ALL-SG9312M-10G

12-port 10G SFP+ L2 Switch

User Manual

Default-IP

192.168.2.1

Username & Password:

admin

Table of Contents

Chapter 1 Introduction

1.1 General Description

This switch is 12-port 10G SFP+ L2 Switch. The switch provides exceptionally smart Web management features, such as VLAN, QoS, RSTP, IGMP Snooping, LACP, IEEE802.1X, Strom Control…etc. The switch is standard 19” rack-mount design to fit into the rack environment. With these features, the switch is a superb choice for medium or large network environment to strengthen its network connection and efficiency.

1.2 The Front Panel

The following figure shows the front panel of the switch.

This device provides extensive LEDs to show the activities on power, system and ports.
See the following description for your reference:

LED	Status	Operation
PWR	Green Off	Power off or fail.
	Green On	Power on.
SYS	Green Off	Power off or fail
	Blinking Green	System booting up.
	Green On	System is ready
ALERT	Red Off	Switch is normal condition
	Red On	Alarm for system failure because of overheat, wrong voltage.
1-12 Port LED: (SFP+)	Off	Port disconnected or link fail
	Steady Green	10Gbps connected.
	Steady Amber	1000Mbps connected
	Blinking	Sending or receiving data.

The Reset Button

Reset the switch to its factory default configuration via the RESET button. Press the Reset button for ten seconds and release. The switch automatically reboots and reloads its factory configuration file. The Reset button is on the front panel of the switch.

1.4 The Rear Panel

The following figure shows the rear panel of the switch:

Power Receptacle

To be compatible with the electric service standards around the world, the switch is designed to afford the power supply in the range from 100 to 240 VAC, 50/60 Hz. Please make sure that your outlet standard to be within this range.
To power on the switch, please plug the female end of the power cord firmly into the receptacle of the switch, the other end into an electric service outlet. After the switch powered on, please check if the power LED is lit for a normal power status.

1.5 Hardware Installation

To install this switch, please place it on a large flat surface with a power socket close by. This surface should be clean, smooth, and level. Also, please make sure that there is enough space around this switch for RJ45 cable or fiber cable, power cord and ventilation.
If you're installing this switch on a 19-inch rack, please make sure to use the rack-mount kit (L brackets) and screws come with the product package. ALL screws must be fastened so the rack-mount kit and your product are tightly conjoined before installing it on your 19-inch rack.

SFP Installation

While install the SFP transceiver, make sure the SFP type of the 2 ends is the same and the transmission distance, wavelength, fiber cable can meet your request. It is suggested to purchase the SFP transceiver with the switch provider to avoid any incompatible issue.
The way to connect the SFP transceiver is to Plug in SFP fiber transceiver fist. The SFP transceiver has 2 plug for fiber cable, one is TX (transmit), the other is RX (receive). Cross-connect the transmit channel at each end to the receive channel at the opposite end.

Rack-mount Installation

Attach the brackets to the device by using the screws provided in the Rack Mount kit. Mount the device in the 19-inch rack by using four rack-mounting screws provided by the rack manufacturer.

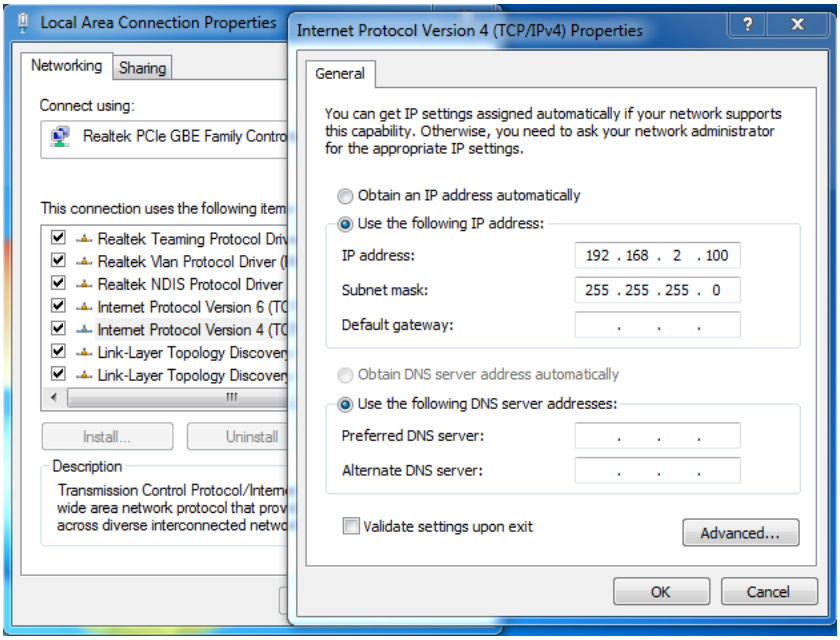
Chapter 2 Getting Started

2.1 Preparation for Web Interface

The web management page allows you to use a standard web-browser such as Microsoft Internet Explorer, Google Chrome or Mozilla Firefox, to configure and interrogate the switch from anywhere on the network.

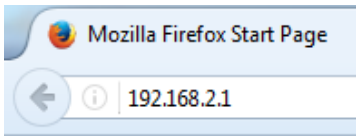
Before you attempt to use the web user interface to manage switch operation, verify that your switch is properly installed on your network and that every PC on this network can access the switch via the web browser.

1. Verify that your network interface card (NIC) is operational, and that your operating system supports TCP/IP protocol.
2. Wire the switch power and connect your computer to the switch.
3. The switch default IP address is **192.168.2.1**. The Switch and the connected PC should locate within the same IP Subnet.
4. Change your computer's IP address to 192.168.2.XX or other IP address which is located in the 192.168.2.x (For example: IP Address: 192.168.2.100; Subnet Mask: 255.255.255.0) subnet.



2.2 System login

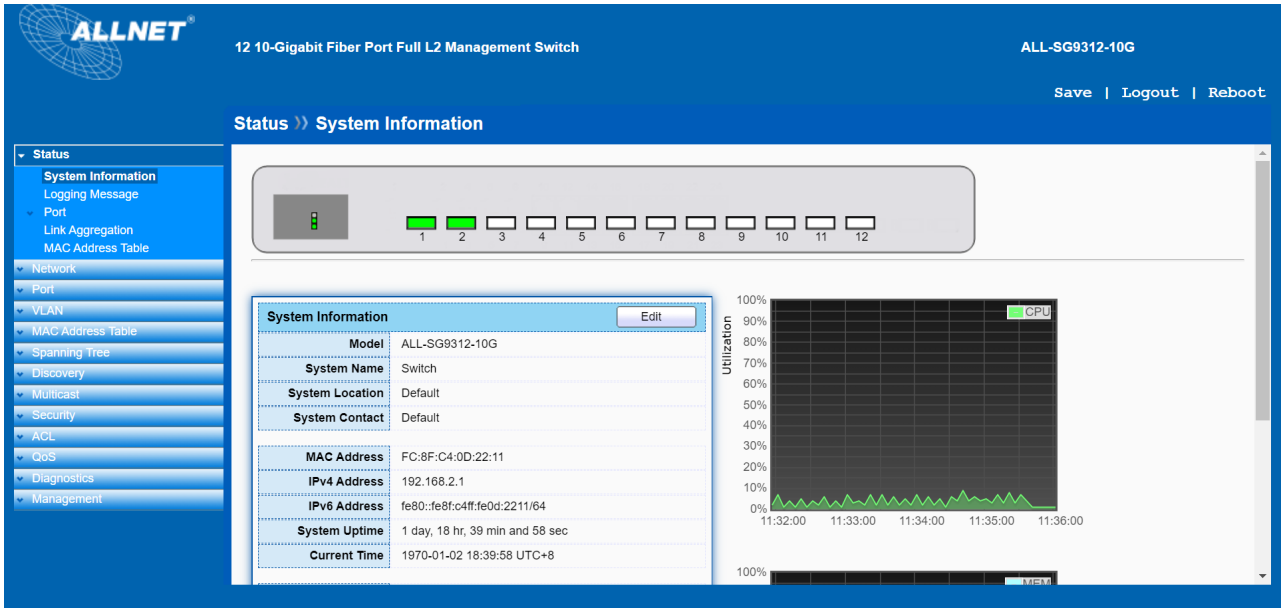
1. Start your web browser.
2. Type “http://”and the IP address of the switch (for example, the default management IP address is **192.168.2.1**) in the Location or Address field. Press **[ENTER]**.



3. The login screen appears. The default username and password are “**admin**”, so you can click **Login** and go to the web configuration screen directly.

2.3 The Graphic User Interface

After the password authorization, the System page shows up. You may click on each folder on the left column of each page to get access to each configuration page. The Graphic User Interface is as follows:



In the navigation panel, click a main link to reveal a list of submenu links shown as the following:

The following table describes the links in the navigation panel.

LINKS	Submenu
Status	System Information. Logging Message Port - Statistics, Error Disabled, Bandwidth Utilization Link Aggregation MAC Address Table
Network	IP Address System Time
Port	Port Setting Error Disabled Link Aggregation - Group, Port Setting, LACP Jumbo Frame
VLAN	VLAN - Create VLAN, VLAN Configuration, Membership, Port Setting Voice VLAN - Property, Voice OUI Protocol VLAN - Protocol Group, Group Binding MAC VLAN - MAC Group, Group Binding Surveillance VLAN - Property, Surveillance OUI GVRP - Property, Membership, Statistics
MAC Address Table	Dynamic Address Static Address Filtering Address
Spanning Tree	Property Port Setting MST Instance MST Port Setting Statistics
Discovery (LLDP)	Property Port Setting MED Network Policy MED Port Setting Packet View Local Information Neighbor Statistics
Multicast	General - Property, Group Address, Router Port, Forward All, Throttling, Filtering Profile, Filtering Binding IGMP Snooping - Property, Querier, Statistics MLD Snooping - Property, Statistics MVR - Property, Port Setting, Group Address
Security	RADIUS TACACS+ AAA - Method List, Login Authentication Management Access - Management VLAN, Management Service, Management ACL, Management ACE Authentication Manager - Property, Port Setting, MAC-Based Local Account, WEB-Based Local Account, Sessions Port Security Traffic Segmentation Storm Control DoS - Property, Port Setting Dynamic ARP Inspection - Property, Statistics DHCP Snooping - Property, Statistics, Option82 Property, Option82 Circuit ID

	IP Source Guard - Port Setting, IMPV Binding, Save Database
ACL	MAC ACL MAC ACE IPv4 ACL IPv4 ACE IPv6 ACL IPv6 ACE ACL Binding
QoS	General - Property, Queue Scheduling, CoS Mapping, DSCP Mapping, IP Precedence Mapping Rate Limit - Ingress/Egress Port, Egress Queue
Diagnostics	Logging - Property, Remove Server Mirroring Ping Traceroute Fiber Module UDLD - Property, Neighbor
Management	User Account Firmware – Upgrade/Backup, Active Image Configuration - Upgrade/Backup, Save Configuration SNMP - View, Group, Community, User, Engine ID, Trap Event, Notification RMON - Statistics, History, Event, Alarm

Please note, you have to click  **to save the configuration after changing any settings.**

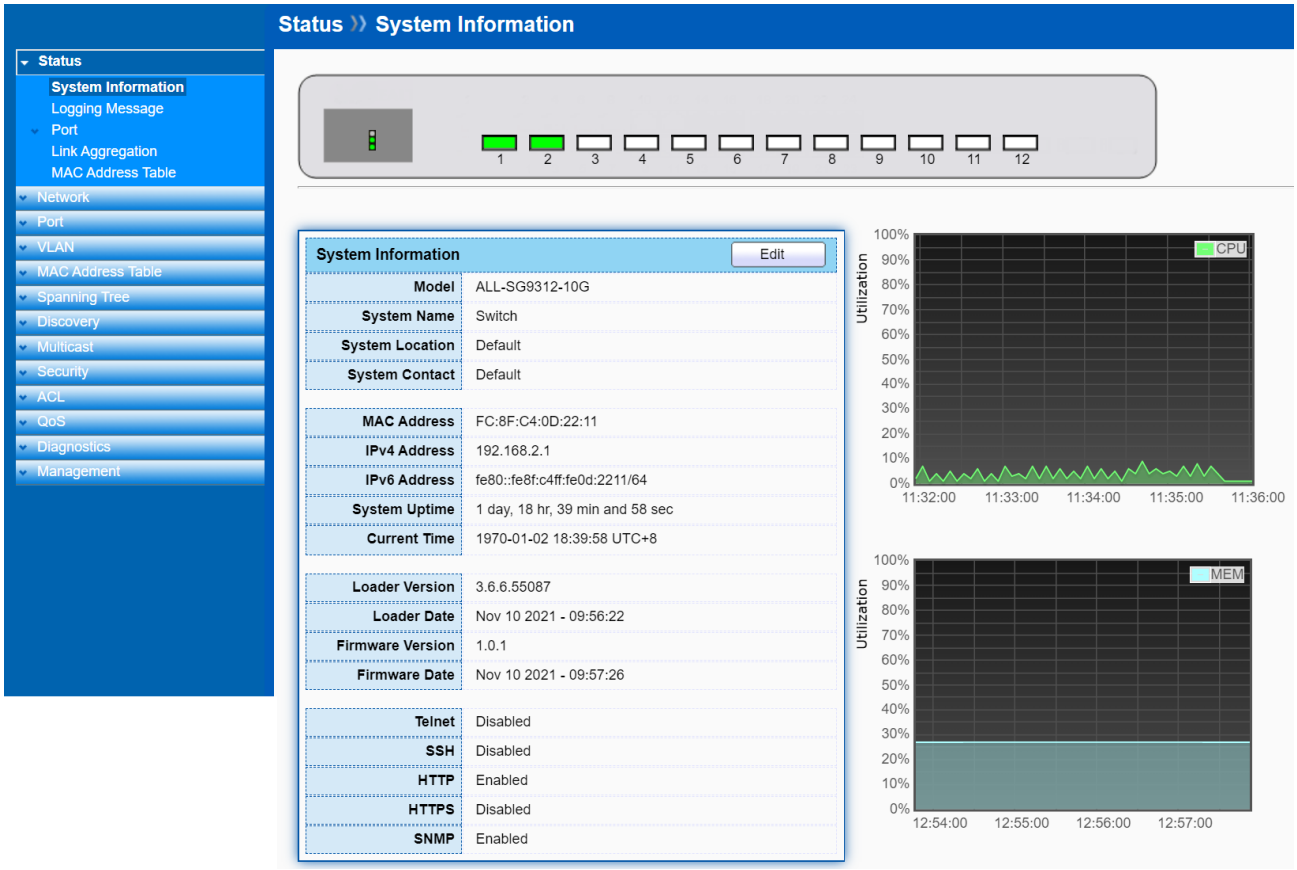
Chapter 3 Status

Use the Status pages to view system information and status.

3.1 System Information

Click **Status** > **System Information**

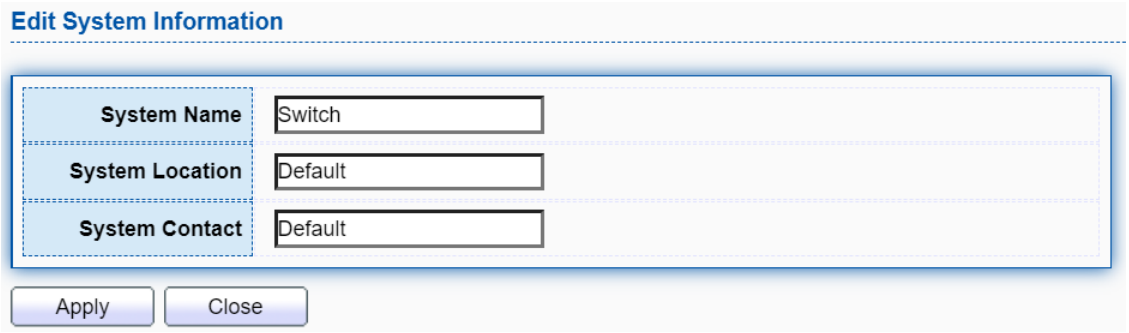
This page shows switch panel, CPU utilization, Memory utilization and other system current information. It also allows user to edit some system information.



Field	Description
Model	Model name of the switch
System Name	System name of the switch. This name will also use as CLI prefix of each line
System Location	Location information of the switch
System Contact	Contact information of the switch
MAC Address	Base MAC address of the switch
IPv4 Address	Current system IPv4 address
IPv6 Address	Current system IPv6 address
System Uptime	Total elapsed time from booting
Current Time	Current system time
Loader Version	Boot loader image version
Loader Date	Boot loader image build date
Firmware Version	Current running firmware image version
Firmware Date	Current running firmware image build date
Telnet	Current Telnet service enable/disable state
SSH	Current SSH service enable/disable state

HTTP	Current HTTP service enable/disable state
HTTPS	Current HTTPS service enable/disable state
SNMP	Current SNMP service enable/disable state

Click "**Edit**" button on the table title to edit following system information.

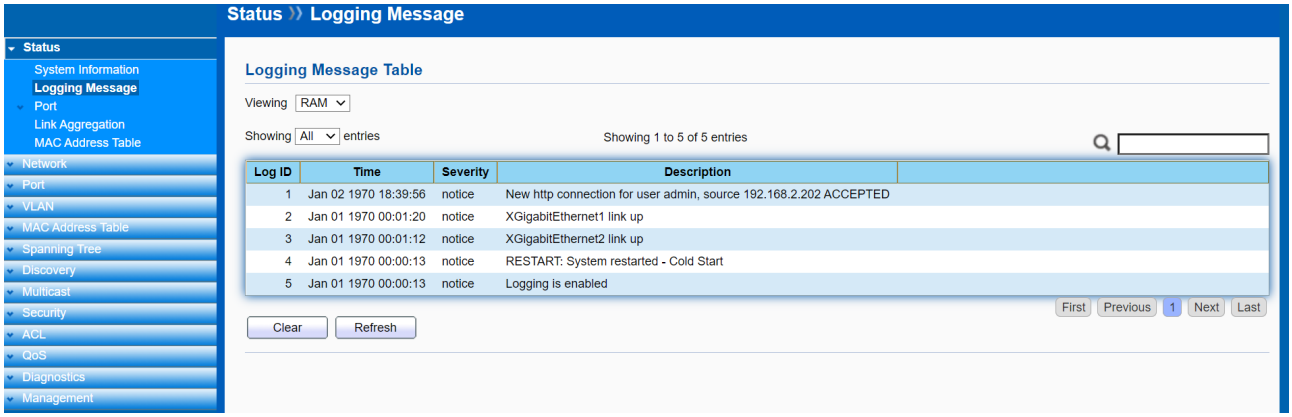


Field	Description
System Name	System name of the switch. This name will also use as CLI prefix of each line.
System Location	Location information of the switch.
System Contact	Contact information of the switch.

3.2 Logging Message

Click **Status** > **Logging Message**

This page shows logging messages stored on the RAM and Flash.



Field	Description
Viewing	The logging view including: **RAM**: Show the logging messages stored on the RAM **Flash**: Show the logging messages stored on the Flash.
Clear	Clear the logging messages.
Refresh	Refresh the logging messages.
Log ID	The log identifier.
Time	The time stamp for the logging message.
Severity	The severity for the logging message.
Description	The description of logging message.

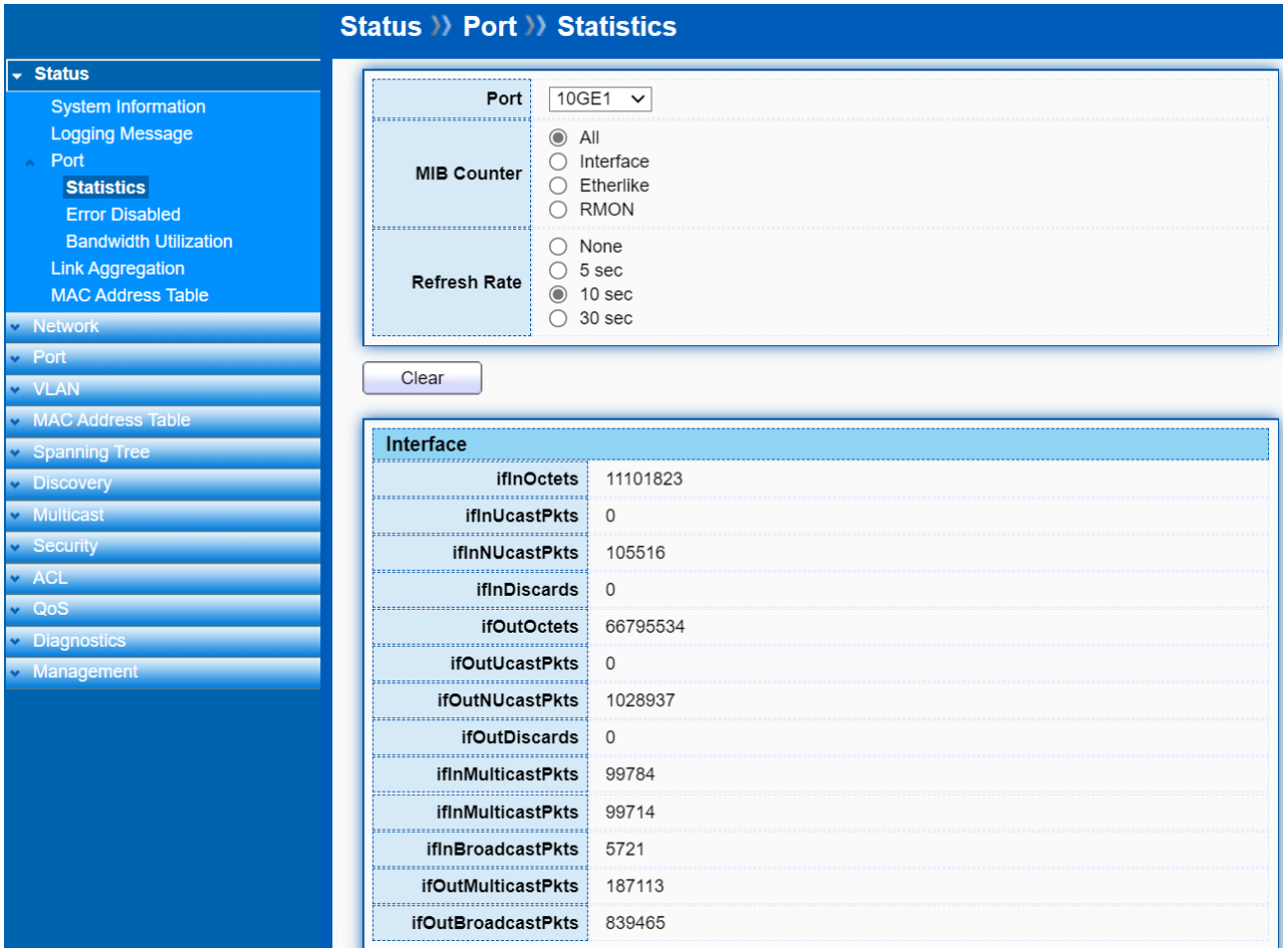
3.3 Port

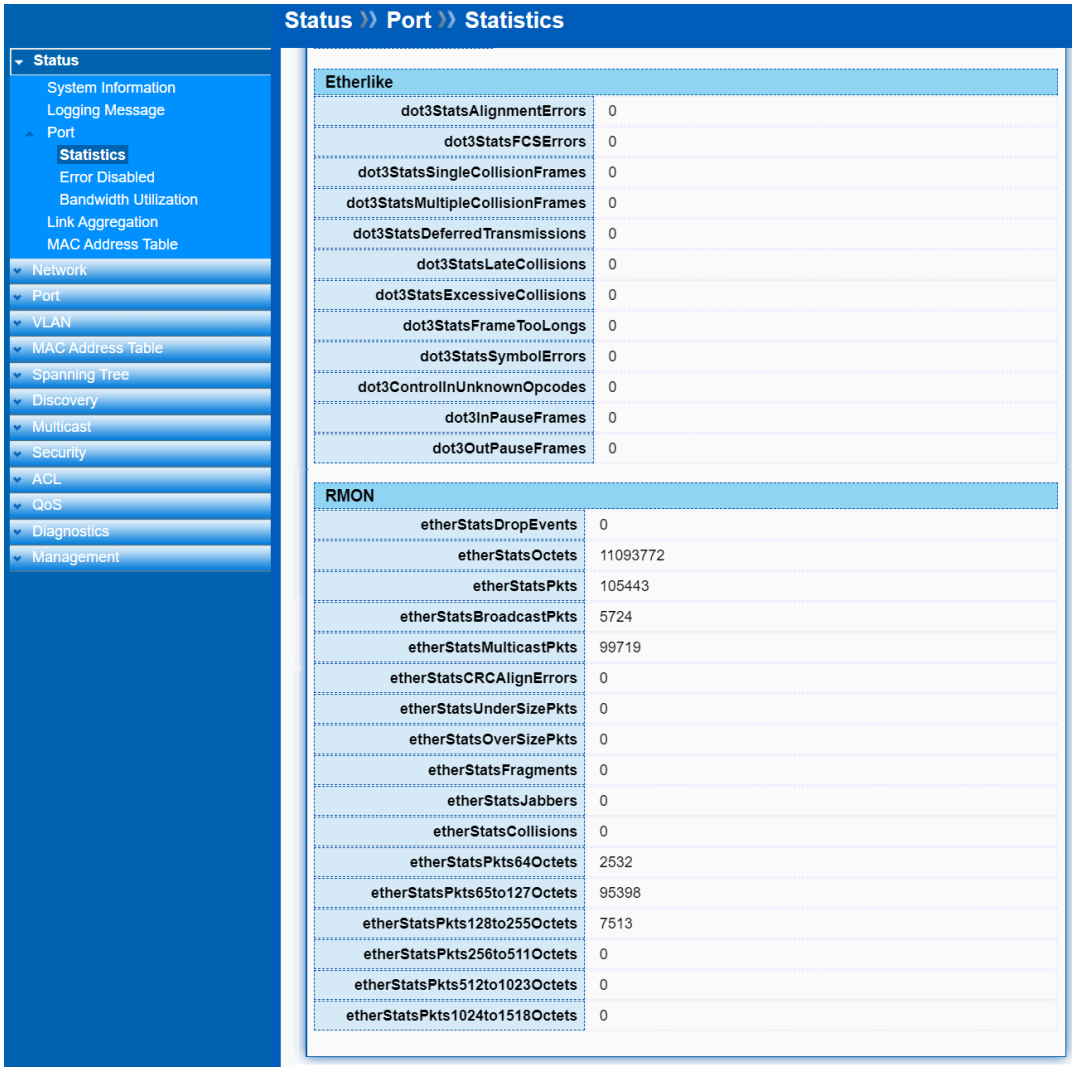
The port configuration page displays port summary and status information.

