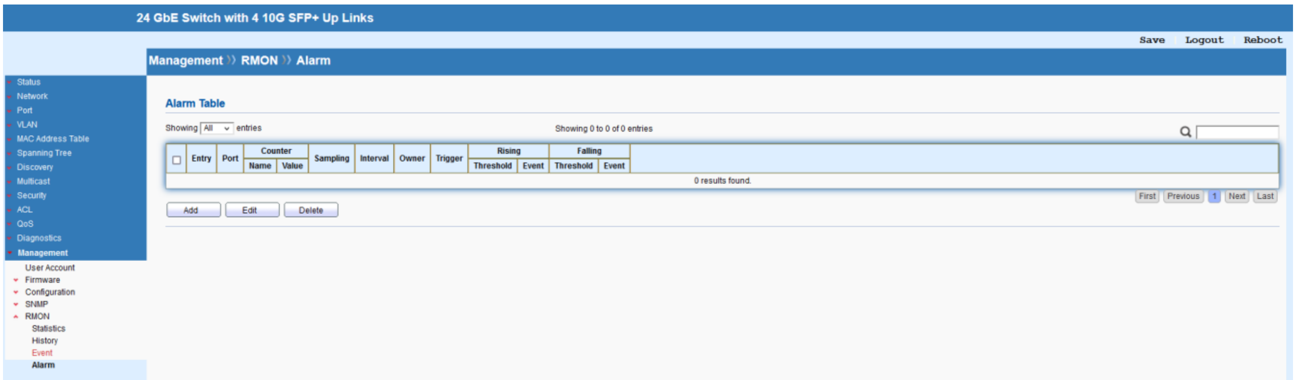
Entry	1
Notification	● None ○ Event Log ○ Trap ○ Event Log and Trap
Community	Default Community
Description	Default Description
Owner	Test

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.

15.5.4 Alarm

This page allows to configure RMON Event table.



Alarm Table

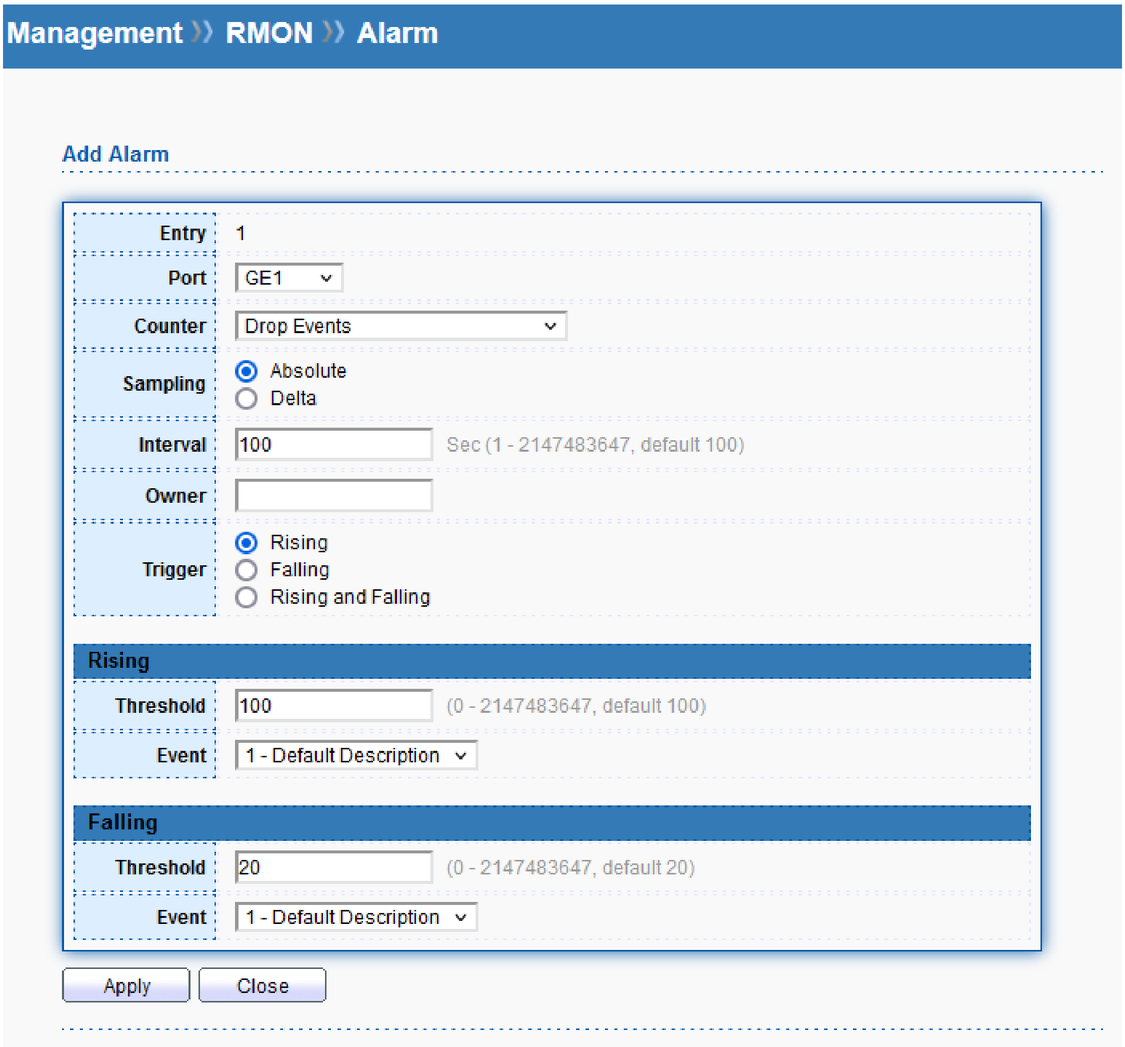
Showing All entries

Showing 0 to 0 of 0 entries

□	Entry	Port	Counter		Sampling	Interval	Owner	Trigger	Rising		Falling	
			Name	Value					Threshold	Event	Threshold	Event

0 results found.

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



Management » RMON » Alarm

Add Alarm

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

Rising

Threshold	100 (0 - 2147483647, default 100)
Event	1 - Default Description

Falling

Threshold	20 (0 - 2147483647, default 20)
Event	1 - Default Description

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 (-2147483648-2147483647).
Event	Rising event index.
Falling	
Threshold	Falling threshold value (-2147483648-2147483647)
Event	Falling event index.
Apply	Apply the settings to the switch.
Close	Close the setting page and back to previous page.