3.3.1 Statistics

Click **Status** > **Port** > **Statistics**

On this page user can get standard counters on network traffic from the interfaces, Ethernet-like and RMON MIB. Interfaces and Ethernet-like counters display errors on the traffic passing through each port. RMON counters provide a total count of different frame types and sizes passing through each port.





The "**Clear**" button will clear MIB counter of current selected port.

Field	Description
Port	Select one port to show counter statistics.
MIB Counter	Select the MIB counter to show different count type **All**: All counters. **Interface**: Interface related MIB counters **Etherlike**: Ethernet-like related MIB counters **RMON** : RMON related MIB counters
Refresh Rate	Refresh the web page every period of seconds to get new counter of specified port.

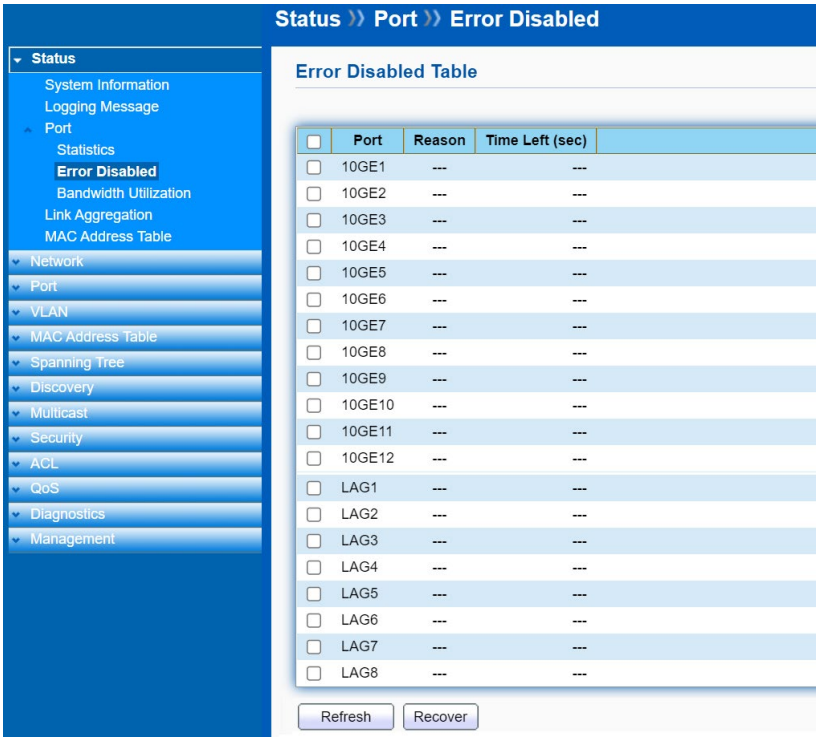
3.3.2 Error Disabled

Click **Status** > **Port** > **Error Disabled**

Error Disabled is a feature that automatically disables a port on a switch and this feature is designed to inform the administrator when there is a port problem or error. The reasons a switch can go into Error Disabled mode and shutdown a port are many and include: **BPDU Guard**, **UDLD**, **Self Loop**, **Broadcast Flood**, **Unknown Multicast Flood**, **Unicast Flood**, **ACL**, **Port Security**, **DHCP Rate**

Limit and **ARP Rate Limit**. When a port is in Error Disabled state, it is effectively shut down and no traffic is sent or received on that port.

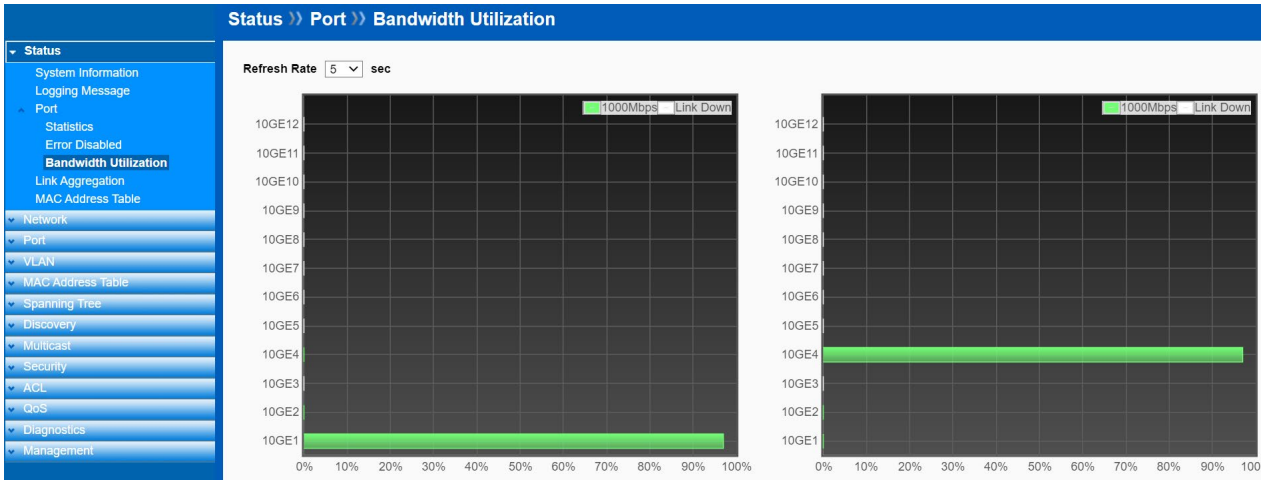
You can observe which port(s) is(are) disabled with the reason here. Click **Recover** to recover the port.



3.3.3 Bandwidth Utilization

Click **Status** > **Port** > **Bandwidth Utilization**

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

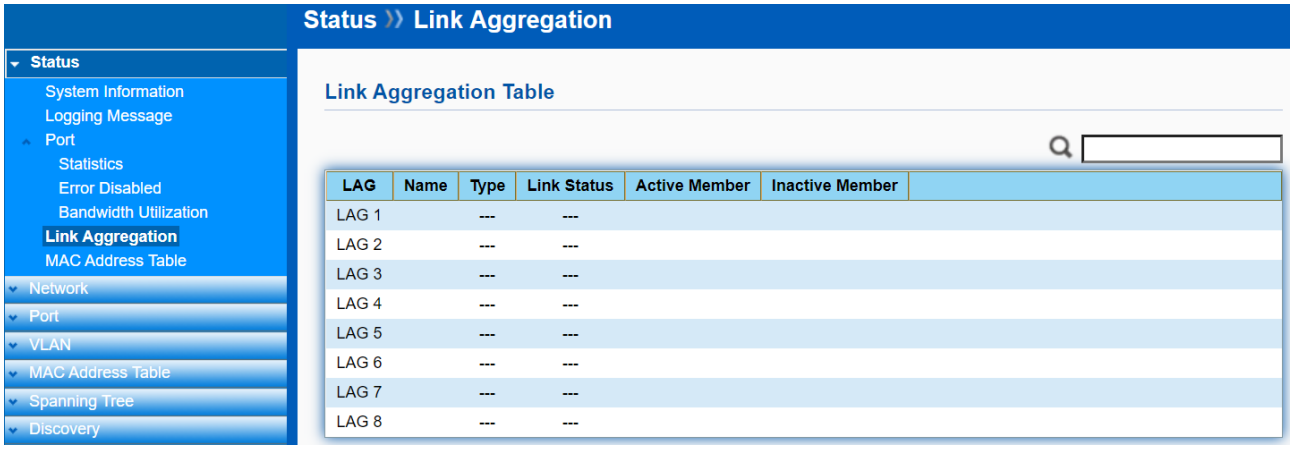


Field	Description
Refresh Rate	Refresh the web page every period of second to get new bandwidth utilization data.

3.4 Link Aggregation

Click **Status** > **Link Aggregation**

Display the Link Aggregation status of web page.

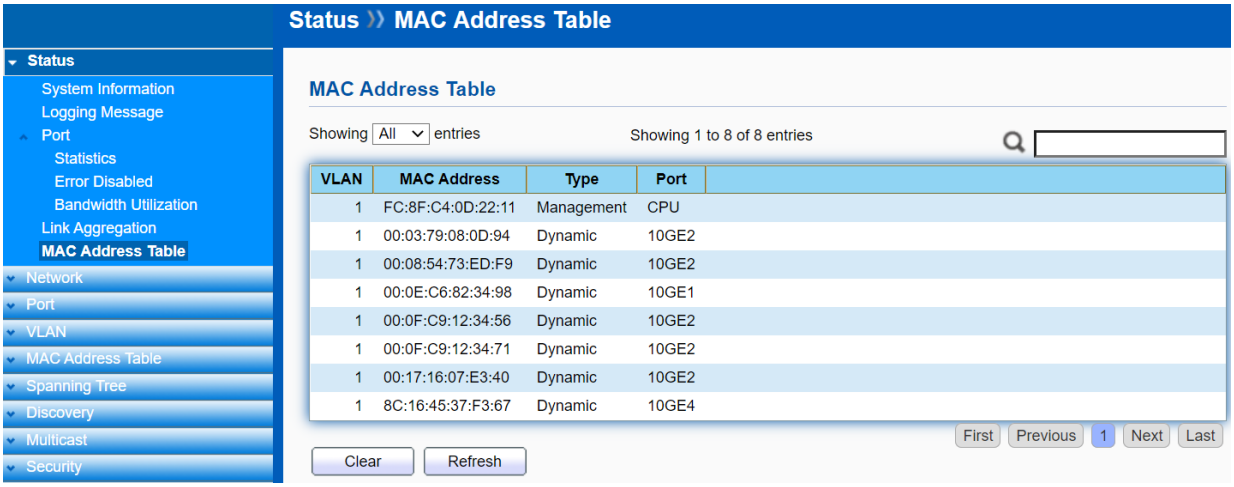


Field	Description
LAG	LAG Name.
Name	LAG port description
Type	The type of the LAG **Static**: The group of ports assigned to a static LAG are always active members. **LACP**: The group of ports assigned to dynamic LAG are candidate ports. LACP determines which candidate ports are active member ports.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

3.5 MAC Address Table

Click **Status** > **MAC Address Table**

The MAC address table page displays all MAC address entries on the switch including static MAC address created by administrator or auto learned from hardware.



The “**Clear**” button will clear all dynamic entries and “Refresh” button will retrieve latest MAC address entries and show them on page.

Field	Description
VLAN	VLAN ID of the MAC address.
MAC Address	MAC address
Type	The type of MAC address **Management**: DUT’s base MAC address for management purpose. **Static**: Manually configured by administrator. **Dynamic**: Auto learned by hardware.
Port	The type of port **CPU** : DUT’s CPU port for management purpose **Other** : Normal switch port

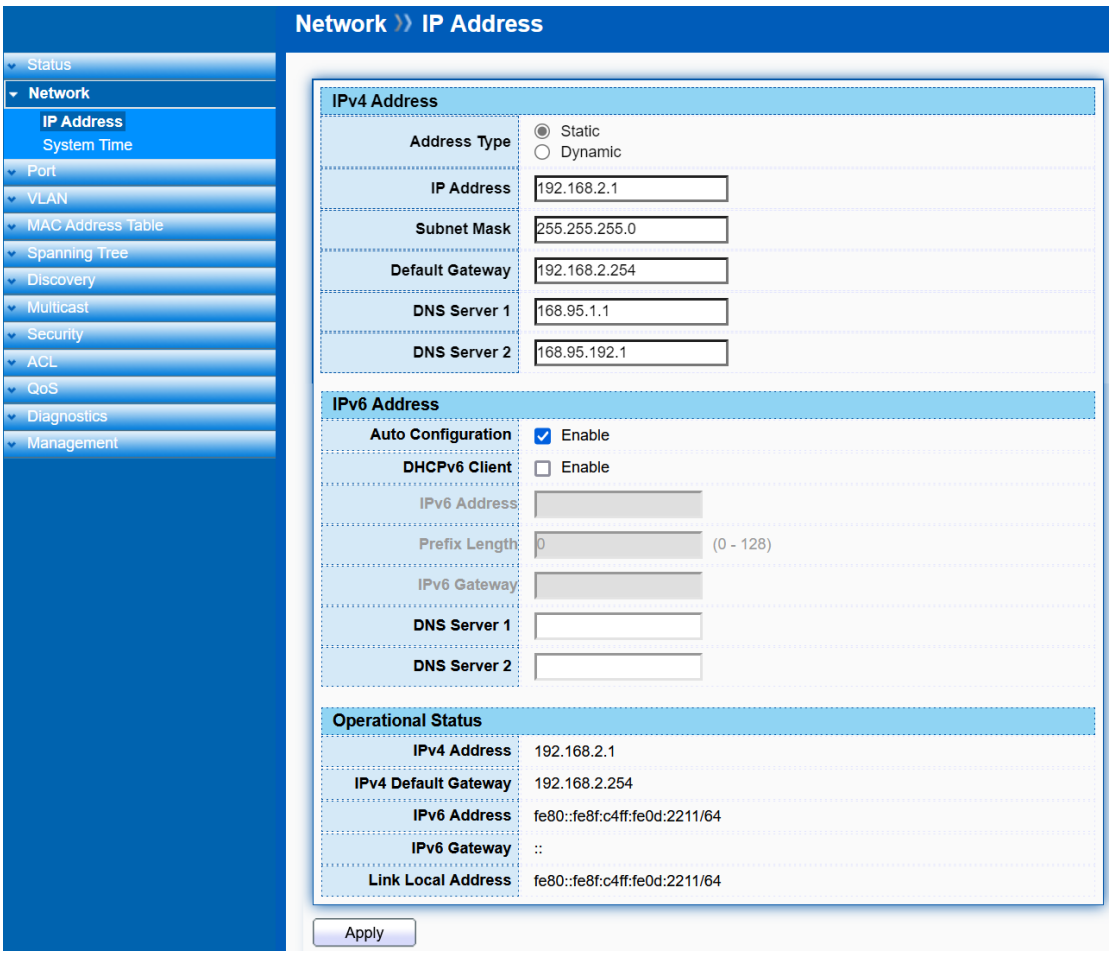
Chapter 4 Network

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

4.1 IP Address

Click **Network** > **IP Address**

Use the IP Setting screen to configure the switch IP address and the default gateway device. The gateway field specifies the IP address of the gateway (next hop) for outgoing traffic. The switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.2.1. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.



Field	Description
IPv4 Address Field	
Address Type	Select the address type of IP configuration ·**Static**: Static IP configured by users will be used. ·**Dynamic**: Enable DHCP to obtain IP information from a DHCP server on the network.

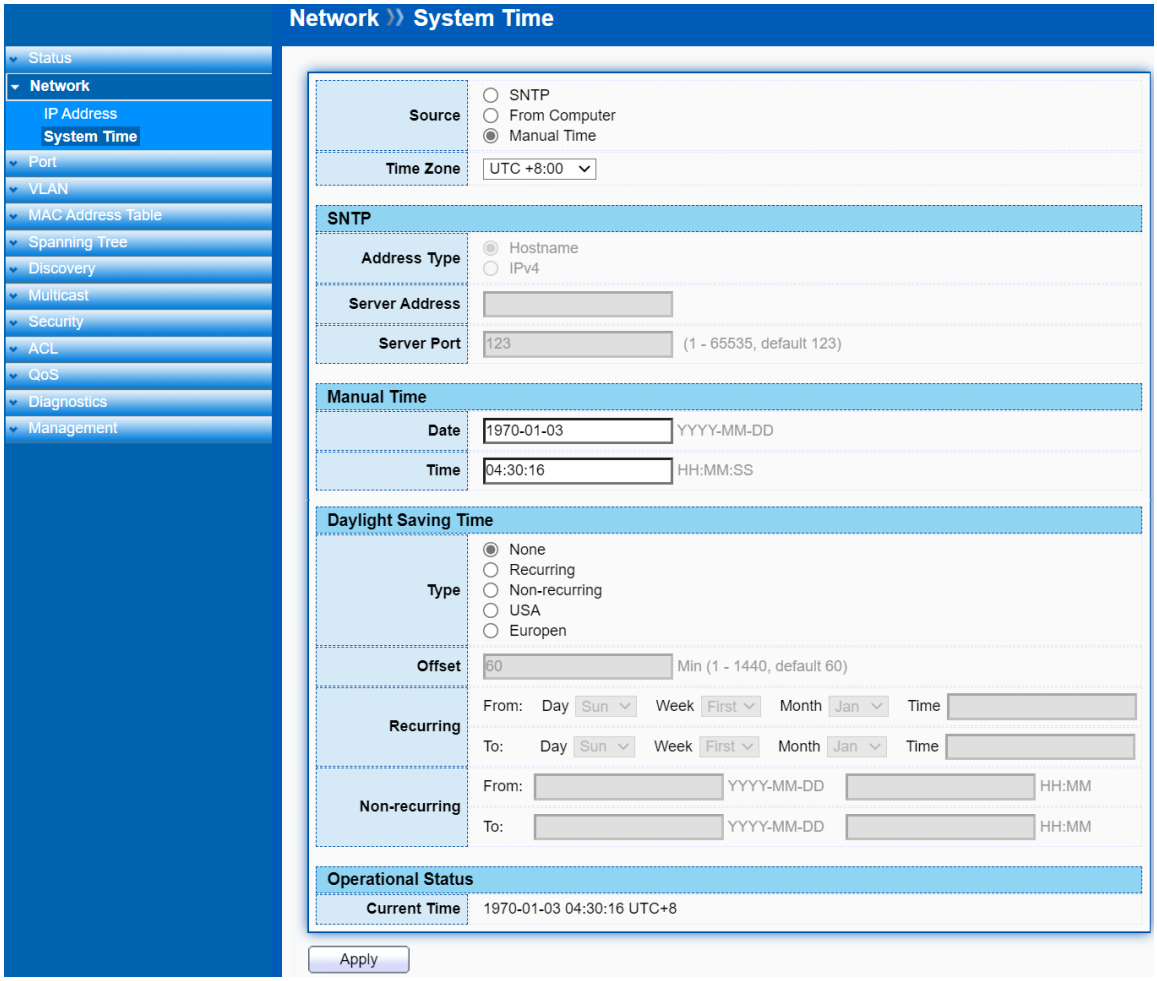
IP Address	Enter the IP address of your switch in dotted decimal notation for example 192.168.2.1. If static mode is enabled, enter IP address in this field.
Subnet Mask	Enter the IP subnet mask of your switch in dotted decimal notation for example 255.255.255.0. If static mode is enabled, enter subnet mask in this field.
Default Gateway	Specify the default gateway on the static configuration. The default gateway must be in the same subnet with switch IP address configuration
DNS Server 1	If static mode is enabled, enter primary DNS server address in this field.
DNS Server 2	If static mode is enabled, enter secondary DNS server address in this field.
IPv6 Address Field	
Auto Configuration	Select **Enable** or **Disable** the IPv6 auto configuration.
DHCPv6 Client	DHCPv6 client state. ·**Enable**: Enable DHCPv6 client function. ·**Disable**: Disable DHCPv6 client function
IPv6 Address	Specify the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.
IPv6 Prefix	Specify the prefix for the IPv6 address, when the IPv6 auto configuration and DHCPv6 client are disabled.
Gateway	Specify the IPv6 default gateway, when the IPv6 auto configuration and DHCPv6 client are disabled.
DNS Server 1	Specify the primary user-defined IPv6 DNS server configuration.
DNS Server 2	Specify the secondary user-defined IPv6 DNS server configuration.
Operational Status	
IPv4 Address	The operational IPv4 address of the switch.
IPv4 Gateway	The operational IPv4 gateway of the switch.
IPv6 Address	The operational IPv6 address of the switch.
IPv6 Gateway	The operational IPv6 gateway of the switch.
Link Local Address	The operational IPv6 link local address for the switch.

4.2 System Time

Click **Network** > **System Time**

This page allow user to set time source, static time, time zone and daylight saving settings.

Time zone and daylight saving takes effect both static time or time from SNTP server.



Field	Description
Source	Select the time source ·**SNTP**: Time sync from NTP server. ·**From Computer**: Time set from browser host. ·**Manual Time**: Time set by manually configure.
Time Zone	Select a time zone difference from listing district.
SNTP	
Address Type	Select the address type of NTP server. This is enabled when time source is SNTP.
Server Address	Input IPv4 address or hostname for NTP server. This is enabled when time source is SNTP.
Server Port	Input NTP port for NTP server. Default is 123. This is enabled when time source is SNTP.
Manual Time	
Date	Input manual date. This is enabled when time source is manual.
Time	Input manual time. This is enabled when time source is manual.
Daylight Saving Time	
Type	Select the mode of daylight saving time. **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 in March and ending on the last Sunday in October.
Offset	Specify the adjust offset of daylight saving time.
Recurring From	Specify the starting time of recurring daylight saving time. This field available when selecting “Recurring” mode.
Recurring To	Specify the ending time of recurring daylight saving time. This field available when selecting “Recurring” mode.
Non-recurring From	Specify the starting time of non-recurring daylight saving time. This field available when selecting “Non-Recurring” mode.
Non-recurring To	Specify the ending time of non-recurring daylight saving time. This field available when selecting “Non-Recurring” mode.

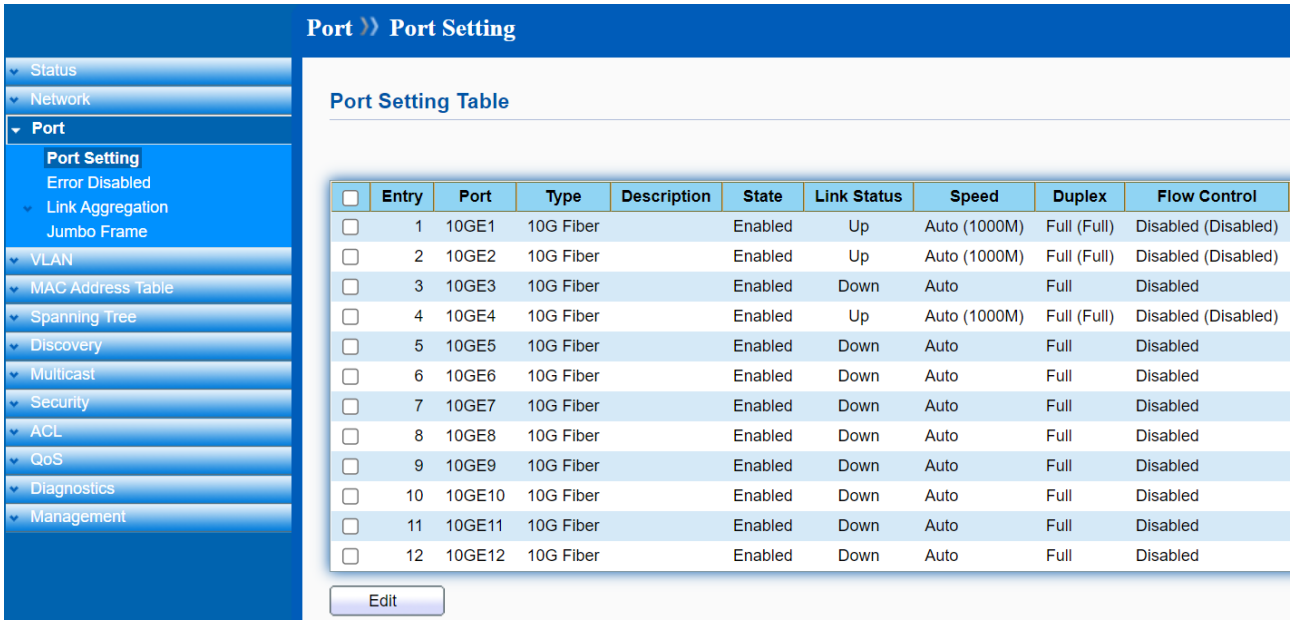
Chapter 5 Port

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

5.1 Port Setting

Click **Port** > **Port Setting**

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

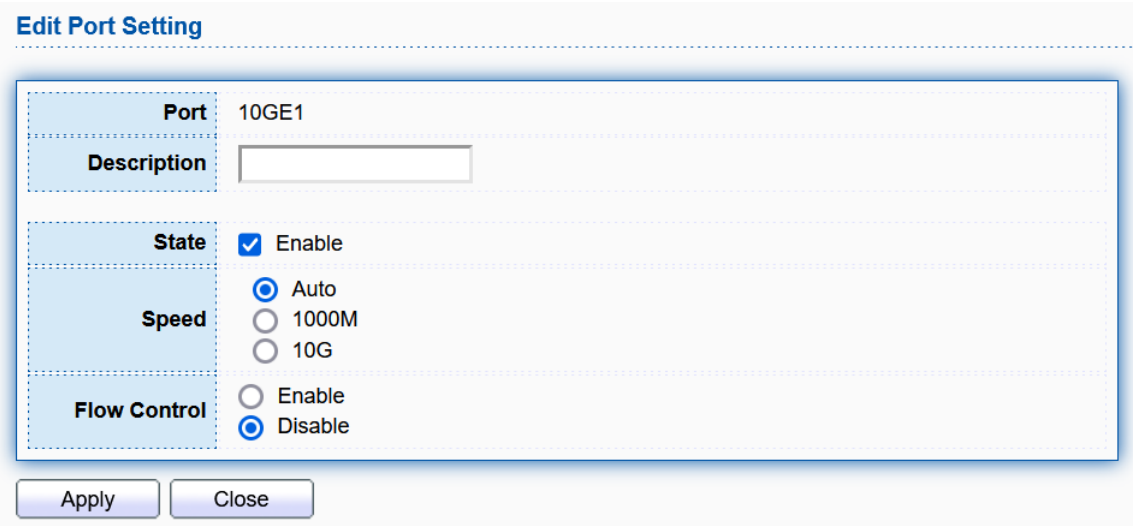


Field	Description
Port	Port Name.
Type	Allows you to Enable/Disable the port. When Enable is selected, the port can forward the packets normally.
Description	Port description
State	Port admin state. **Enabled**: Enable the port. **Disabled**: Disable the port.
Link Status	Current port link status **Up**: Port is link up. **Down**: Port is link down.
Speed	Current port speed configuration and link speed status.
Duplex	Current port duplex configuration and link duplex status.
Flow Control	Current port flow control configuration and link flow control status.

Note:

1. The switch can't be managed through the disable port.
2. The switch might lose connection temporarily for the specific port (which connect to the management PC) setting. If it happens, refresh WEB GUI can recover the connection.

Edit Port Setting

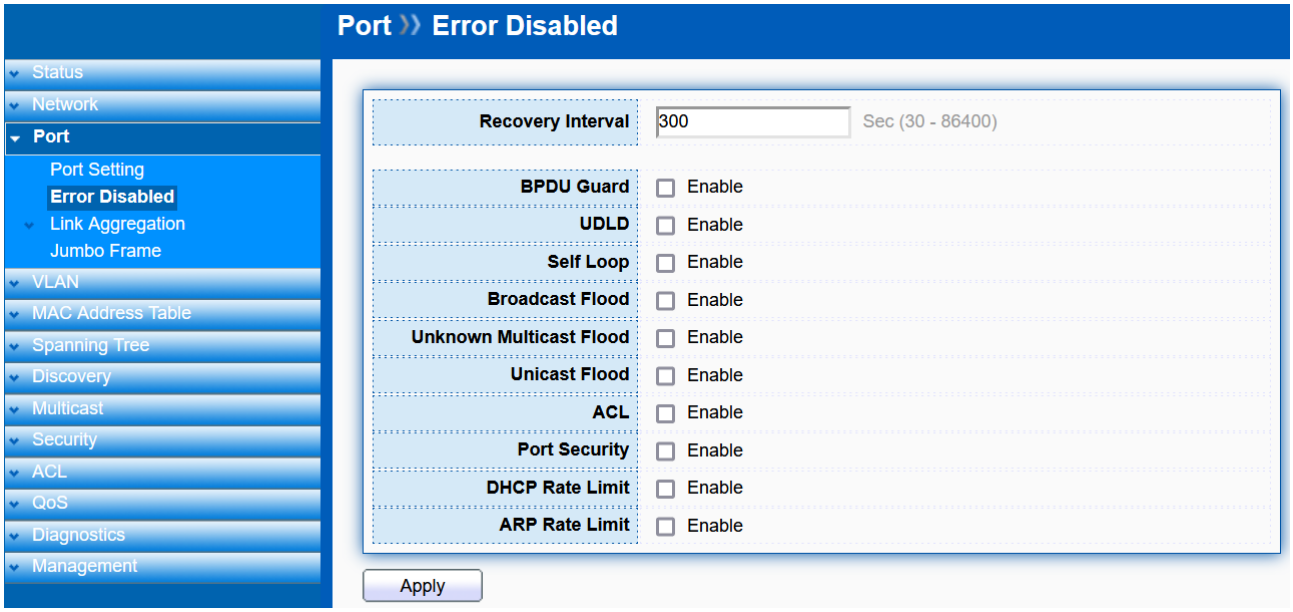


Field	Description
Port	Selected Port list.
Description	Port description
State	Port admin state. **Enabled**: Enable the port. **Disabled**: Disable the port.
Link Status	Current port link status **Up**: Port is link up. **Down**: Port is link down.
Speed	Select the Port speed/duplex capabilities for the ports you need: ·**Auto**: Auto-negotiation speed/ duplex with all capabilities. ·**1000M**: Force speed with 1000M ability ·**10G**: Force speed with 10G ability
Flow Control	Port flow control capabilities ·**Enabled**: Enable flow control ability. ·**Disabled**: Disable flow control ability.

5.2 Error Disabled

Click **Port** > **Error Disabled**

Error Disabled is a feature that automatically disables a port on a switch and this feature is designed to inform the administrator when there is a port problem or error. The reasons a switch can go into Error Disabled mode and shutdown a port are many and include: **BPDU Guard**, **UDLD**, **Self Loop**, **Broadcast Flood**, **Unknown Multicast Flood**, **Unicast Flood**, **ACL**, **Port Security**, **DHCP Rate Limit** and **ARP Rate Limit**. When a port is in Error Disabled state, it is effectively shut down and no traffic is sent or received on that port.



Field	Description
BPDU Guard	Enable STP and enable BPDU Guard. When the port receive the BPDU packet.
UDLD	When UDLD (UniDirectional Link Detection) happened.
Self Loop	Enable STP and disable BPDU Guard. When the port receive the BPDU from itself.
Broadcast Flood	The incoming broadcast packets on the port exceed the rate limit set in **Storm Control** and set **Action** to **Shutdown**.
Unknown Multicast Flood	The incoming unknown multicast packets on the port exceed the rate limit set in **Storm Control** and set **Action** to **Shutdown**.
Unicast Flood	The incoming unknown unicast packets on the port exceed the rate limit set in **Storm Control** and set **Action** to **Shutdown**
ACL	The packets match the rules set in **ACL** and set **Action** to **Shutdown**.
Port Security	The number of learning MAC addresses in the port exceeds the limit set in **Port Security** and set **Action** to **Shutdown**.
DHCP Rate Limit	The incoming DHCP packets on the port exceed the rate limit set in **DHCP Snooping**.
ARP Rate Limit	The incoming ARP packets on the port exceed the rate limit set in **Dynamic ARP Inspection**.

5.3 Link Aggregation

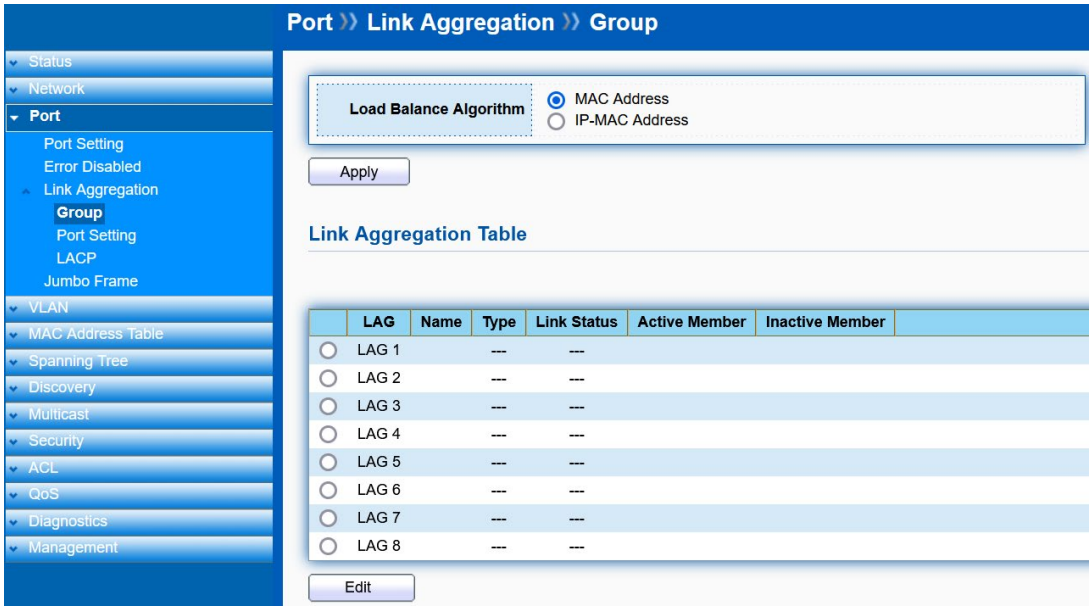
Click **Port** > **Link Aggregation**

The Link Aggregation is used to combine a number of ports together to make a single high-bandwidth data path, which can highly extend the bandwidth.

5.3.1 Trunk Group Setting

Click **Port** > **Link Aggregation** > **Group**

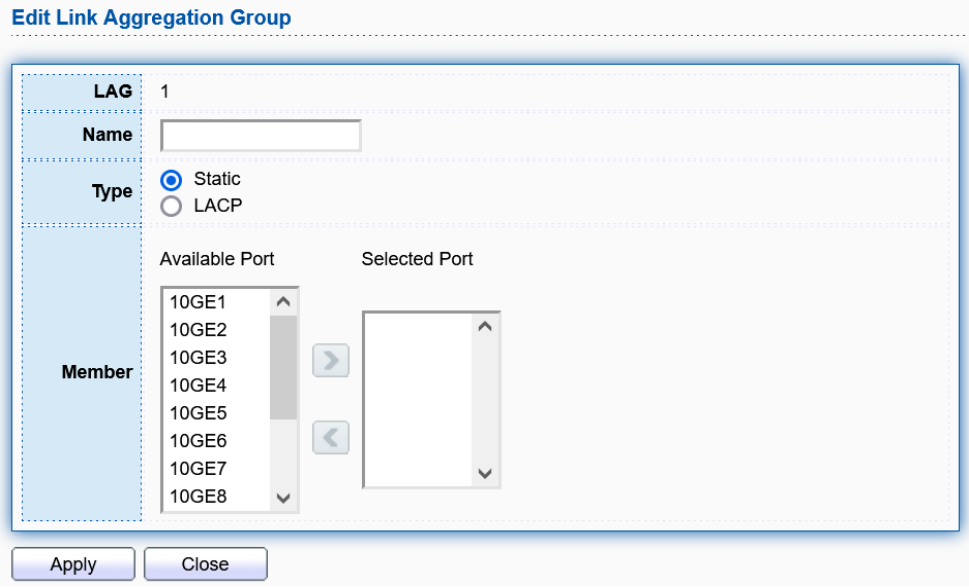
This page allow user to configure link aggregation group load balance algorithm and group member.



Field	Description
Load Balance Algorithm	LAG load balance distribution algorithm. **MAC Address**: Based on MAC address **IP-MAC Address**: Based on MAC address and IP address
LAG	LAG (Link Aggregation Group) Name.
Name	LAG port description
Type	The type of the LAG. **Static**: The group of ports assigned to a static LAG are always active members. **LACP**: The group of ports assigned to dynamic LAG are candidate ports. LACP determines which candidate ports are active member ports.
Link Status	LAG port link status.
Active Member	Active member ports of the LAG.
Inactive Member	Inactive member ports of the LAG.

Select Link Aggregation Table and click “**Edit**” button to edit LAG setting.

Edit LAG Group Setting

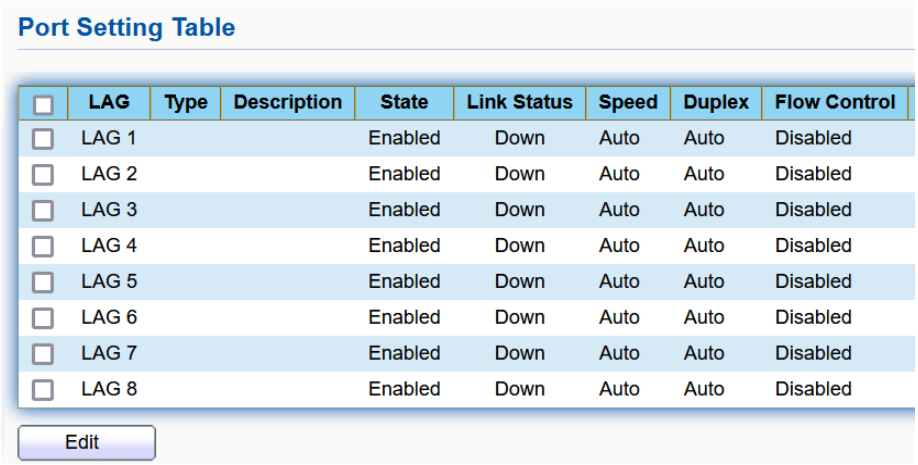


Field	Description
LAG	Selected LAG Group ID
Name	LAG port description
Type	The type of the LAG. **Static**: The group of ports assigned to a static LAG are always active members. **LACP**: The group of ports assigned to dynamic LAG are candidate ports. LACP determines which candidate ports are active member ports.
Member	Select available port to be LAG group member port.

5.3.2 Port Setting

Click **Port** > **Link Aggregation** > **Port Setting**

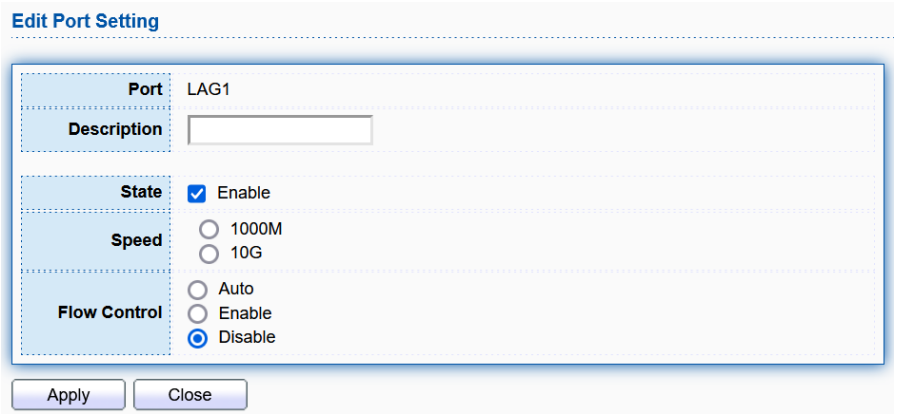
This page shows LAG port current status and allows user to edit LAG port configurations.



Field	Description
LAG	LAG Port Name
Type	LAG Port media type
Description	LAG port description

State	LAG Port admin state. **Enable**: Enable the port **Disable**: Disable the port
Link Status	Current LAG port link status. **Up**: Port is link up **Down**: Port is link down
Speed	Current LAG port speed configuration and link speed status.
Duplex	Current LAG port duplex configuration and link duplex status.
Flow Control	Current LAG port flow control configuration and link flow control status.

Select Port Setting Table and click "**Edit**" button to edit port setting.

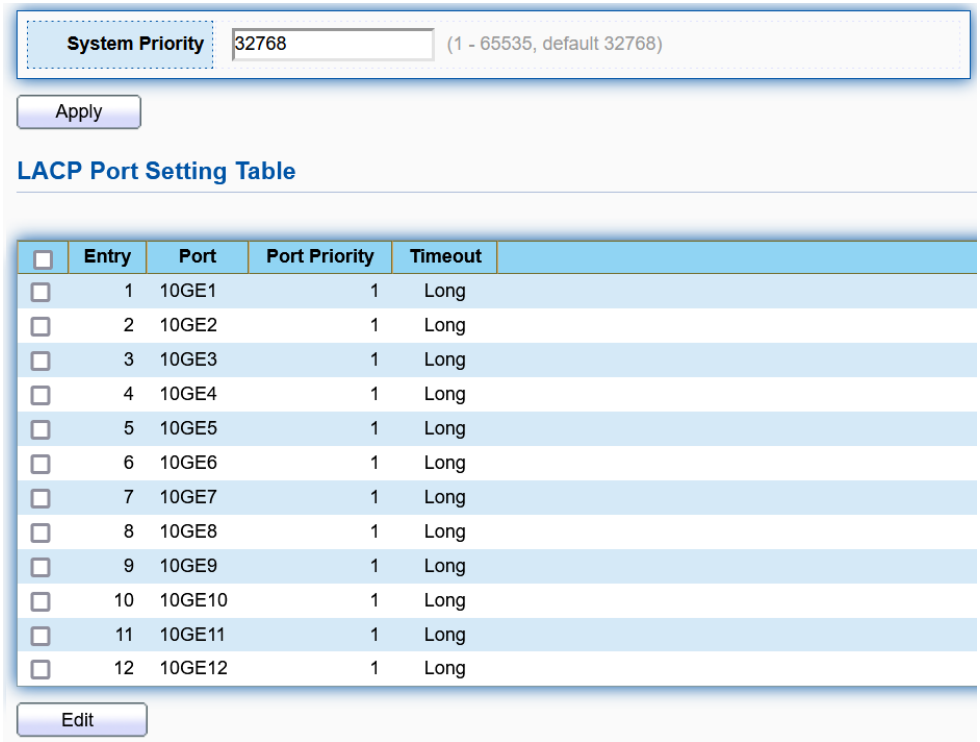


Field	Description
Port	Selected port list
Description	Port description
State	Port admin state **Enable**: Enable the port **Disable**: Disable the port
Speed	Port speed capabilities. ·**1000M**: Force speed with 1000M ability. ·**10G**: Force speed with 10G ability
Flow Control	Port flow control. ·**Auto**: Auto flow control by negotiation. ·**Enabled**: Enable flow control ability. ·**Disabled**: Disable flow control ability.

5.3.3 LACP

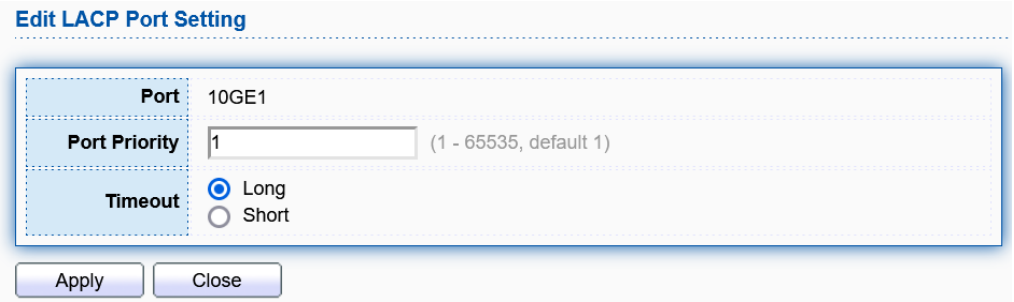
Click **Port** > **Link Aggregation** > **LACP**

This page allow user to configure LACP global and port configurations.



Field	Description
System Priority	Configure the system priority of LACP. This decides the system priority field in LACP PDU.
Port	Port Name.
Port Priority	LACP priority value of the port.
Timeout	The periodic transmissions type of LACP PDUs. **Long**: Transmit LACP PDU with slow periodic (30s). **Short**: Transmit LACP PDU with fast periodic (1s).

Select ports and click "**Edit**" button to edit port configuration.

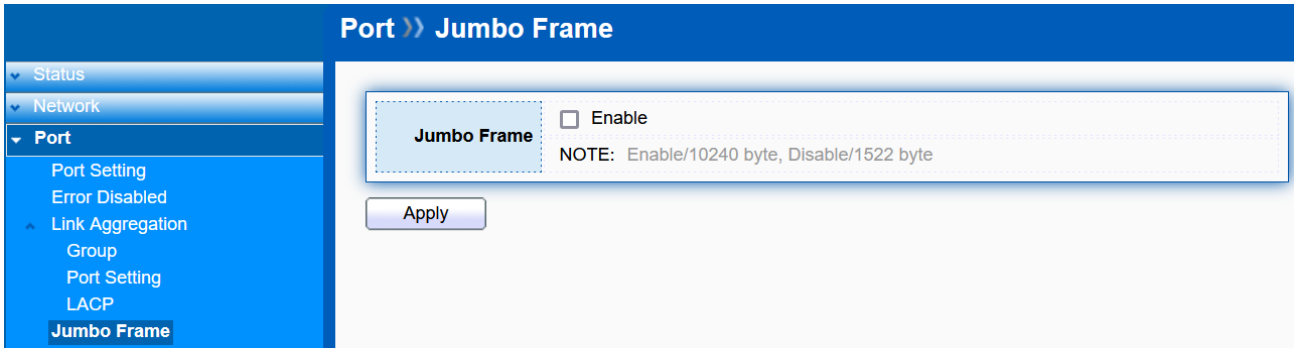


Field	Description
Port	Selected port list.
Port Priority	Enter the LACP priority value of the port.
Timeout	The periodic transmissions type of LACP PDUs. **Long**: Transmit LACP PDU with slow periodic (30s). **Short**: Transmit LACP PDU with fast periodic (1s).

5.4 Jumbo Frame

Click **Port** > **Jumbo Frame**

This page allows user to configure switch jumbo frame size.



Field	Description
Jumbo Frame	Enable or Disable jumbo frame. When jumbo frame is enabled, the frame size 10240 will be used. When jumbo frame is disabled, default frame size 1522 will be used.

Chapter 6 VLAN

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

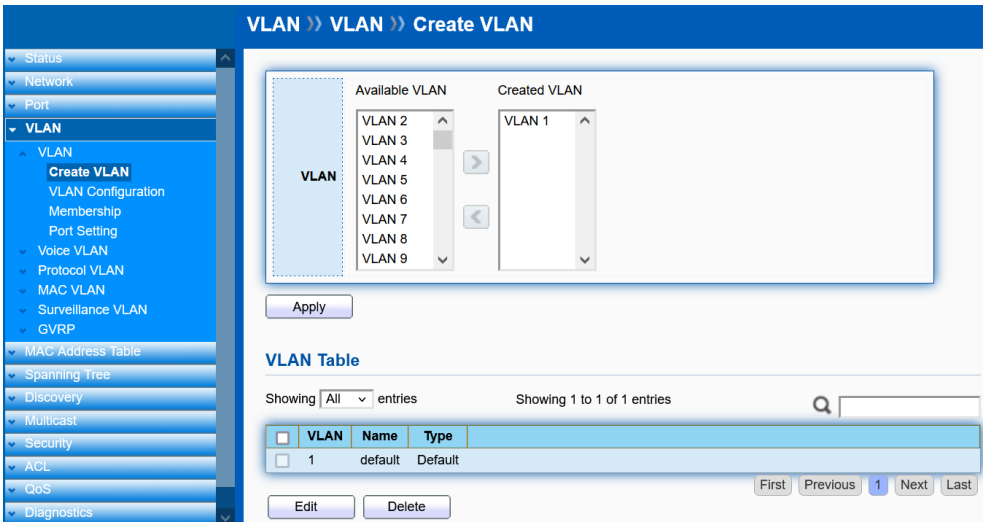
6.1 VLAN

Use the VLAN pages to configure settings of VLAN and all VLAN-related protocol.

6.1.1 Create VLAN

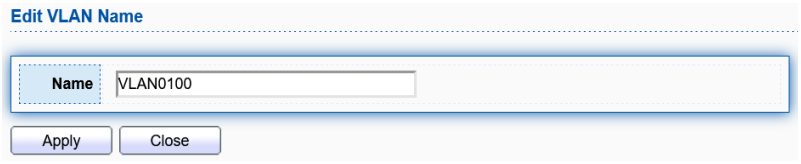
Click **VLAN** > **VLAN** > **Create VLAN**

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



Field	Description
Available VLAN	VLAN has not created yet. Select available VLANs from left box then move to right box to add.
Created VLAN	VLAN had been created. Select created VLANs from right box then move to left box to delete.

Click "**Edit**" button to edit VLAN name

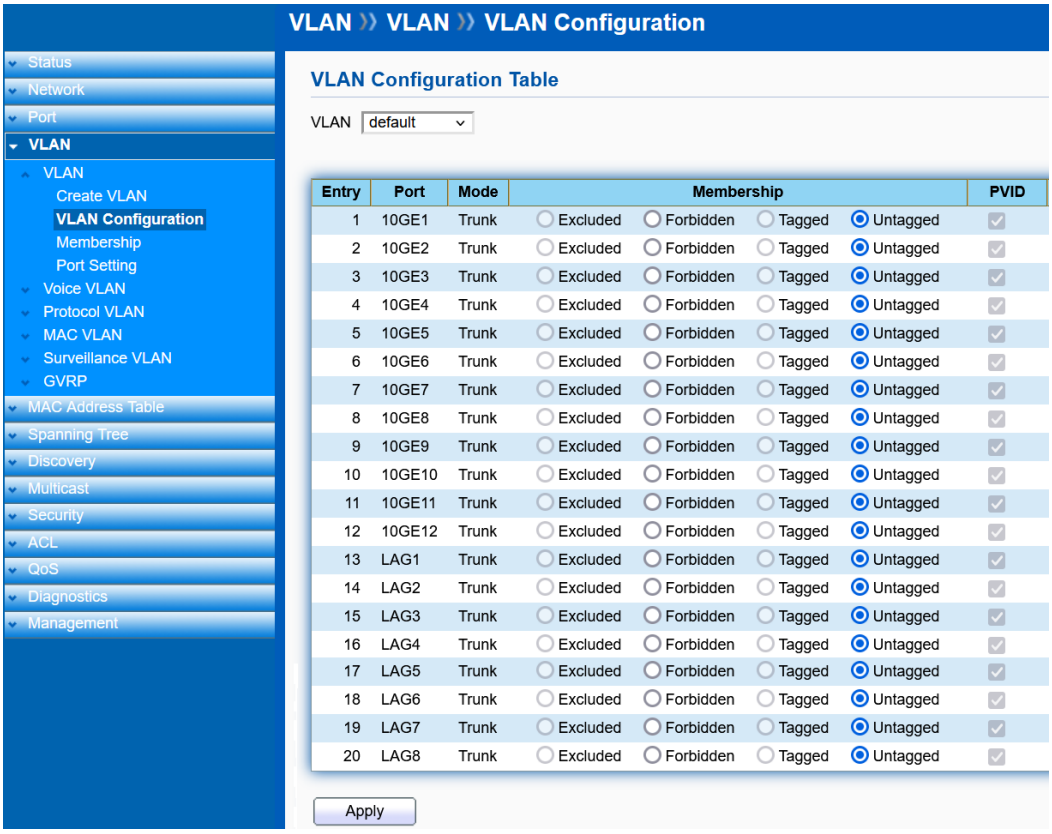


Field	Description
Name	Input VLAN name.

6.1.2 VLAN Configuration

Click **VLAN** > **VLAN** > **VLAN Configuration**

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

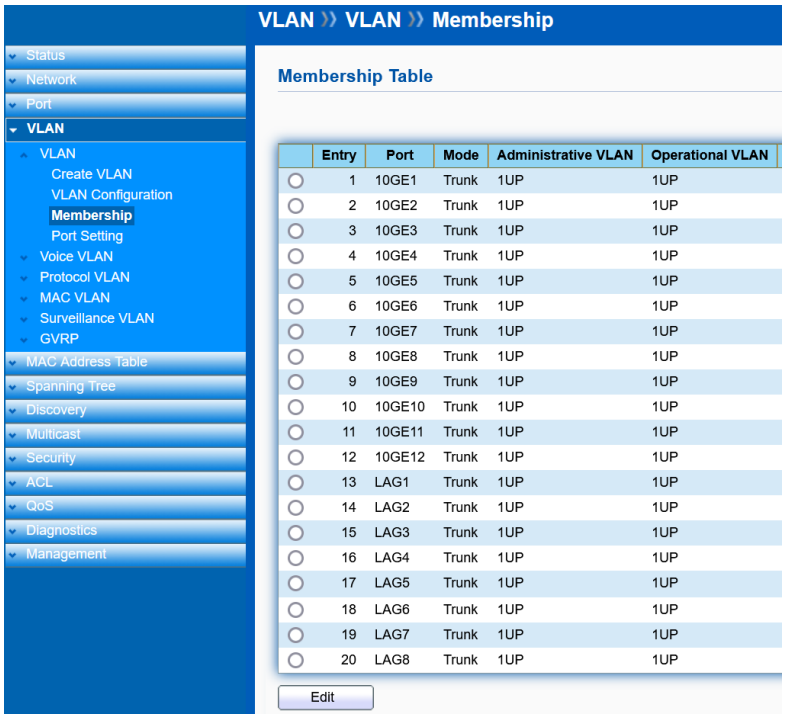


Field	Description
VLAN	Select specified VLAN ID to configure VLAN configuration.
Port	Display the interface of port entry.
Mode	Display the interface VLAN mode of port.
Membership	Select the membership for this port of the specified VLAN ID. **Forbidden**: Specify the port is forbidden in the VLAN. **Excluded**: Specify the port is excluded in the VLAN. **Tagged**: Specify the port is tagged member in the VLAN. **Untagged**: Specify the port is untagged member in the VLAN.
PVID	Display if it is PVID of interface.

6.1.3 Membership

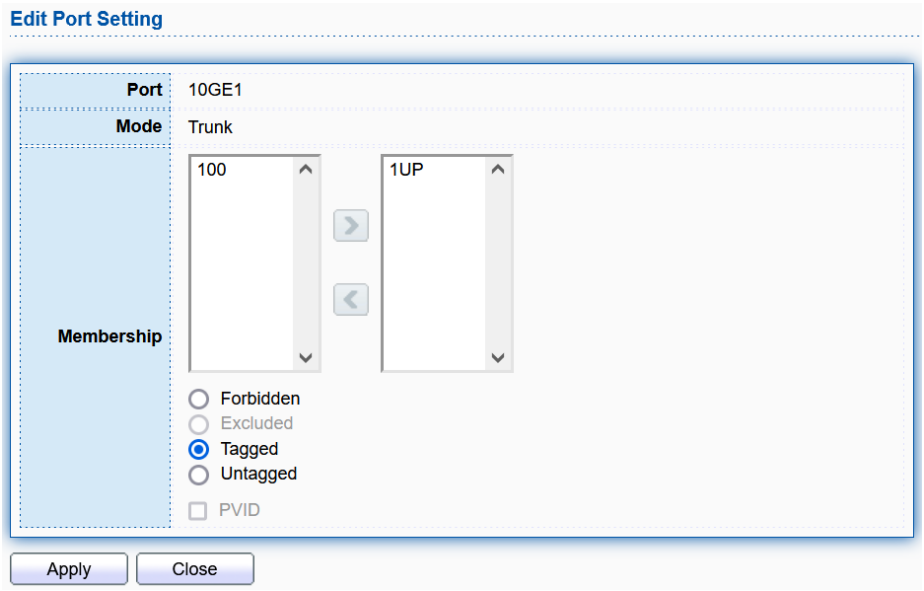
Click **VLAN** > **VLAN** > **Membership**

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



Field	Description
Port	Display the interface of port entry.
Mode	Display the interface VLAN mode of port.
Administrative VLAN	Display the administrative VLAN list of this port.
Operational VLAN	Display the operational VLAN list of this port. Operational VLAN means the VLAN status that really runs in device. It may different to administrative VLAN.

Click “**Edit**” button to edit VLAN membership



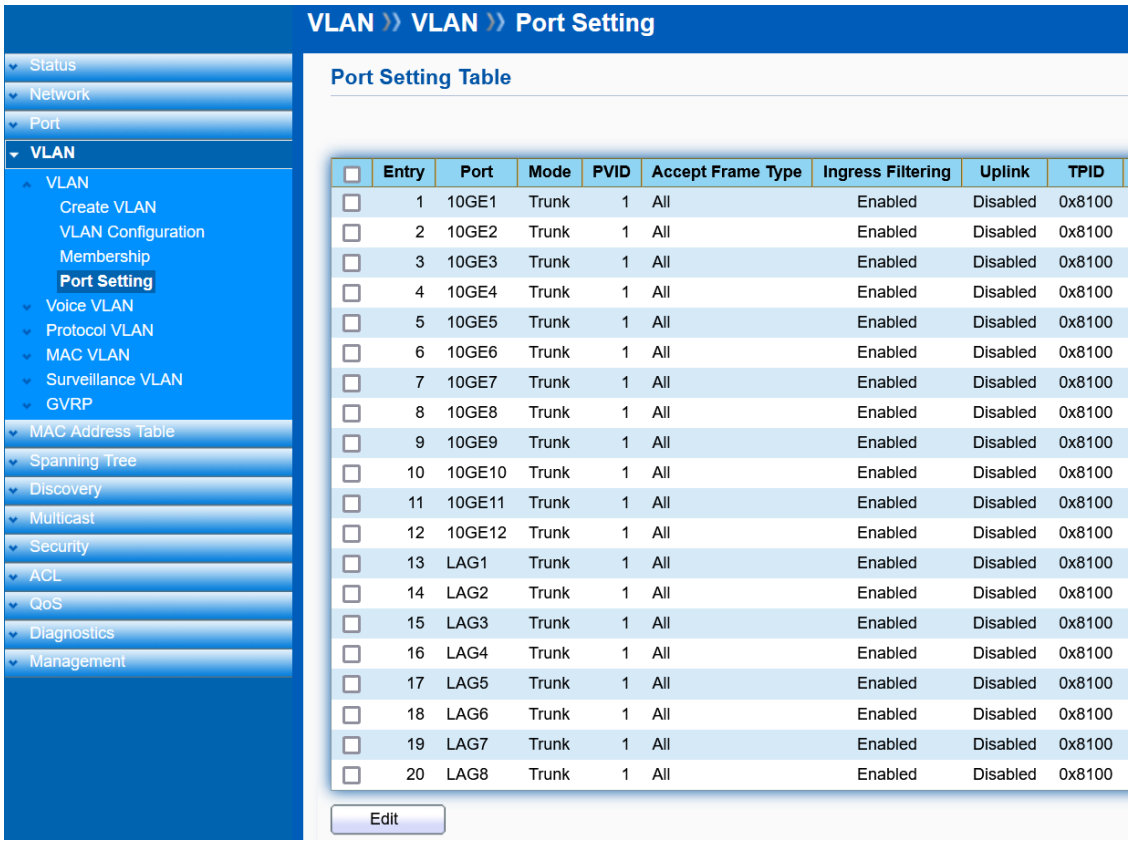
Field	Description
Port	Display the interface of port entry.
Mode	Display the VLAN mode of interface.
Membership	Select VLANs of left box and select one of following membership then move to right box to add membership. Select VLANs of right box then move to left box to remove membership. Tagging membership may not choose in differ VLAN port mode. **Forbidden**: Set VLAN as forbidden VLAN.

	Excluded: Set option is always disabled. **Tagged**: Set VLAN as tagged VLAN. **Untagged**: Set VLAN as untagged VLAN. **PVID**: Check this checkbox to select the VLAN ID to be the port-based VLAN ID for this port. PVID may auto select or can't select in differ settings.

6.1.4 Port Setting

Click **VLAN** > **VLAN** > **Port Setting**

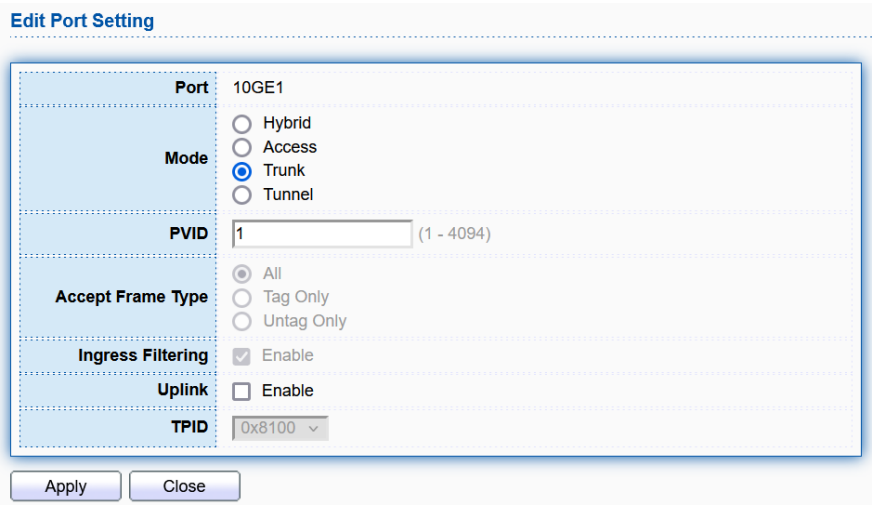
This page allows user to configure port VLAN settings such as VLAN port mode, PVID etc. The attributes depend on different VLAN port mode.



Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
1	10GE1	Trunk	1	All	Enabled	Disabled	0x8100
2	10GE2	Trunk	1	All	Enabled	Disabled	0x8100
3	10GE3	Trunk	1	All	Enabled	Disabled	0x8100
4	10GE4	Trunk	1	All	Enabled	Disabled	0x8100
5	10GE5	Trunk	1	All	Enabled	Disabled	0x8100
6	10GE6	Trunk	1	All	Enabled	Disabled	0x8100
7	10GE7	Trunk	1	All	Enabled	Disabled	0x8100
8	10GE8	Trunk	1	All	Enabled	Disabled	0x8100
9	10GE9	Trunk	1	All	Enabled	Disabled	0x8100
10	10GE10	Trunk	1	All	Enabled	Disabled	0x8100
11	10GE11	Trunk	1	All	Enabled	Disabled	0x8100
12	10GE12	Trunk	1	All	Enabled	Disabled	0x8100
13	LAG1	Trunk	1	All	Enabled	Disabled	0x8100
14	LAG2	Trunk	1	All	Enabled	Disabled	0x8100
15	LAG3	Trunk	1	All	Enabled	Disabled	0x8100
16	LAG4	Trunk	1	All	Enabled	Disabled	0x8100
17	LAG5	Trunk	1	All	Enabled	Disabled	0x8100
18	LAG6	Trunk	1	All	Enabled	Disabled	0x8100
19	LAG7	Trunk	1	All	Enabled	Disabled	0x8100
20	LAG8	Trunk	1	All	Enabled	Disabled	0x8100

Field	Description
Port	Display the interface.
Mode	Display the VLAN mode of port.
PVID	Display the Port-based VLAN ID of port.
Accept Frame Type	Display accepted frame type of port.
Ingress Filtering	Display ingress filter status of port.
Uplink	Display the Uplink status of port.
TPID	Display the TPID of port.

Click "**Edit**" button to edit VLAN port setting



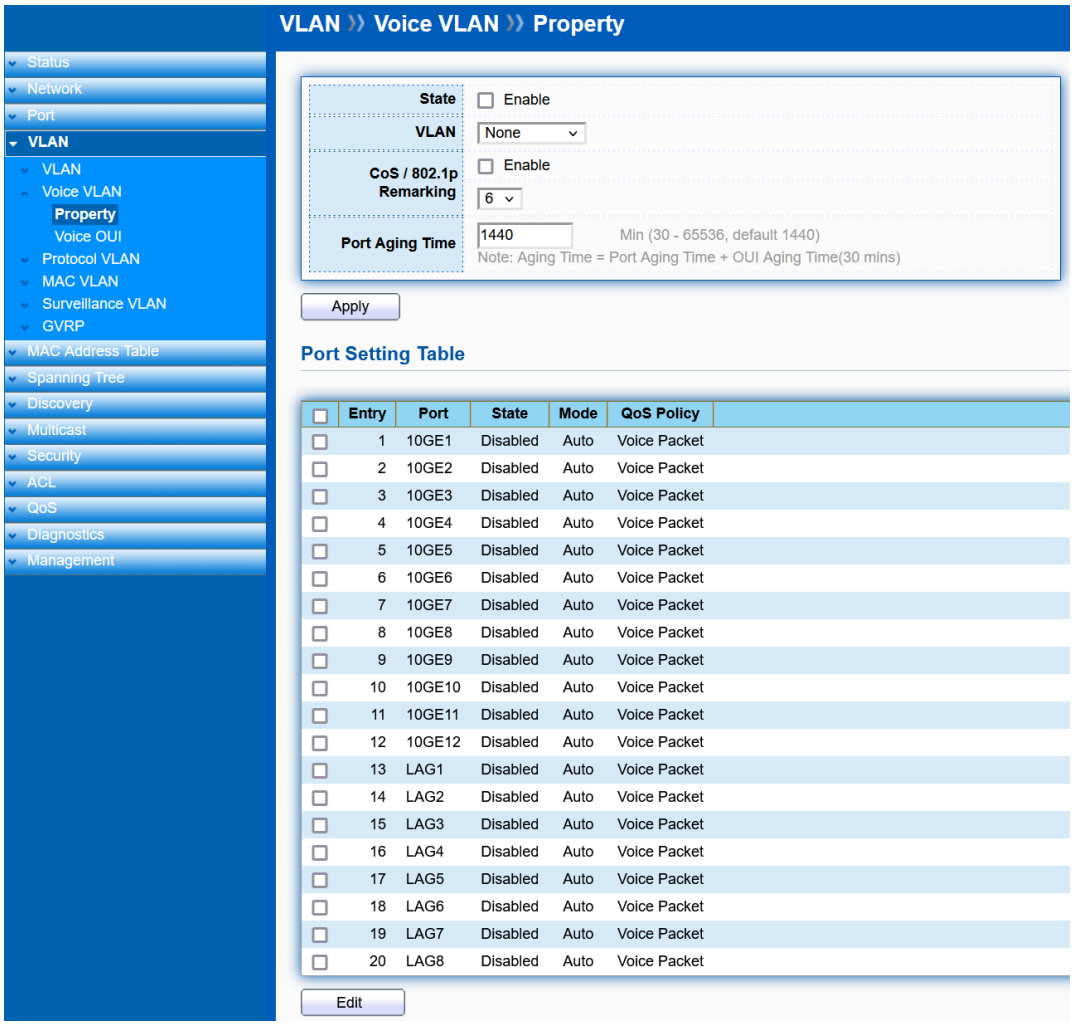
Field	Description
Port	Display the interface of port entry.
Mode	Select the VLAN mode of the interface. **Hybrid**: Support all functions as defined in IEEE802.1Q specification. **Access**: Accepts only untagged frames and join an untagged VLAN. **Trunk**: An untagged member of one VLAN at most, and is a tagged member of zero or more VLANs.
PVID	Specify the port-based VLAN ID (1~4094). It's only available with hybrid and Trunk mode.
Accept Frame Type	Specify the acceptable-frame-type of the specified interfaces. It's only available with Hybrid mode.
Ingress Filtering	Specify the status of ingress filtering. It's only available with Hybrid mode.
Uplink	Check to enable Uplink. It's only available with Trunk mode.
TPID	The options are: 0x8100, 0x88a8, 0x9100, 0x9200.

6.2 Voice VLAN

6.2.1 Property

Click **VLAN** > **Voice VLAN** > **Property**

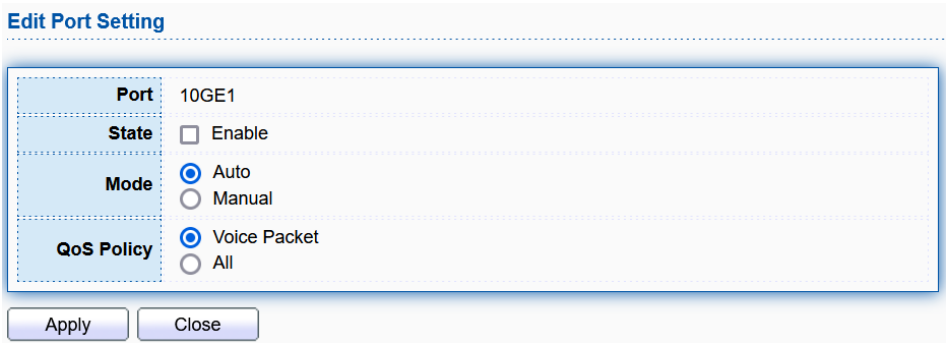
This page allows user to configure global and per interface setting of voice VLAN.



Field	Description
State	Set checkbox to enable or disable voice VLAN function.
VLAN	Select Voice VLAN ID. Voice VLAN ID cannot be default VLAN.
Cos/802.1p Remarking	Set checkbox to enable or disable 1p remarking. If enabled, qualified packets will be remark by this value. Select a value of VPT. Qualified packets will use this VPT value as inner priority. (Range: 0-7; Default: 6)
Aging Time	Input value of aging time. Default is 1440 minutes. A voice VLAN entry will be age out after this time if without any packet pass through.

Field	Description
Port	Display port entry
State	Display enable/disable status of interface.
Mode	Display voice VLAN mode.
QoS Policy	Display voice VLAN remark will effect which kind of packet

Click “**Edit**” button to edit Property Port.

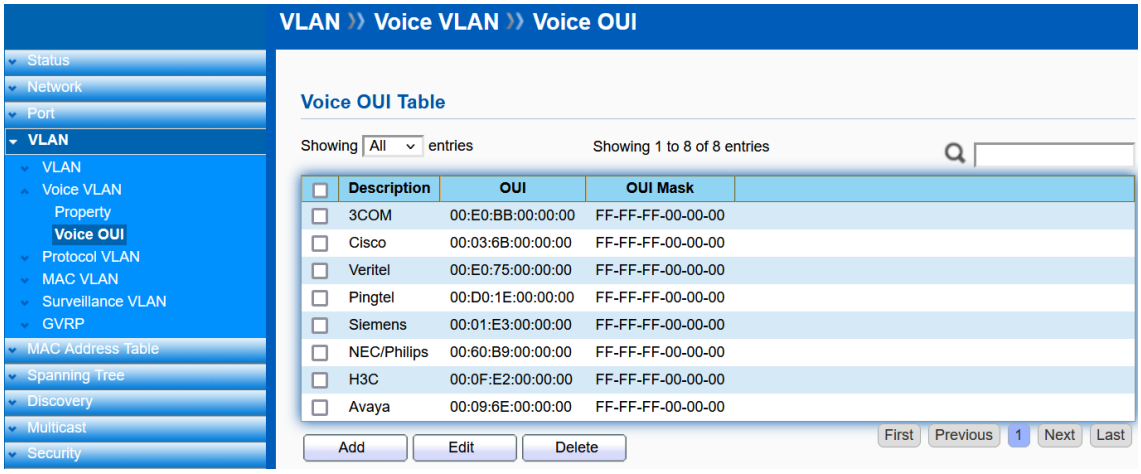


Field	Description
Port	Display selected port to be edited.
State	Set checkbox to enable/disable voice VLAN function of interface.
Mode	Select port voice VLAN mode. **Auto**: Voice VLAN auto detect packets that match OUI table and add received port into voice VLAN ID tagged member. **Manual**: User need add interface to VLAN ID tagged member manually.
QoS Policy	Select port QoS Policy mode **Voice Packet**: QoS attributes are applied to packets with OUIs in the source MAC address. **All**: QoS attributes are applied to packets that are classified to the Voice VLAN.

6.2.2 Voice OUI

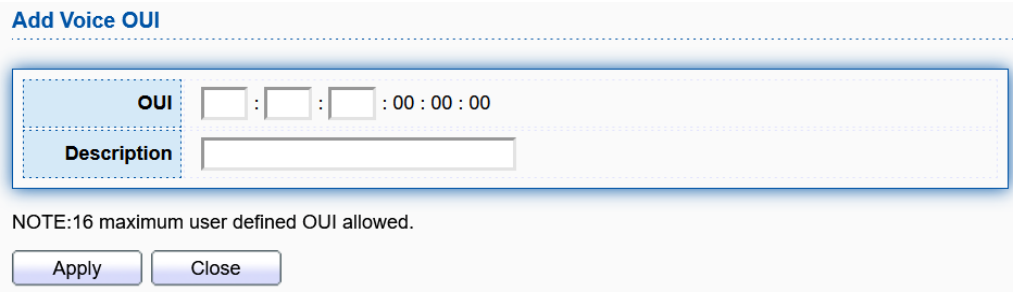
Click **VLAN** > **Voice VLAN** > **Voice OUI**

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



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

Click “**Add**” or “**Edit**” buttons to add or edit Voice OUI.



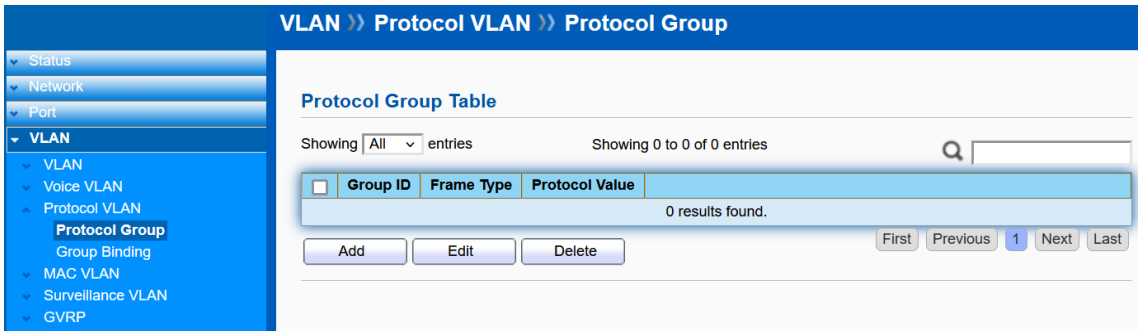
Field	Description
OUI	Input OUI MAC address. Can't be edited in edit dialog.
Description	Input description of the specified MAC address to the voice VLAN OUI table.

6.3 Protocol VLAN

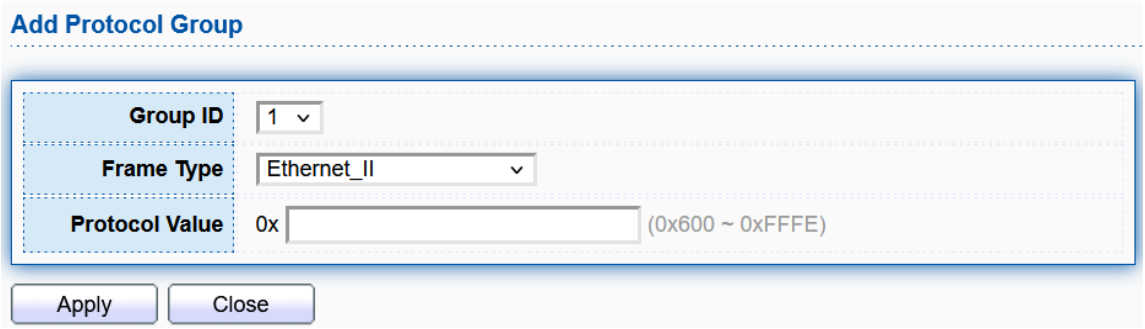
6.3.1 Protocol Group

Click **VLAN** > **Protocol VLAN** > **Protocol Group**

This page allows you to add new protocols to Group ID (unique for each Group) mapping entries as well as allow you to see and delete already mapped entries for the selected stack switch unit.



Click "**Add**" or "**Edit**" button to add or edit Protocol VLAN Group.

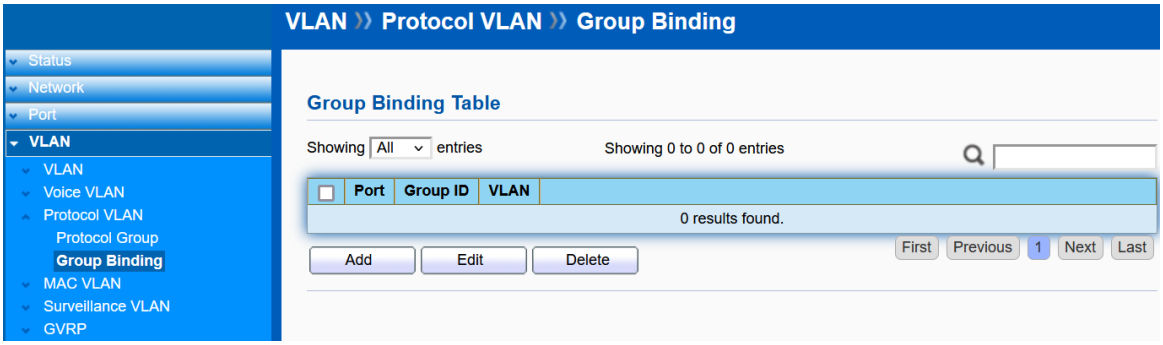


Field	Description
Group ID	Select Group ID 1 to 8.
Frame Type	Select Frame Type. The options are "**Ethernet_II**", "**IEEE802.3_LL_Other**" and "**RFC_1042**".
Protocol Value	Set Protocol Value. The range is 0x600 to 0xFFFE.

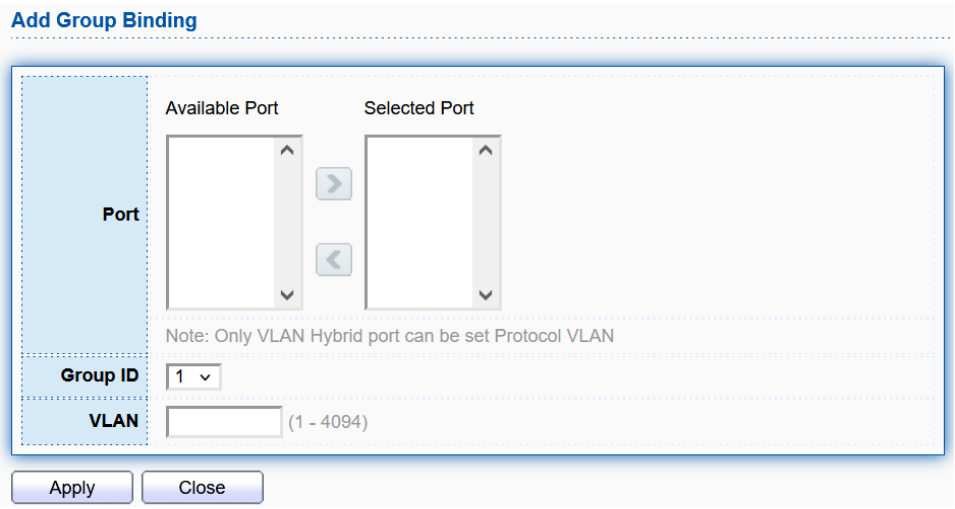
6.3.2 Group Binding

Click **VLAN** > **Protocol VLAN** > **Group Binding**

This page allows you to map an already configured Group ID to a VLAN for the selected port.



Click “**Add**” or “**Edit**” button to add or edit Group Binding.



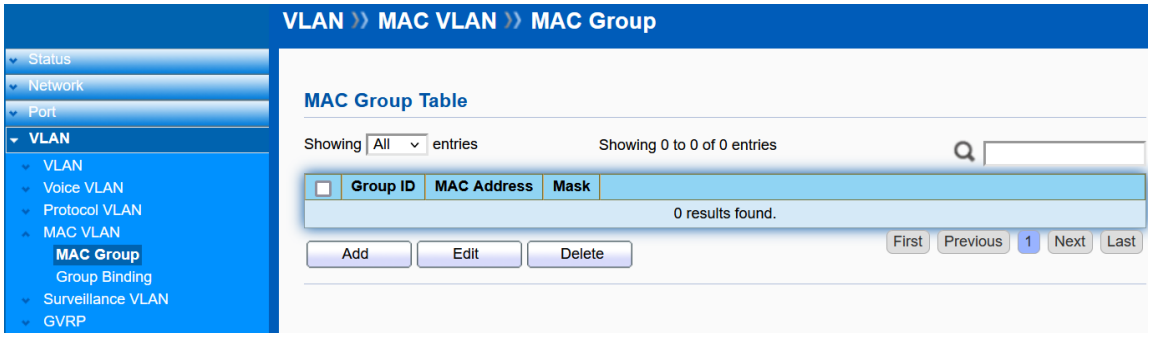
Field	Description
Port	Select the port(s) to set Protocol VLAN.
Group ID	Select the Group ID.
VLAN	Indicates the VLAN ID.

6.4 MAC VLAN

6.4.1 MAC Group

Click **VLAN** > **MAC VLAN** > **MAC Group**

The MAC-based VLAN entries can be configured here. This page allows for adding and deleting MAC-based VLAN entries.



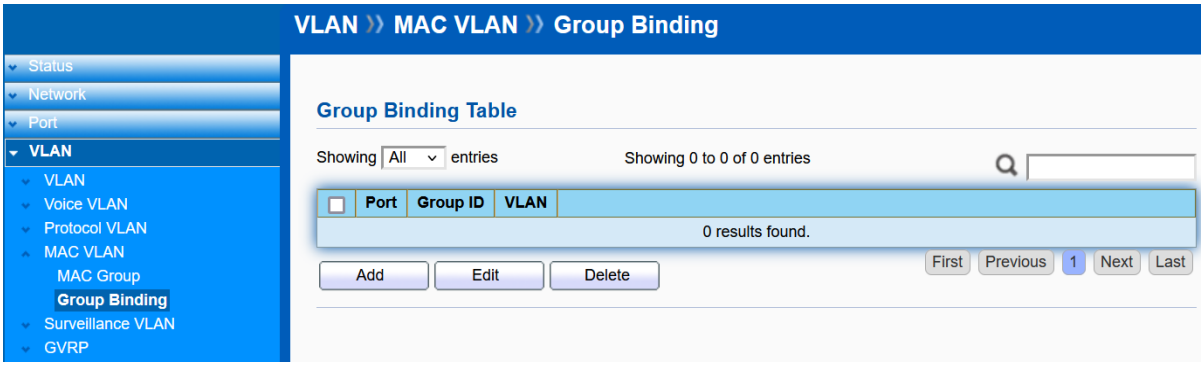
Click “**Add**” or “**Edit**” button to add or edit MAC VLAN.

Field	Description
Group ID	Indicates the Group ID.
MAC Address	Indicates the MAC address.
Mask	Indicates the mask.

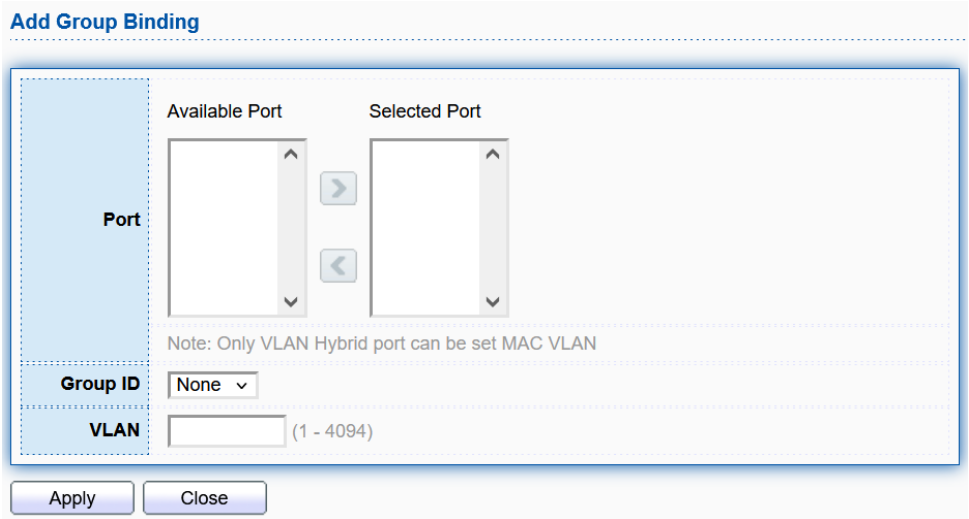
6.4.2 Group Binding

Click **VLAN** > **MAC VLAN** > **Group Binding**

This page allows for assigning the MAC Group to different ports.



Click "**Add**" or "**Edit**" button to add or edit Group Binding.



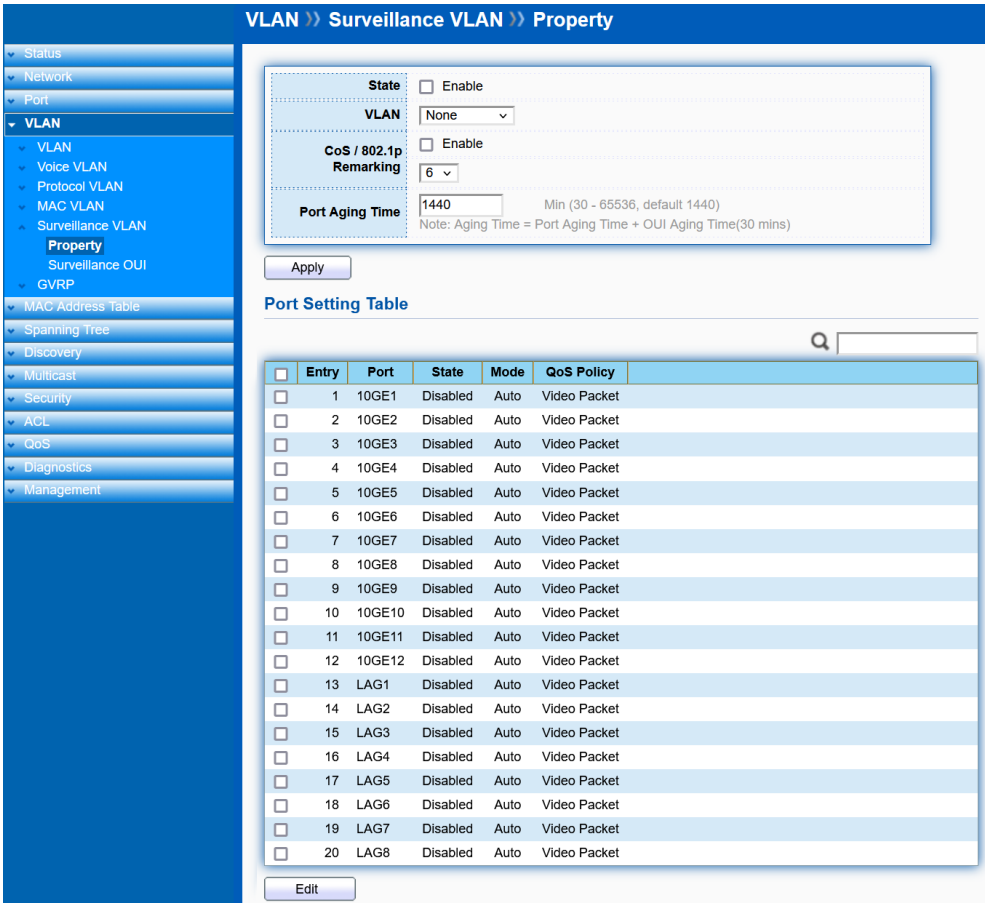
Field	Description
Port	Select the port(s) to set MAC VLAN.
Group ID	Select the Group ID.
VLAN	Indicates the VLAN ID.

6.5 Surveillance VLAN

6.5.1 Property

Click **VLAN** > **Surveillance VLAN** > **Property**

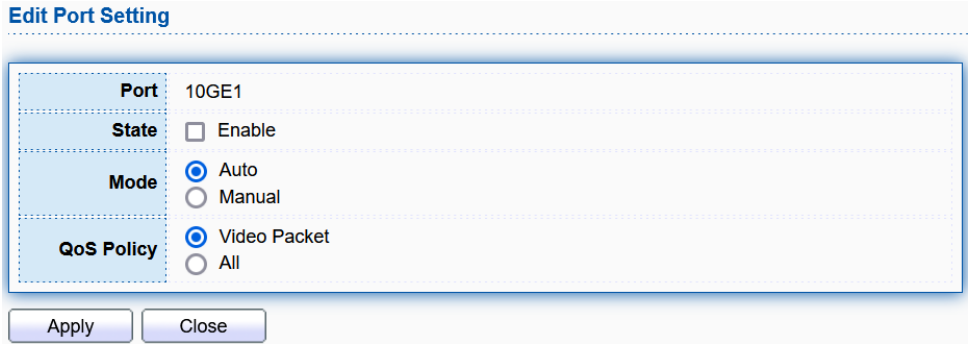
This page allows user to configure global and per interface setting of surveillance VLAN.



Field	Description
State	Set checkbox to enable or disable voice VLAN function.
VLAN	Select Video VLAN ID. Video VLAN ID cannot be default VLAN.
Cos/802.1p Remarking	Set checkbox to enable or disable 1p remarking. If enabled, qualified packets will be remark by this value. Select a value of VPT. Qualified packets will use this VPT value as inner priority. (Range: 0-7; Default: 6)
Aging Time	Input value of aging time. Default is 1440 minutes. A voice VLAN entry will be age out after this time if without any packet pass through.

Field	Description
Port	Display port entry
State	Display enable/disable status of interface.
Mode	Display video VLAN mode.
QoS Policy	Display video VLAN remark will effect which kind of packet

Click “**Edit**” buttons to edit the Surveillance VLAN.

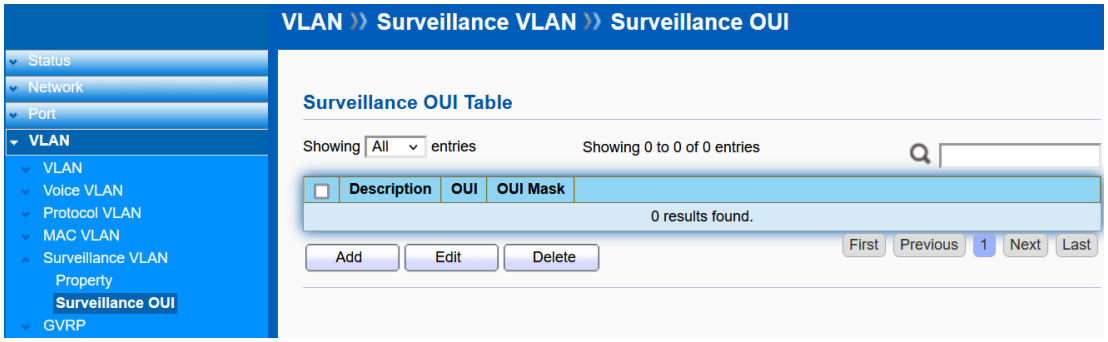


Field	Description
Port	Display selected port to be edited.
State	Set checkbox to enable/disable video VLAN function of interface.
Mode	Select port video VLAN mode. **Auto**: Video VLAN auto detect packets that match OUI table and add received port into voice VLAN ID tagged member. **Manual**: User need add interface to VLAN ID tagged member manually.
QoS Policy	Select port QoS Policy mode **Video Packet**: QoS attributes are applied to packets with OUIs in the source MAC address. **All**: QoS attributes are applied to packets that are classified to the Video VLAN.

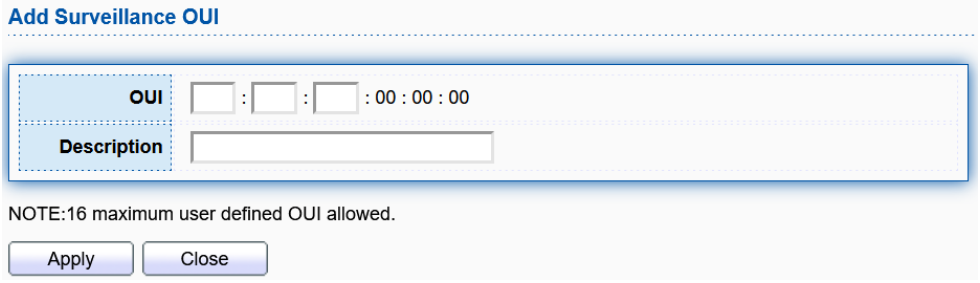
6.5.2 Surveillance OUI

Click **VLAN** > **Surveillance VLAN** > **Surveillance OUI**

This page allow user to add, edit or delete OUI MAC addresses.



Click “**Add**” or “**Edit**” buttons to add or edit Surveillance OUI.



Field	Description
OUI	Input OUI MAC address.
Description	Input description of the specified MAC address to the video VLAN OUI table.

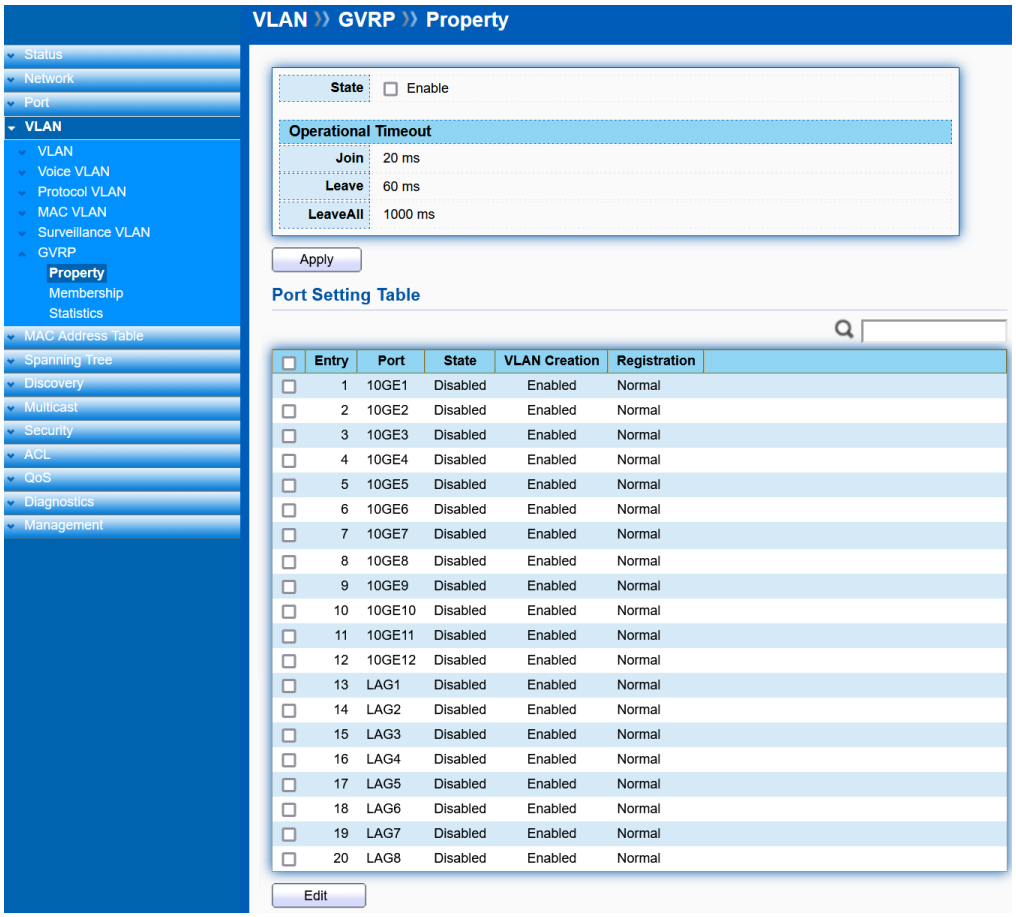
6.6 GVRP

6.6.1 Property

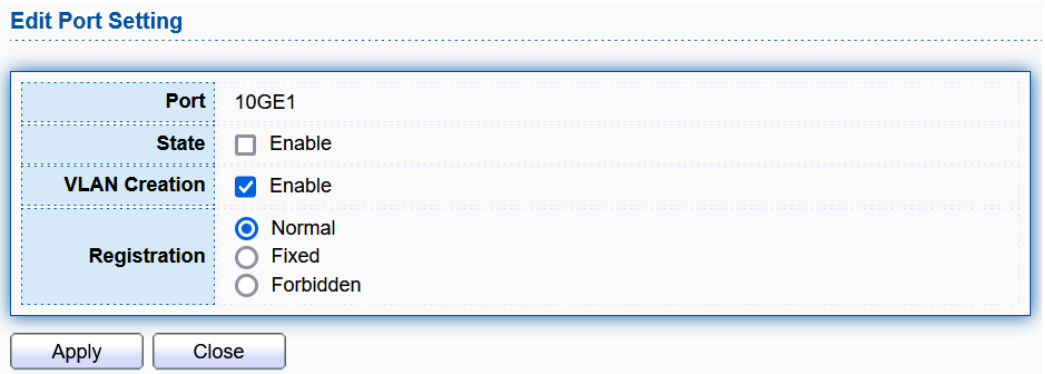
Click **VLAN** > **GVRP** > **Property**

GVRP (GARP VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices.

GVRP provides dynamic registration of VLAN membership; therefore, members can be added or removed from a VLAN at any time, saving the overhead of maintaining static VLAN configuration on switch ports. Additionally, VLAN membership information stays current, limiting the broadcast domain of a VLAN only to the active members of that VLAN.



Click “**Edit**” buttons to edit GVRP.

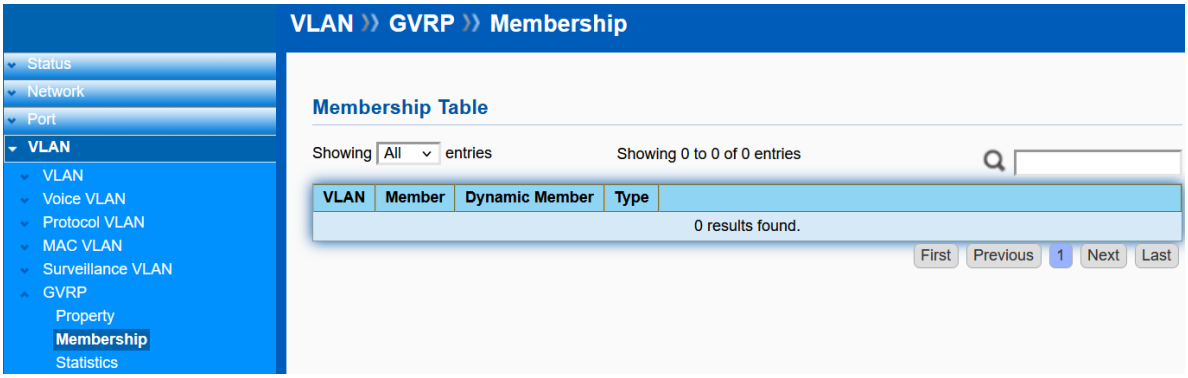


Field	Description
State	Check to enable GVRP.
VLAN Creation	Check to enable dynamic VLAN Creation.
Registration	Select Registration mode. By default GVRP ports are in **Normal** registration mode. These ports use GVRP join messages from neighboring switches to prune the VLANs running across the 802.1Q trunk link. If the device on the other side is not capable of sending GVRP messages, or if you do not want to allow the switch to prune any of the VLANs, use the **Fixed** mode. Fixed mode ports will forward for all VLANs that exist in the switch database. Ports in **Forbidden** mode forward only for VLAN 1.

6.6.2 Membership

Click **VLAN** > **GVRP** > **Membership**

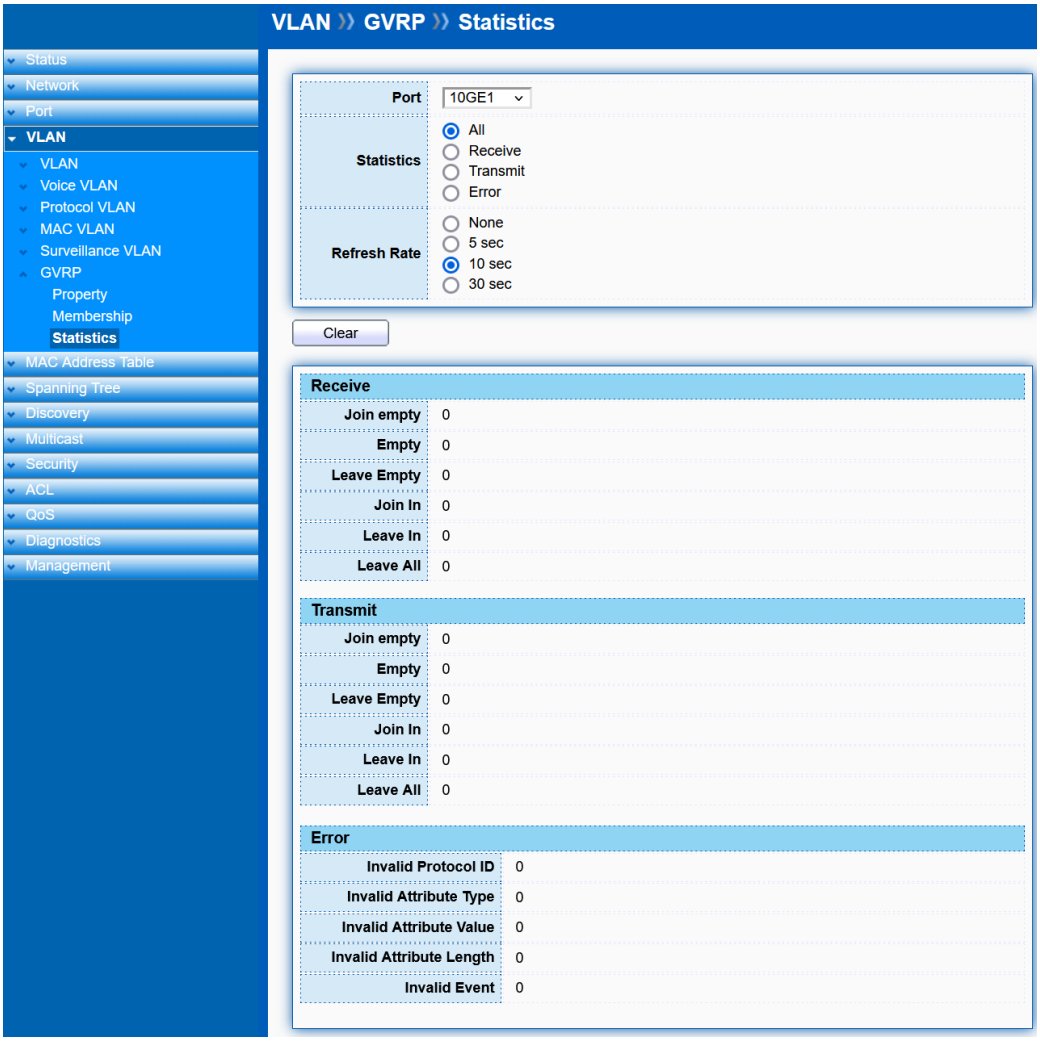
This page allow user to view GVRP membership information.



6.6.3 Statistics

Click **VLAN** > **GVRP** > **Statistics**

This page allow user to view GVRP statistics in each port.


VLAN » GVRP » Statistics
Status
Network
Port
VLAN
VLAN
Voice VLAN
Protocol VLAN
MAC VLAN
Surveillance VLAN
GVRP
Property
Membership
Statistics
MAC Address Table
Spanning Tree
Discovery
Multicast
Security
ACL
QoS
Diagnostics
Management
Port
10GE1
Statistics
All
Receive
Transmit
Error
Refresh Rate
None
5 sec
10 sec
30 sec
Clear
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

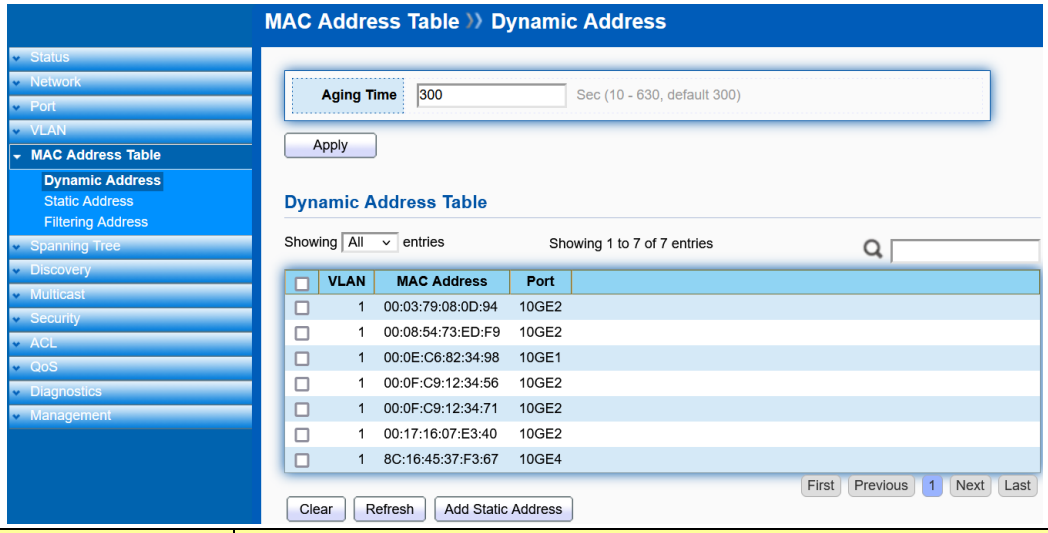
Chapter 7 MAC Address Table

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

7.1 Dynamic Address

Click **MAC Address Table** > **Dynamic Address**

Configure the aging time of the dynamic address. Click **Add Static Address** to add a MAC address to a static MAC address.

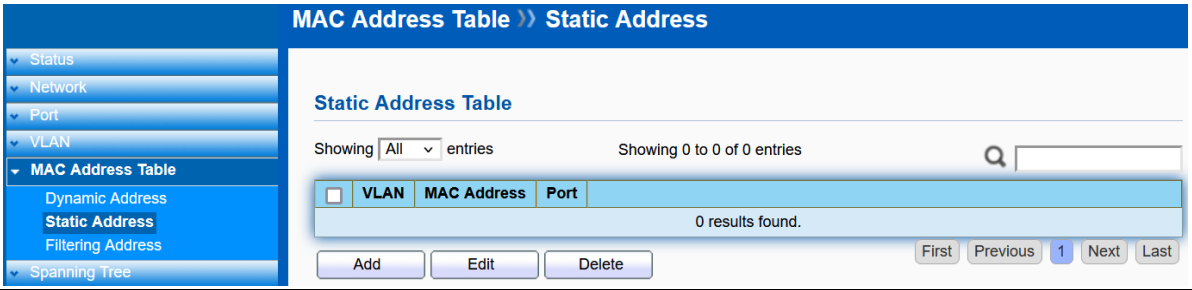


Field	Description
Aging Time	The time in seconds that an entry remains in the MAC address table. Its valid range is from 10 to 630 seconds, and the default value is 300 seconds

7.2 Static Address

Click **MAC Address Table** > **Static Address**

To display the static MAC address. Click **Add**, **Edit** or **Delete** to add, edit or delete a static MAC address.

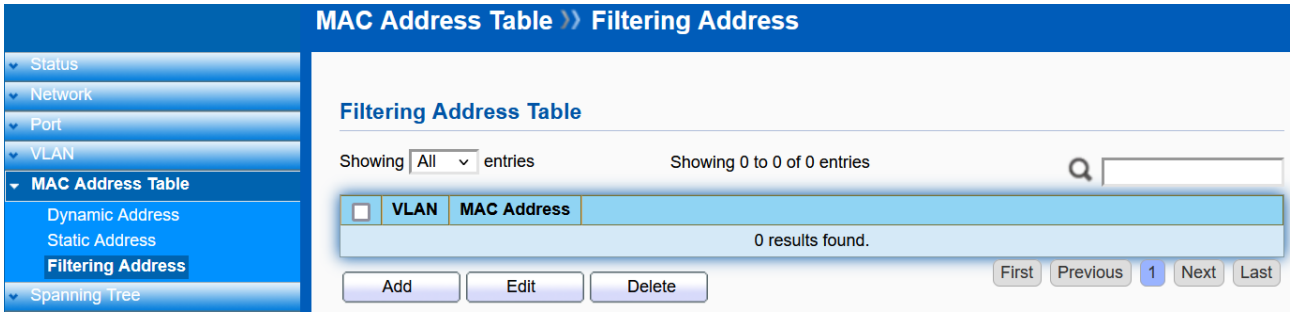


Field	Description
MAC Address	The MAC address to which packets will be statically fowarded.
VLAN	The VLAN ID that MAC address used.
Port	Interface or port number.

7.3 Filtering Address

Click **MAC Address Table** > **Filtering Address**

To display the filtering MAC address. Click **Add**, **Edit** or **Delete** to add, edit or delete a filtering MAC address.



Field	Description
VLAN	The VLAN ID that MAC address used.
MAC Address	The MAC address to which packets will be filtered.

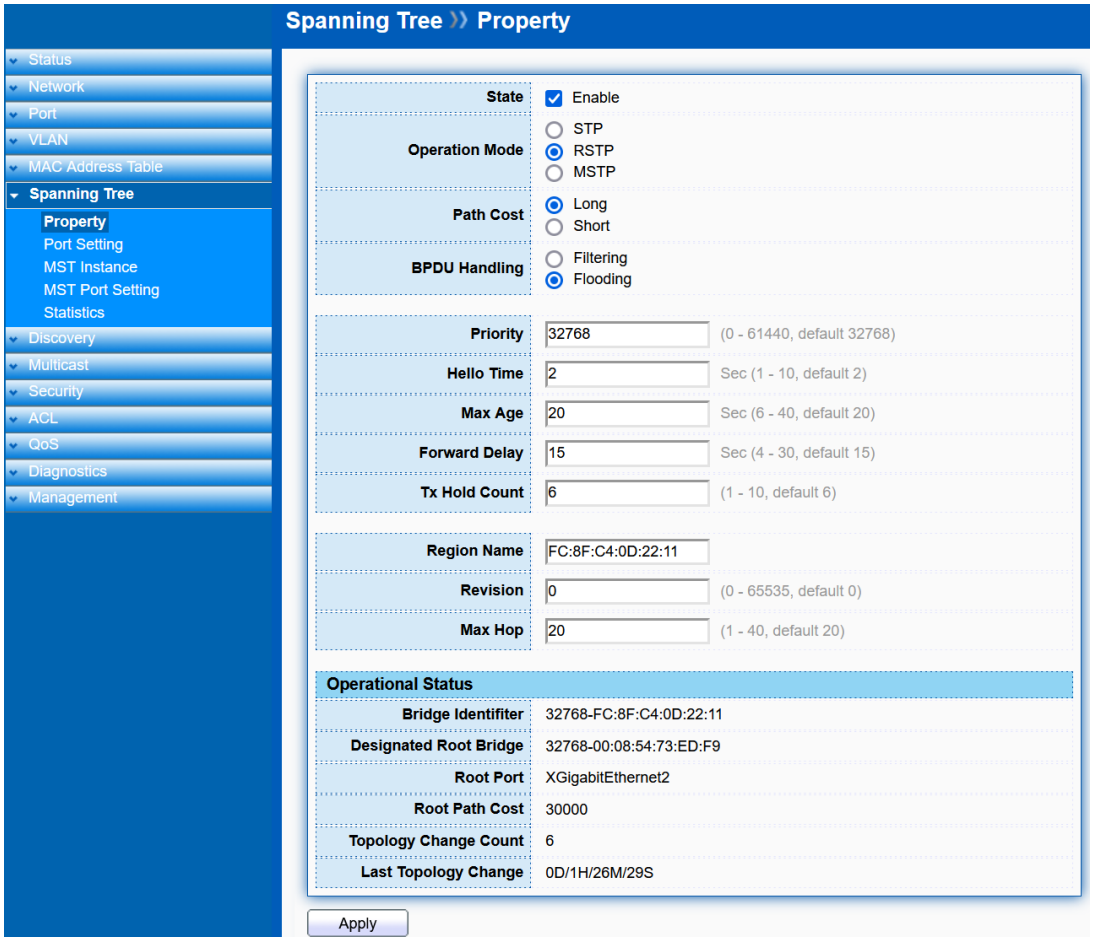
Chapter 8 Spanning Tree

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

Click **Spanning Tree** > **Property**

Configure and display STP property configuration.



Field	Description
State	Enable/Disable the STP on the switch.
Operation Mode	Specify the STP operation mode. **STP**: Enable the Spanning Tree (STP) operation. **RSTP**: Enable the Rapid Spanning Tree (RSTP) operation. **MSTP**: Enable the Multiple Spanning Tree (MSTP) operation.
Path Cost	Specify the path cost method. **Long**: Specifies that the default port path costs are within the range: 1~200,000,000. **Short**: Specifies that the default port path costs are within the range: 1~65,535.
BPDU Handling	Specify the BPDU forward method when the STP is disabled. **Filtering**: Filter the BPDU when STP is disabled. **Flooding**: Flood the BPDU when STP is disabled.
Priority	Specify the bridge priority. The valid range is from 0 to 61440, and the value should be the multiple of 4096. It ensures the probability that the

	switch is selected as the root bridge, and the lower value has the higher priority for the switch to be selected as the root bridge of the topology.
Hello Time	Specify the STP hello time in second to broadcast its hello message to other 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 10 seconds.
TX Hold Count	Specify the tx-hold-count used to limit the maximum numbers of packets transmission per second. The valid range is from 1 to 10.
Region Name	This name uniquely identifies the MSTI (Multiple Spanning Tree Instance). Enter a descriptive name (up to 32 characters) for an MST region. The default is the MAC address name of the device running MSTP.
Revision	This value, along with the Region Name, identifies the MSTP region configured on the Switch. Devices must have the same revision number to belong to the same region
Max Hop	Used to set the number of hops between devices in a spanning tree region before the BPDU packet sent by the Switch is discarded. Each Switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BDPU packet and the information held for the port will age out. The user may set a hop count from 1 to 40. The default value is: 20.

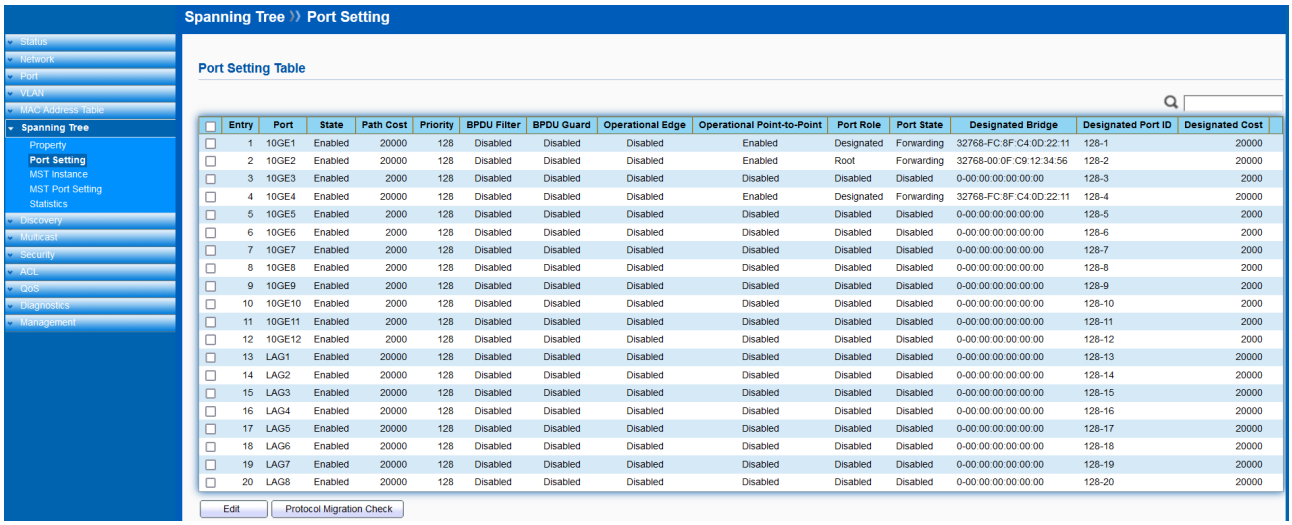
STP operational status

Field	Description
Bridge Identifier	Bridge identifier of the switch.
Designated Root Identifier	Bridge identifier of the designated root bridge.
Root Port	Operational root port of the switch.
Root Path Cost	Operational root path cost.
Topology Change Count	Numbers of the topology changes.
Last Topology Change	The last time for the topology change.

8.2 Port Setting

Click **Spanning Tree** > **Port Setting**

Configure and display STP port settings.

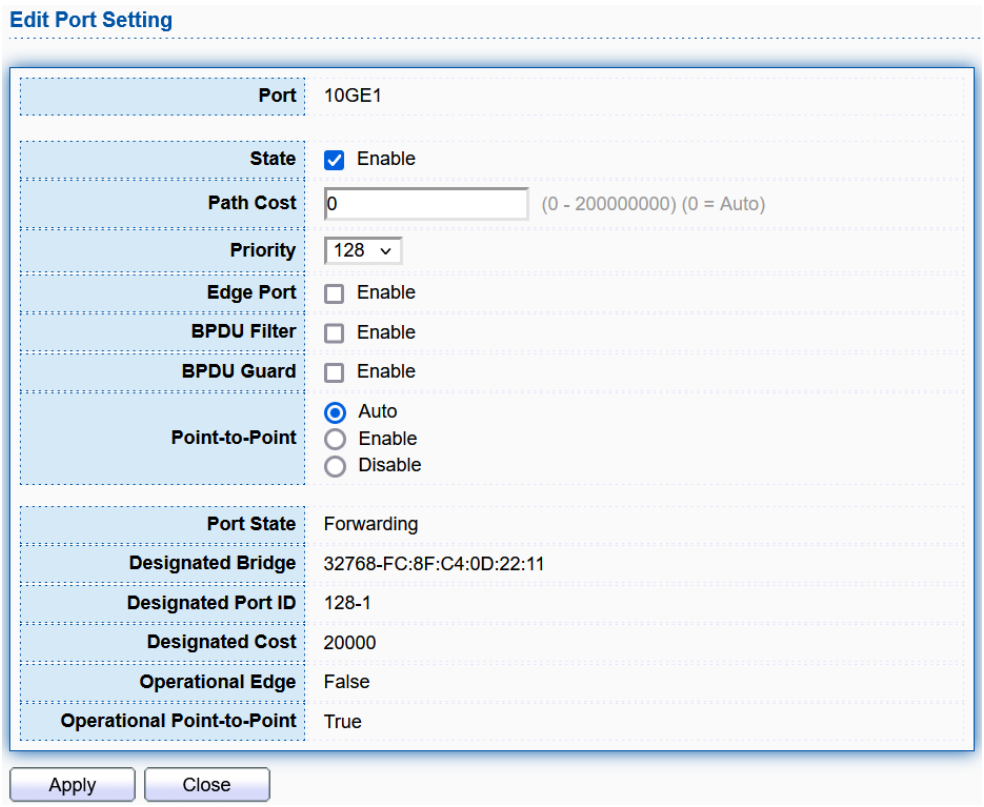


Field	Description
Port	Specify the interface ID or the list of interface IDs.
State	The operational state on the specified port.
Path Cost	STP path cost on the specified port.
Priority	STP priority on the specified port.
BPDU Filter	Control whether a port will transmit and receive BPDUs.
BPDU Guard	Control whether a port will disable itself upon reception of a BPDU. The port will enter the Error Disabled state, and will be removed from the active topology
Operational Edge	The operational edge port on the specified port.
Operational Point-to-Point	The operational edge point-to-point status on the specified port.
Port Role	The current port role on the specified port. The possible values are: “Disabled”, “Master”, “Root”, “Designated”, “Alternative”, and “Backup”
Port State	The current port state on the specified port. The possible values are: “Disabled”, “Discarding”, “Learning”, and “Forwarding”.
Designated Bridge	The bridge ID of the designated bridge.
Designated Port ID	The designated port ID on the switch.
Designated Cost	The path cost of the designated port on the switch.

STP port setting buttons

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

Edit STP port setting



Field	Description
State	Enable/Disable the STP on the specified port
Path Cost	Specify the STP path cost on the specified port.
Priority	Specify the STP priority on the specified port.
Edge Port	Specify the edge mode. **Enable**: Force to true state (as link to a host) **Disable**: Force to false state (as link to a bridge) In the edge mode, the interface would be put into the Forwarding state immediately upon link up. If the edge mode is enabled for the interface and there are BPDUs received on the interface, the loop might be occurred in the short time before the STP state change.
BPDU Filter	Control whether a port will transmit and receive BPDUs.
BPDU Guard	Control whether a port will disable itself upon reception of a BPDU. The port will enter the Error Disabled state, and will be removed from the active topology
Point-to-Point	Specify the Point-to-Point port configuration: **Auto**: The state is depended on the duplex setting of the port. **Enable**: Force to true state. **Disable**: Force to false state.

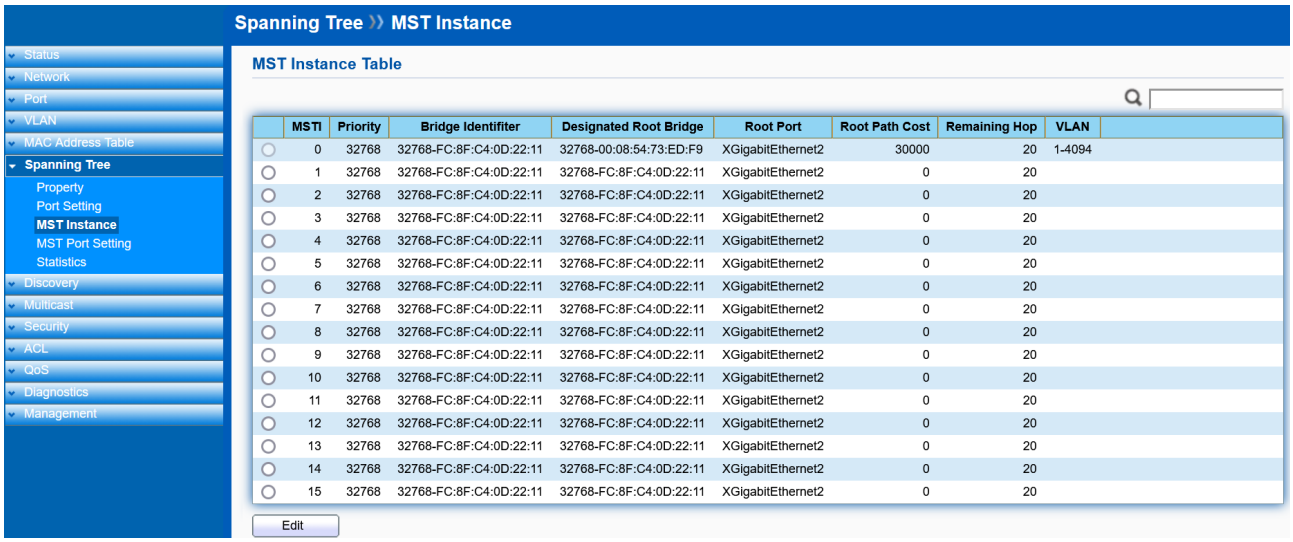
8.3 MST Instance

Click **Spanning Tree** > **MST Instance**

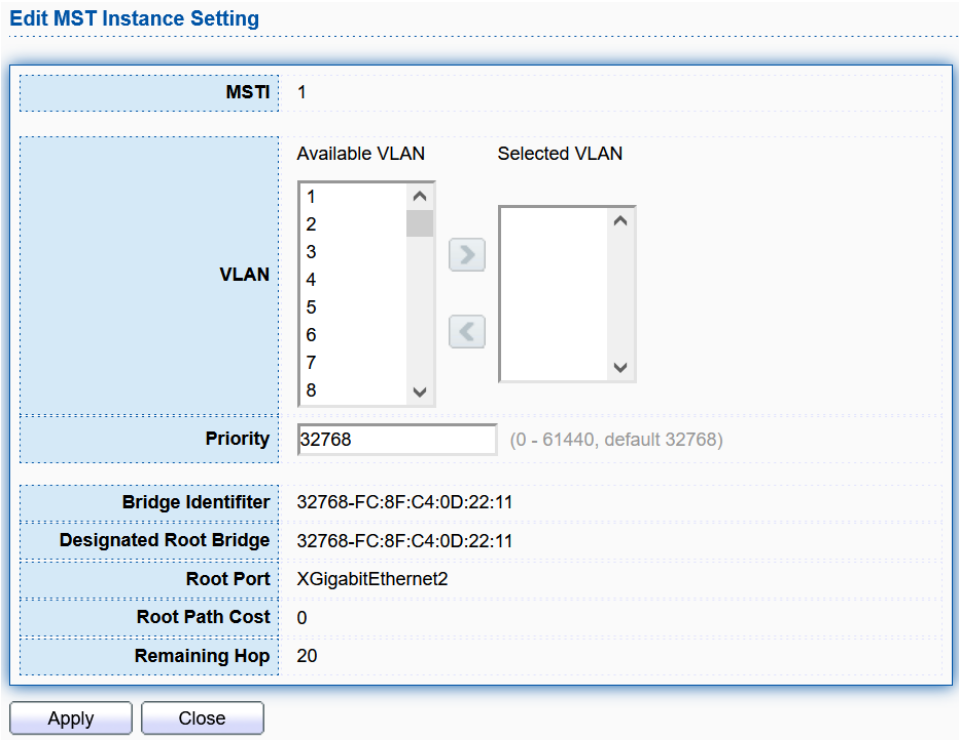
Configure and display MST Instance.

Multiple Spanning Tree Protocol or MSTP enables the grouping of multiple VLANs with the same topology requirements into one Multiple Spanning Tree Instance (MSTI). MSTP then builds an Internal Spanning Tree (IST) for the region containing commonly configured MSTP bridges. Instances are not supported in STP or RSTP. Instead, they have the same spanning tree in common

within the VLAN. MSTP provides the capability to logically divide a Layer 2 network into regions. Every region can contain multiple instances of spanning trees. In MSTP, all of the interconnected bridges that have the same MSTP configuration comprise an MST region.



Edit MST Instance

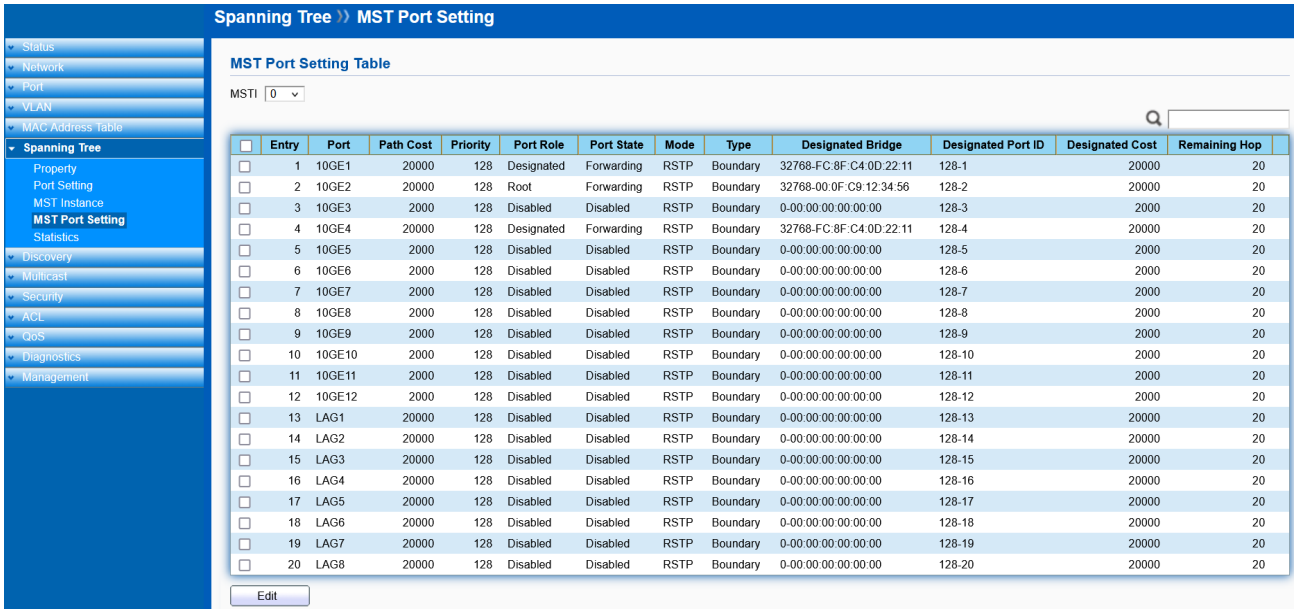


Field	Description
Available VLAN / Selected VLAN	The list of VLANs mapped to the MSTI. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty.
Priority	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.

8.4 MST Port Setting

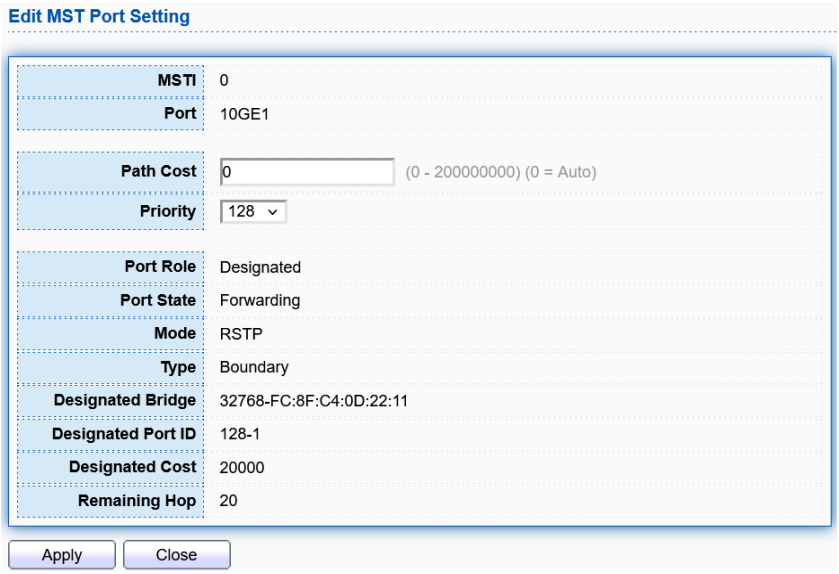
Click **Spanning Tree** > **MST Port Setting**

This page displays the current MSTI configuration information for the Switch. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for ports you wish to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest MAC address into the forwarding state and other interfaces will be blocked. Note that a lower priority values mean higher priorities for forwarding packets.



Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Type	Designated Bridge	Designated Port ID	Designated Cost	Remaining Hop
1	10GE1	20000	128	Designated	Forwarding	RSTP	Boundary	32768-FC:8F:C4:0D:22:11	128-1	20000	20
2	10GE2	20000	128	Root	Forwarding	RSTP	Boundary	32768-00:0F:C9:12:34:56	128-2	20000	20
3	10GE3	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-3	2000	20
4	10GE4	20000	128	Designated	Forwarding	RSTP	Boundary	32768-FC:8F:C4:0D:22:11	128-4	20000	20
5	10GE5	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-5	2000	20
6	10GE6	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-6	2000	20
7	10GE7	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-7	2000	20
8	10GE8	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-8	2000	20
9	10GE9	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-9	2000	20
10	10GE10	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-10	2000	20
11	10GE11	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-11	2000	20
12	10GE12	2000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-12	2000	20
13	LAG1	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-13	20000	20
14	LAG2	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-14	20000	20
15	LAG3	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-15	20000	20
16	LAG4	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-16	20000	20
17	LAG5	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-17	20000	20
18	LAG6	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-18	20000	20
19	LAG7	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-19	20000	20
20	LAG8	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-20	20000	20

Edit MST Port Setting



Field	Description
Path Cost	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the specific setting, a user-defined value can be entered. The path cost is used when establishing

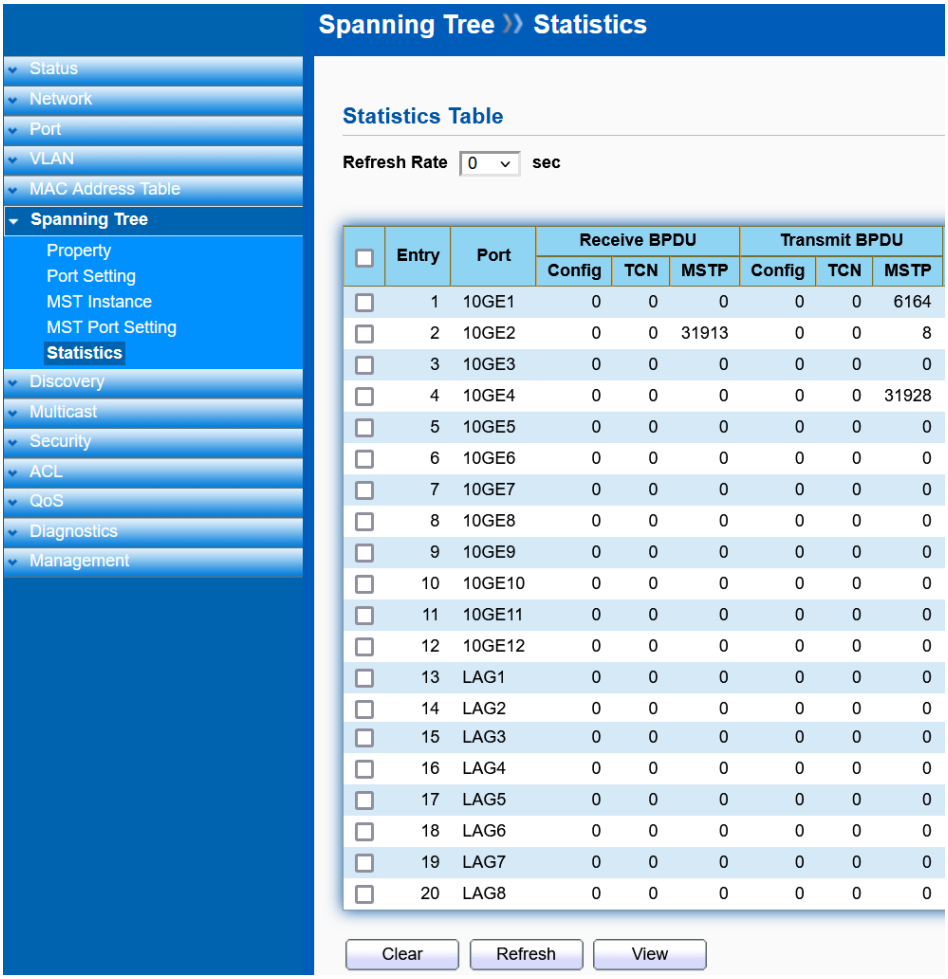
	the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost.
Port Role	Each MST bridge port that is enabled is assigned a Port Role for each spanning tree. The Port Role is one of the following values: Root, Designated, Alternate, Backup, Master, or Disabled.
Port Status	Indicates the current STP state of a port. If enabled, the Port State determines what forwarding action is taken regarding traffic. The possible port states are: •**Disabled**: STP is disabled on the port. The port forwards traffic while learning MAC addresses. •**Blocking**: The port is blocked and cannot be used to forward traffic or learn MAC addresses. •**Listening**: The port is in listening mode. The port cannot forward traffic or learn MAC addresses in this state. •**Learning**: The port is in learning mode. The port cannot forward traffic. However, it can learn new MAC addresses. •**Forwarding**: The port is in forwarding mode. The port can forward traffic and learn new MAC addresses in this state
Mode	The STP mode: Disabled, STP, RSTP or MSTP.
Type	The current type of the port.
Designated Bridge	Displays the Bridge Identifier of the bridge for the Designated Port. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Port ID	Display the Port ID. It is made up using the priority and the port number.
Designated Cost	Displays the operation cost of the path from this bridge to the Root Bridge.
Remaining Hop	The remaining hop number.

8.5 Statistics

Click **Spanning Tree** > **Statistics**

To display STP statistics

Bridge Protocol Data Units (BPDUs) are frames that contain information about the **Spanning tree protocol (STP)**. Switches send BPDUs using a unique MAC address from its origin port and a multicast address as destination MAC (01:80:C2:00:00:00, or 01:00:0C:CC:CC:CD for Per VLAN Spanning Tree). For STP algorithms to function, the switches need to share information about themselves and their connections. What they share are bridge protocol data units (BPDUs). BPDUs are sent out as multicast frames to which only other layer 2 switches or bridges are listening. If any loops (multiple possible paths between switches) are found in the network topology, the switches will co-operate to disable a port or ports to ensure that there are no loops; that is, from one device to any other device in the layer 2 network, only one path can be taken.



Field	Description
Refresh Rate	The option to refresh the statistics automatically.
Receive BPDU (Config)	The counts of the received CONFIG BPDU.
Receive BPDU (TCN)	The counts of the received TCN BPDU.
Receive BPDU (MSTP)	The counts of the received MSTP BPDU.
Transmit BPDU (Config)	The counts of the transmitted CONFIG BPDU.
Transmit BPDU (TCN)	The counts of the transmitted TCN BPDU.
Transmit BPDU (MSTP)	The counts of the transmitted MSTP BPDU.

Field	Description
Clear	Clear the statistics for the selected interfaces.
View	View the statistics for the interface.

Chapter 9 Discovery

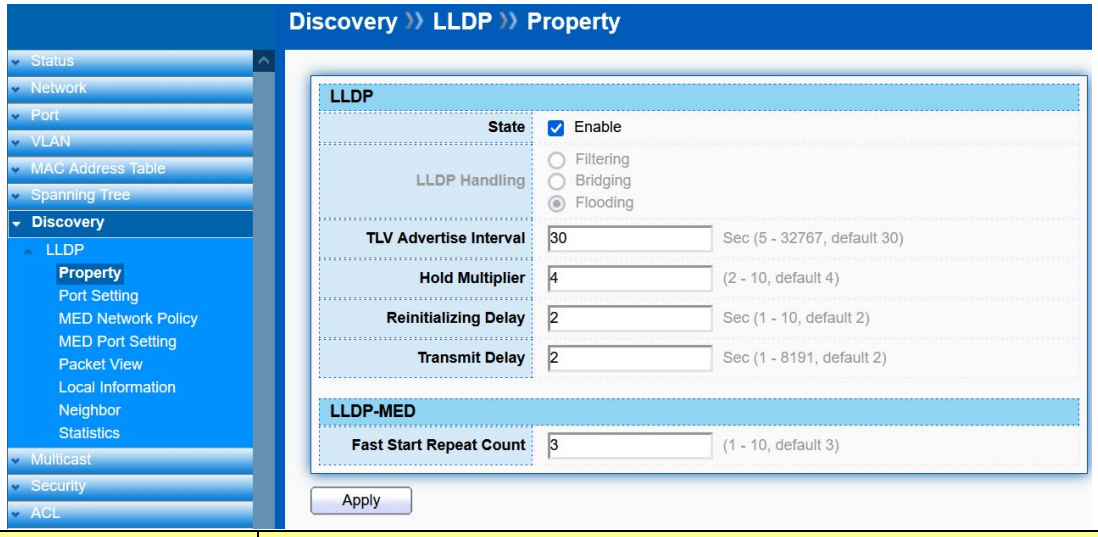
9.1 LLDP

The **Link Layer Discovery Protocol (LLDP)** is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet. The 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

Click **Discovery** > **LLDP** > **Property**

To display LLDP Property Setting web page.

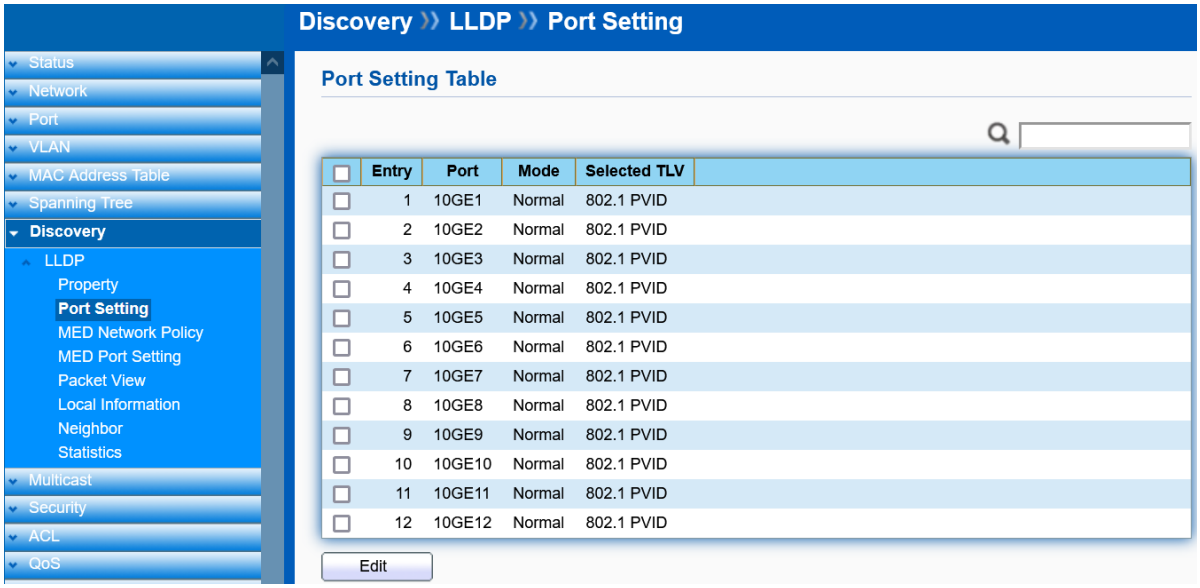


Field	Description
State	Enable/Disable LLDP protocol on this switch
LLDP Handling	Select LLDP PDU handling action to be filtered, bridging or flooded when LLDP is globally disabled. **Filtering**: Deletes the packet. **Bridging**: (VLAN-aware flooding) Forwards the packet to all VLAN members. **Flooding**: Forwards the packet to all ports.
TLV Advertise Interval	Select the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 5~32767 seconds.
Holdtime Multiplier	Select the multiplier on the transmit interval to assign to TTL (range 2~10, default=4).
Reinitialization Delay	Select the delay before a re-initialization (range 1~10 seconds, default=2).
Transmit Delay	Select the delay after an LLDP frame is sent (range 1~8191 seconds, default=3).
Fast Start Repeat Count	Specifies the repeat count value (range 1~10, default=3).

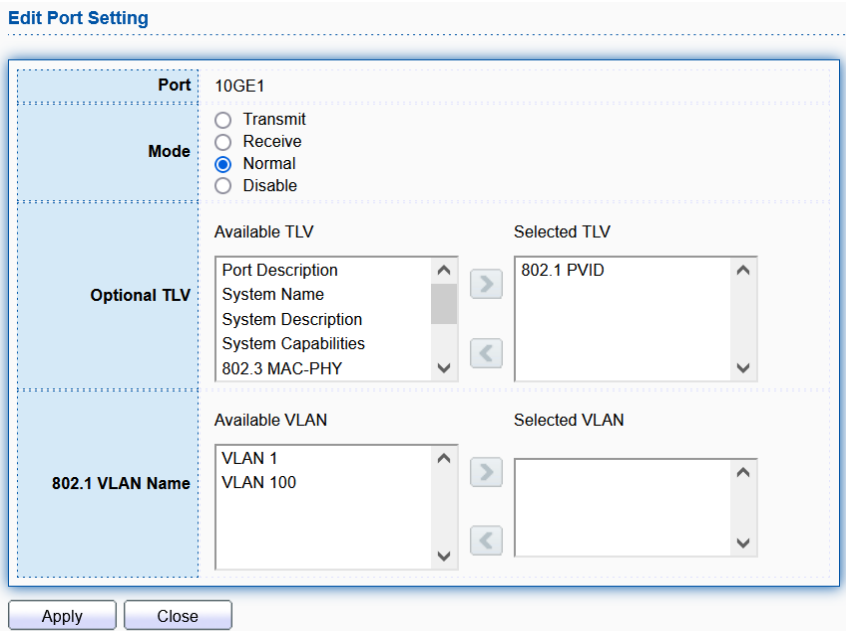
9.1.2 Port Setting

Click **Discovery** > **LLDP** > **Port Setting**

To display LLDP Port Setting.



To Edit LLDP port setting web page, select the port which to set, click button **Edit**.



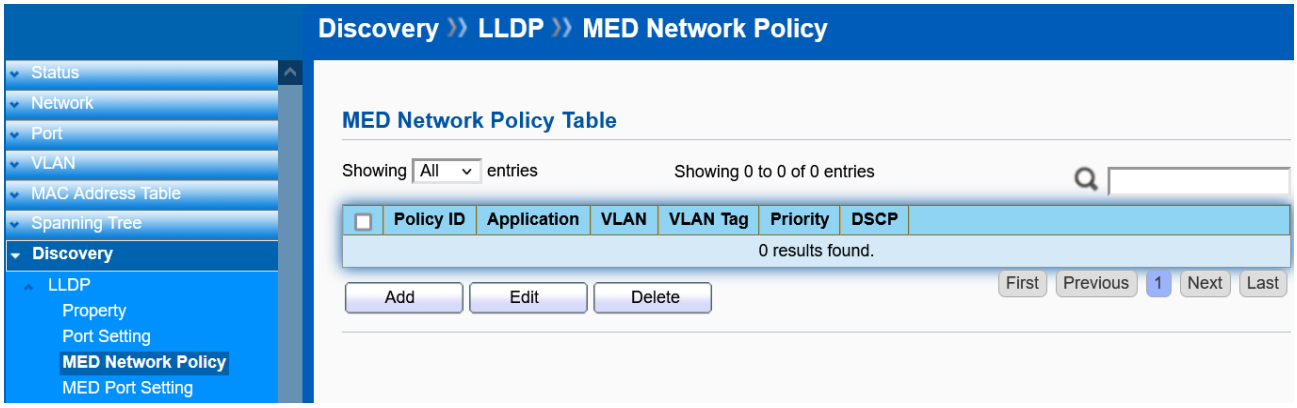
Field	Description
Port	Select specified port or all ports to configure LLDP state.
Mode	Select the transmission state of LLDP port interface. **Transmit**: Transmit LLDP PDUs only. **Receive**: Receive LLDP PDUs only. **Normal**: Transmit and receive LLDP PDUs both. **Disable**: Disable the transmission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

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

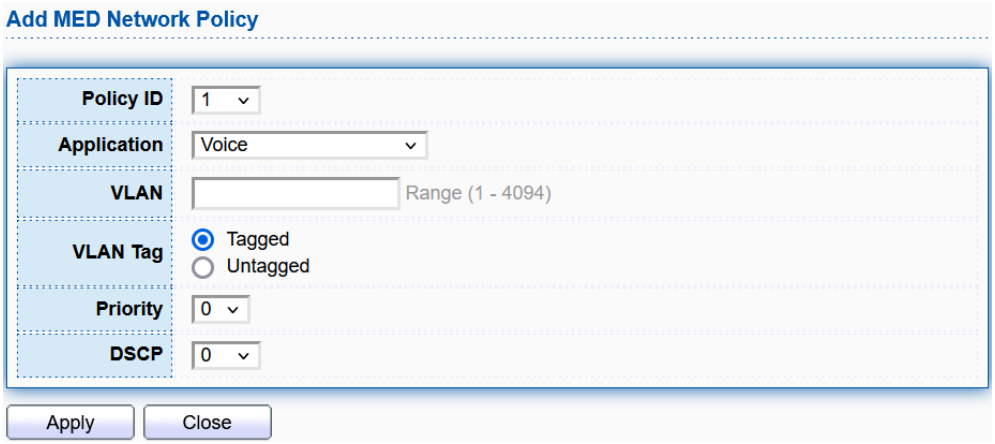
9.1.3 MED Network Policy

Click **Discovery** > **LLDP** > **MED Network Policy**

LLDP Media Endpoint Discovery (LLDP MED) is an extension to LLDP. This protocol enables advanced LLDP features in a Voice over IP (VoIP) network. Whereas LLDP enables network discovery between Network Connectivity devices, LLDP-MED enables network discovery between Network Connectivity devices and media Endpoints such as, IP telephones, softphones, VoIP gateways and conference bridges.



Check "**Enable**" and press "**Apply**" to use "MED Network Policy Voice Auto Mode".
Click "**Add**" or "**Edit**" button to add or edit a policy.



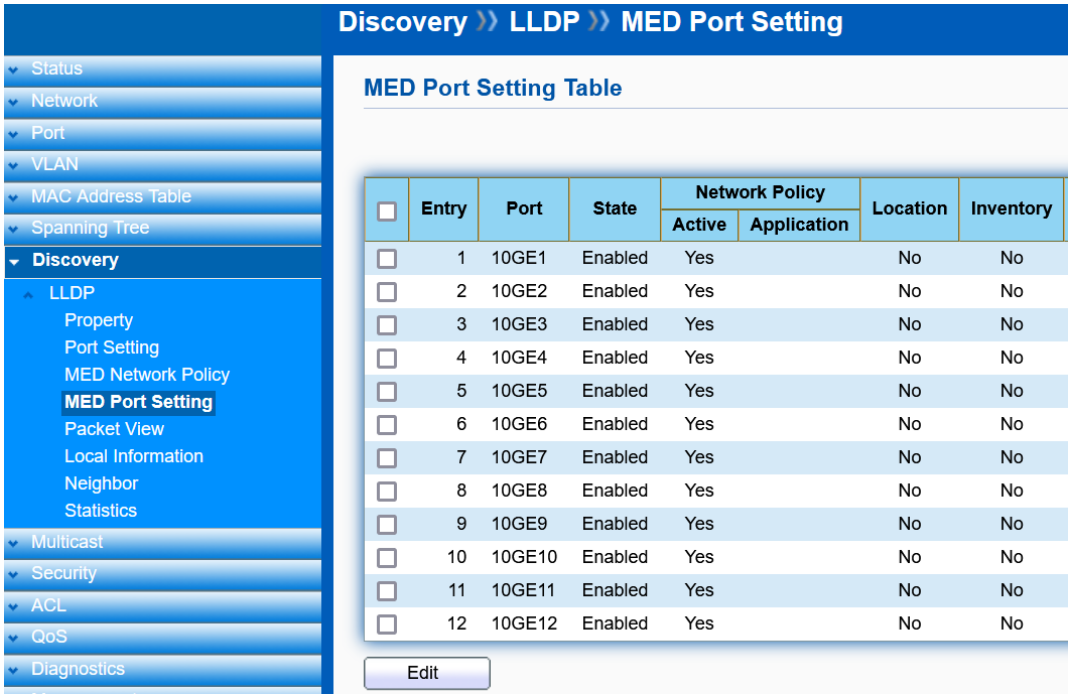
Field	Description
Policy ID	Select the number of the policy to be created.
Application	Select the type of application (type of traffic) from the list for which the network policy is being defined: **Voice**

	Voice Signaling **Guest Voice** **Guest Voice Signaling** **Softphone Voice** **Video Conferencing** **Streaming Video** **Video Signaling**
VLAN	Enter the VLAN ID to which the traffic should be sent.
VLAN Tag	Select whether the traffic is Tagged or Untagged.
Priority	Select the traffic priority applied to traffic defined by this network policy.
DSCP	Select the DSCP value to associate with application data sent by neighbors. This informs them how they should mark the application traffic that they send to the switch.

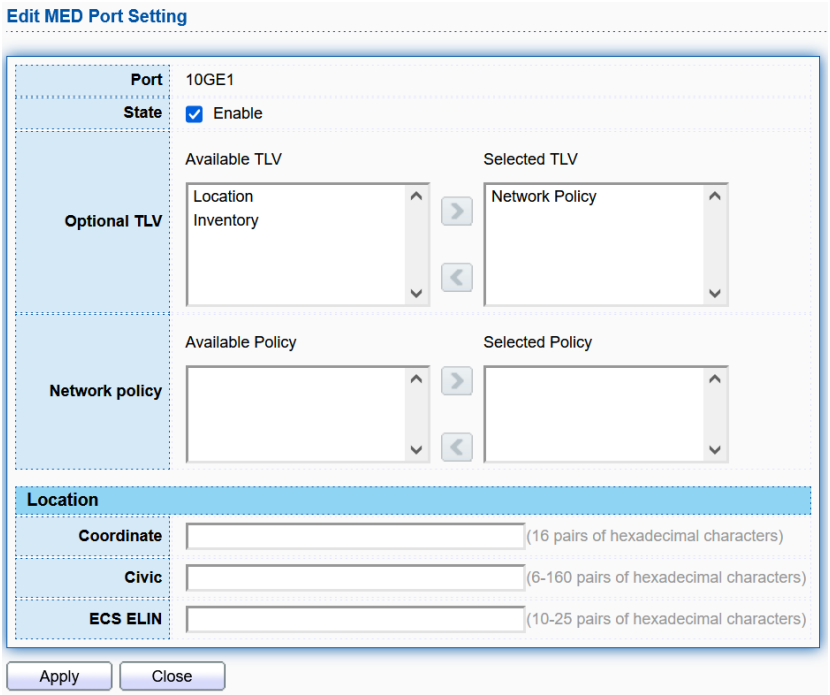
9.1.4 MED Port Setting

Click **Discovery** > **LLDP** > **MED Port Setting**

Use the LLDP MED Port Settings page to select the network policies, configured on the LLDP MED Network Policy page, to be advertised on the port, and select the LLDP MED TLVs to be sent inside the LLDP PDU.



Select the port and click “**Edit**” button to edit.

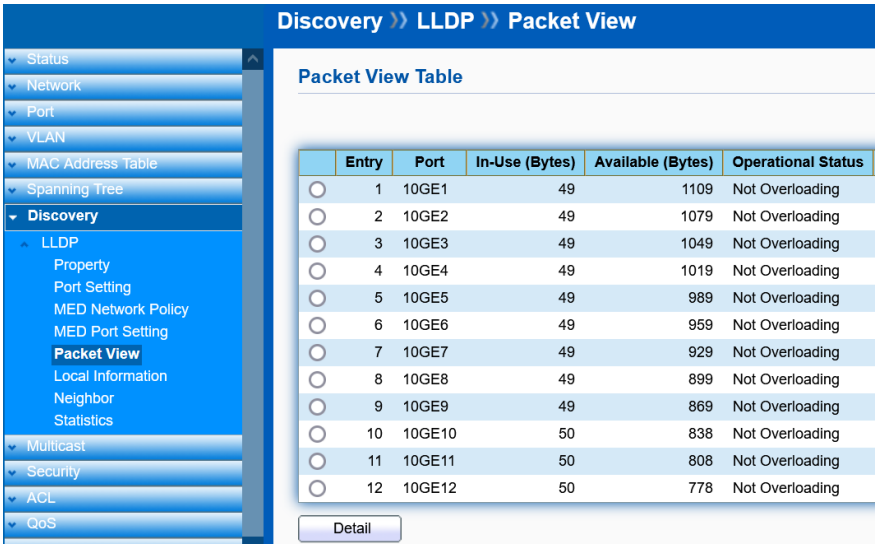


Field	Description
State	Enable or disable LLDP MED on this port.
Optional TLV	Select the TLVs that can be published by the switch, by moving them to the Selected Optional TLVs list.
Network Policy	Select the LLDP MED policies that will be published by LLDP, by moving them to the Selected Policy list. These policies were created on the LLDP MED Network Policy page.
Location	
Coordinate	Enter the coordinate location to be published by LLDP.
Civic	Enter the civic address to be published by LLDP.
ECS ELIN	Enter the Emergency Call Service (ECS) ELIN location to be published by LLDP.

9.1.5 Packet View

Click **Discovery** > **LLDP** > **Packet View**

To display LLDP packet information.



Field	Description
Port	Port Name
In-Use (Bytes)	Total number of bytes of LLDP information in each packet.
Available (Bytes)	Total number of available bytes left for additional LLDP information in each packet.
Operational Status	Overloading or not

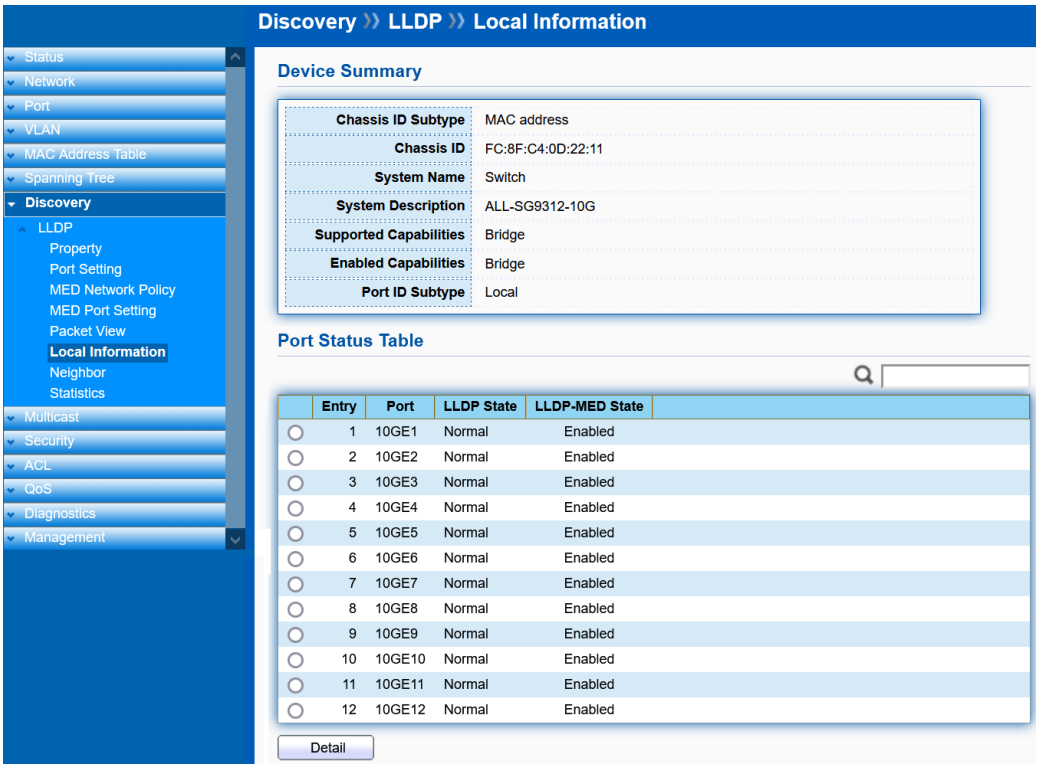
If need detail information, select the port, then click **Detail**.

Field	Description
Port	Port Name
Mandatory TLVs	Total mandatory TLV byte size. Status is sent or overloading.
802.3 TLVs	Total 802.3 TLVs byte size. Status is sent or overloading.
Optional TLVs	Total Optional TLV byte size. Status is sent or overloading.
802.1 TLVs	Total 802.1 TLVs byte size. Status is sent or overloading.
Total	Total number of bytes of LLDP information in each packet.

9.1.6 Local Information

Click **Discovery** > **LLDP** > **Local Information**

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



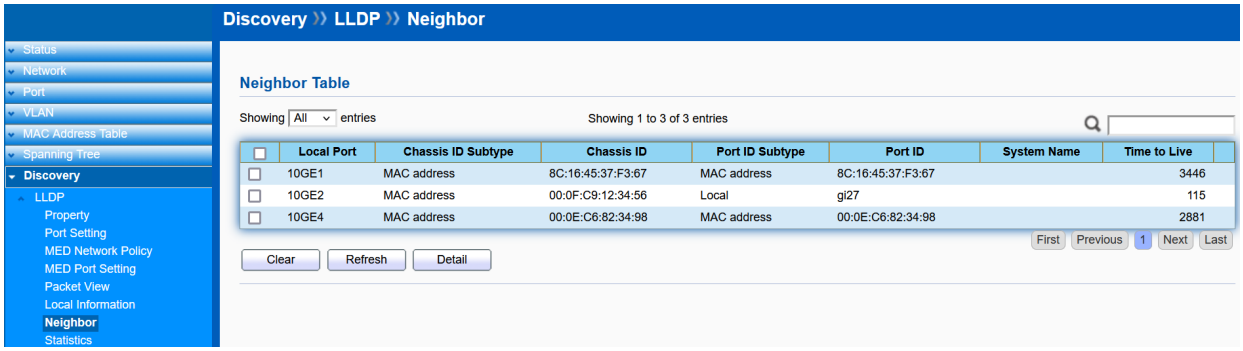
Field	Description
Chassis ID Subtype	Type of chassis ID, such as the MAC address.
Chassis ID	Identifier of chassis. Where the chassis ID subtype is a MAC address, the MAC address of the switch is displayed.
System Name	Name of switch
System Description	Description of the switch.
Capabilities Supported	Primary functions of the device, such as Bridge, WLAN AP, or Router.
Capabilities Enabled	Primary enabled functions of the device.
Port ID Subtype	Type of the port identifier that is shown.
LLDP Status	LLDP Tx and Rx abilities.
LLDP-MED Status	The status of LLDP-MED.

Click “**Detail**” button on the page to view detail information of the selected port.

9.1.7 Neighbor

Click **Discovery** > **LLDP** > **Neighbor**

Use the LLDP Neighbor page to view LLDP neighbors information.



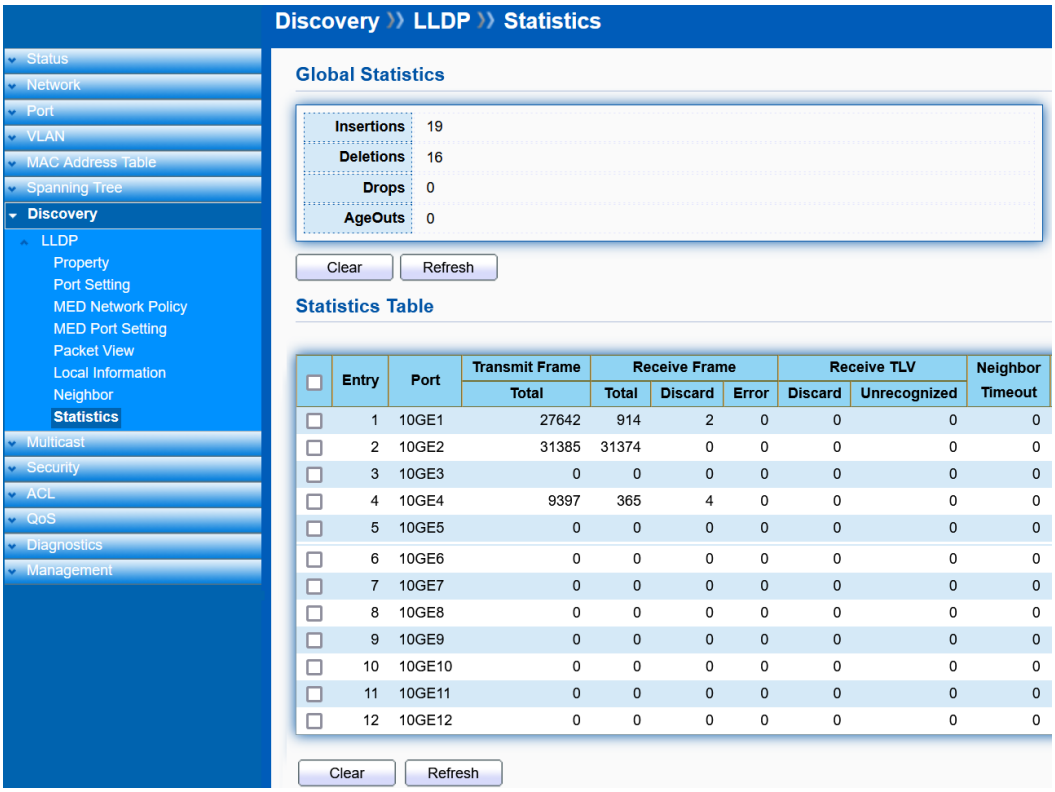
Field	Description
Local Port	Number of the local port to which the neighbor is connected.
Chassis ID Subtype	Type of chassis ID (for example, MAC address)
Chassis ID	Identifier of the 802 LAN neighboring device's chassis.
Port ID Subtype	Type of the port identifier that is shown.
Port ID	Identifier of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

Click "**Detail**" to view selected neighbor detail information.

9.1.8 Statistics

Click **Discovery** > **LLDP** > **Statistics**

The Link Layer Discovery Protocol (LLDP) Statistics page displays summary and per-port information for LLDP frames transmitted and received on the switch.



Field	Description
Insertions	The number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) has been inserted into tables associated with the remote systems.
Deletions	The number of times the complete set of information advertised by MSAP has been deleted from tables associated with the remote systems.
Drops	The number of times the complete set of information advertised by MSAP could not be entered into tables associated with the remote systems because of insufficient resources.
Age Outs	The number of times the complete set of information advertised by MSAP has been deleted from tables associated with the remote system because the information timeliness interval has expired.
Port	Interface or port number.
Transmit Frame Total	Number of LLDP frames transmitted on the corresponding port.
Receive Frame Total	Number of LLDP frames received by this LLDP agent on the corresponding port, while the LLDP agent is enabled.
Receive Frame Discard	Number of LLDP frames discarded for any reason by the LLDP agent on the corresponding port.
Receive Frame Error	Number of invalid LLDP frames received by the LLDP agent on the corresponding port, while the LLDP agent is enabled.
Receive TLV Discard	Number of TLVs of LLDP frames discarded for any reason by the LLDP agent on the corresponding port.
Receive TLV Unrecognized	Number of TLVs of LLDP frames that are unrecognized while the LLDP agent is enabled.
Neighbor Timeout	Number of age out LLDP frames.

Chapter 10 Multicast

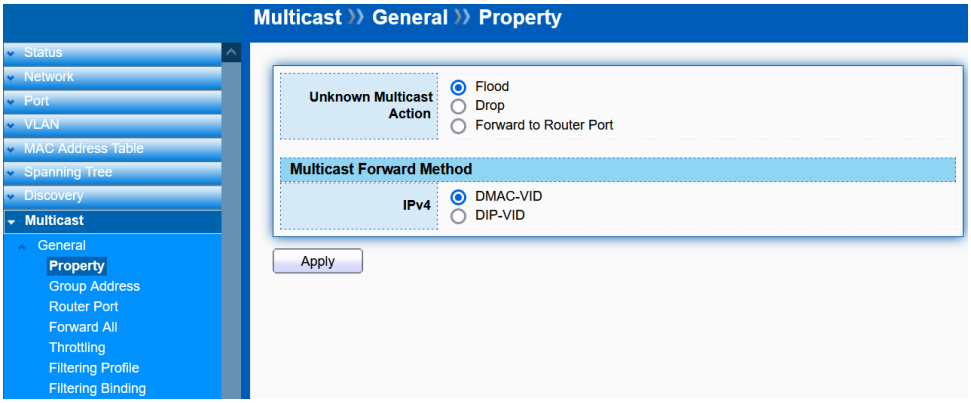
10.1 General

Use the General pages to configure setting of IGMP snooping property and group and router setting function.

10.1.1 Property

Click **Multicast** > **General** > **Property**

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

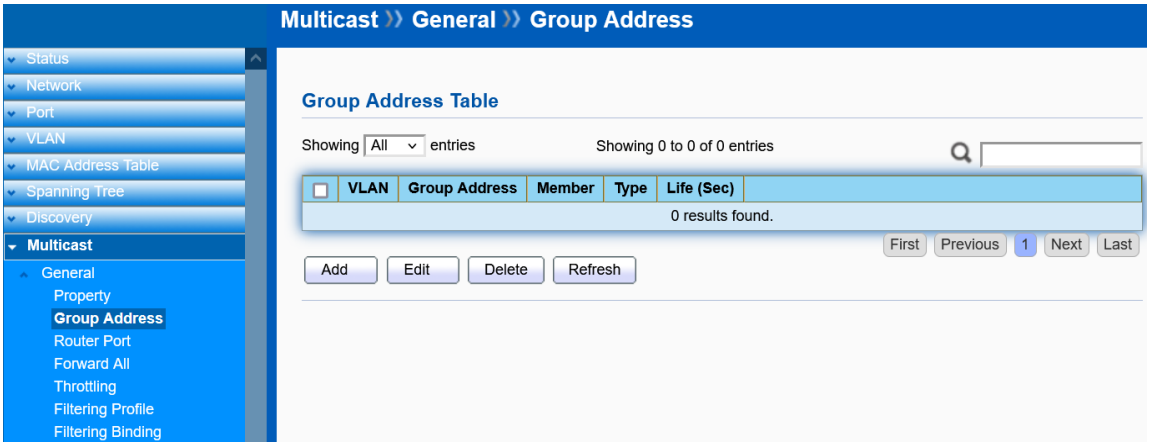


Field	Description
Unknown Multicast Action	Set the unknown multicast action **Drop**: drop the unknown multicast data. **Flood**: flood the unknown multicast data. **Router port**: forward the unknown multicast data to router port.
IPv4	Set the IPv4 multicast forward method. **MAC-VID**: forward method dmac+vid. **DIP-VID**: forward method dip+vid.

10.1.2 Group Address

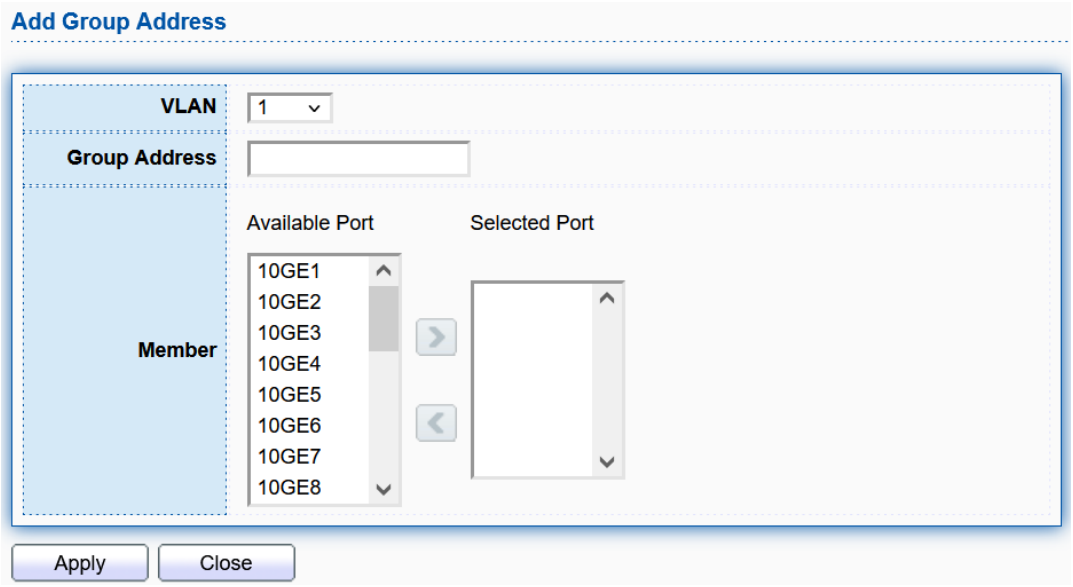
Click **Multicast** > **General** > **Group Address**

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



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

Click "**Add**/**Edit**" to add/edit Group Address.



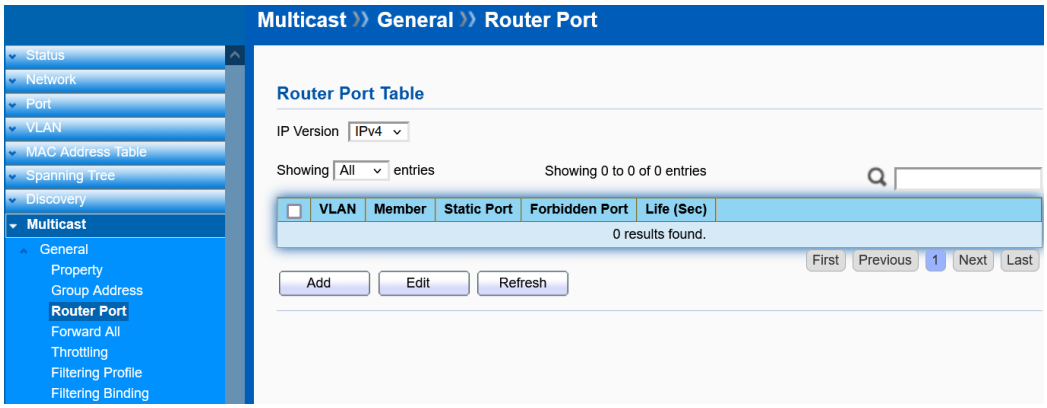
Field	Description
VLAN	The VLAN ID of group.
Group Address	The group IP address.
Member	The member ports of group. **Available Port**: Optional port member **Selected Port**: Selected port member

10.1.3 Router Port

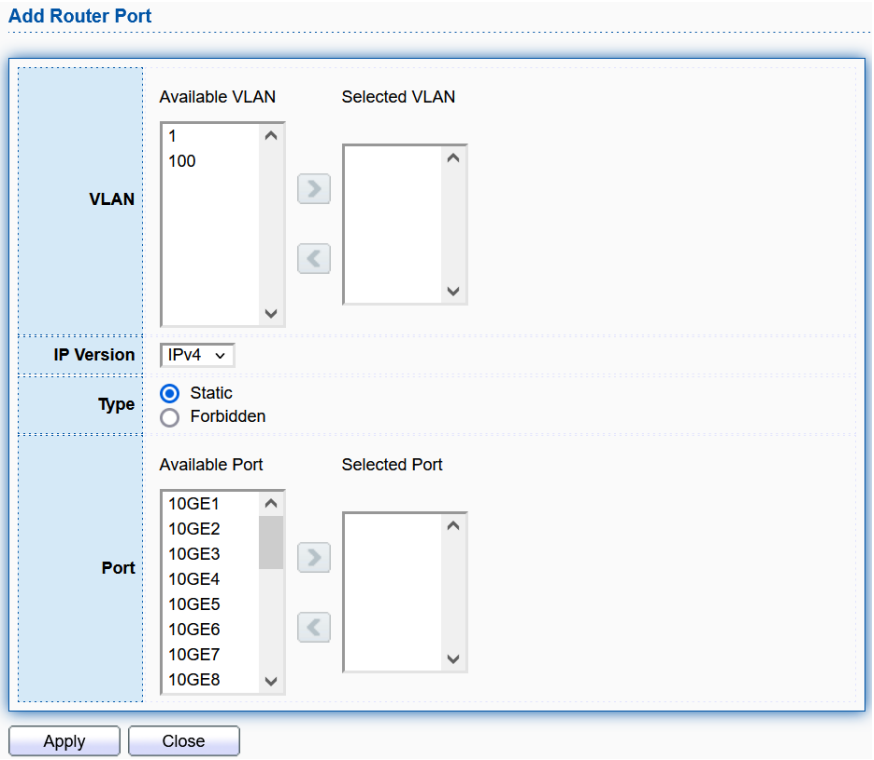
Click **Multicast** > **General** > **Router Port**

A Multicast router (Mrouter) port is a port that connects to a Multicast router. The switch includes the Mrouter port(s) when it forwards Multicast streams and IGMP/ MLD registration messages. It is required in order for all Mrouters can, in turn, forward the Multicast streams and propagate the registration messages to other subnets.

Use the Multicast Router Port page to statically configure or see dynamically detected ports connected to Mrouters.



Click “**Add**/**Edit**” to add/edit Router Port.

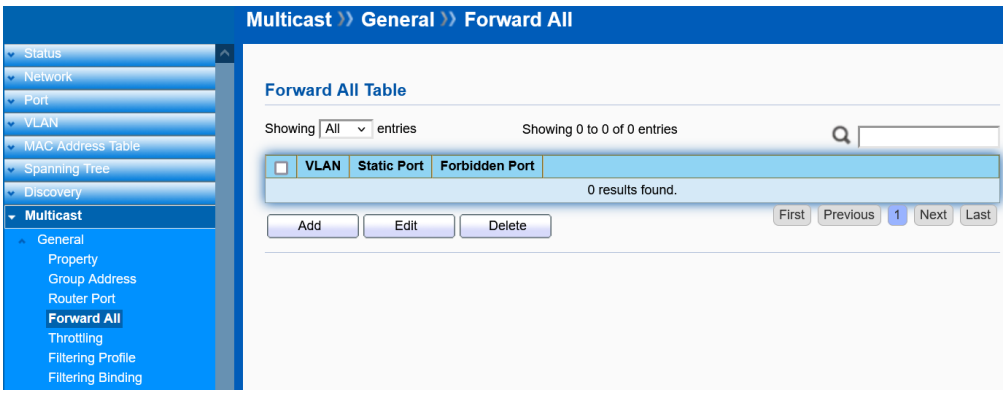


Field	Description
VLAN	Select the VLAN ID for the router ports
IP Version	IPv4 or IPv6
Type	For each interface, select its association type. The options are: **Static**: The port is statically configured as a Multicast router port. **Forbidden**: This port is not to be configured as a Multicast router port, even if IGMP or MLD queries are received on this port.
Port	Select the port(s) for the router ports

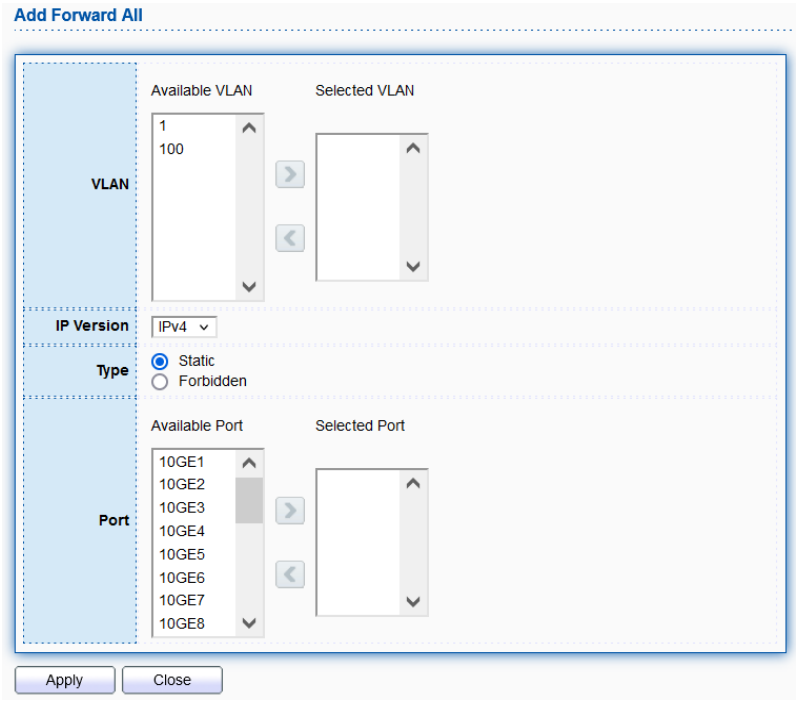
10.1.4 Forward All

Click **Multicast** > **General** > **Forward ALL**

Use the Forward All page to configure the ports or LAGs to receive Multicast streams from a specific VLAN. You can statically configure a port to Forward All if the devices connecting to the port do not support IGMP or MLD.



Click “**Add**/**Edit**” to add/edit Forward ALL table.

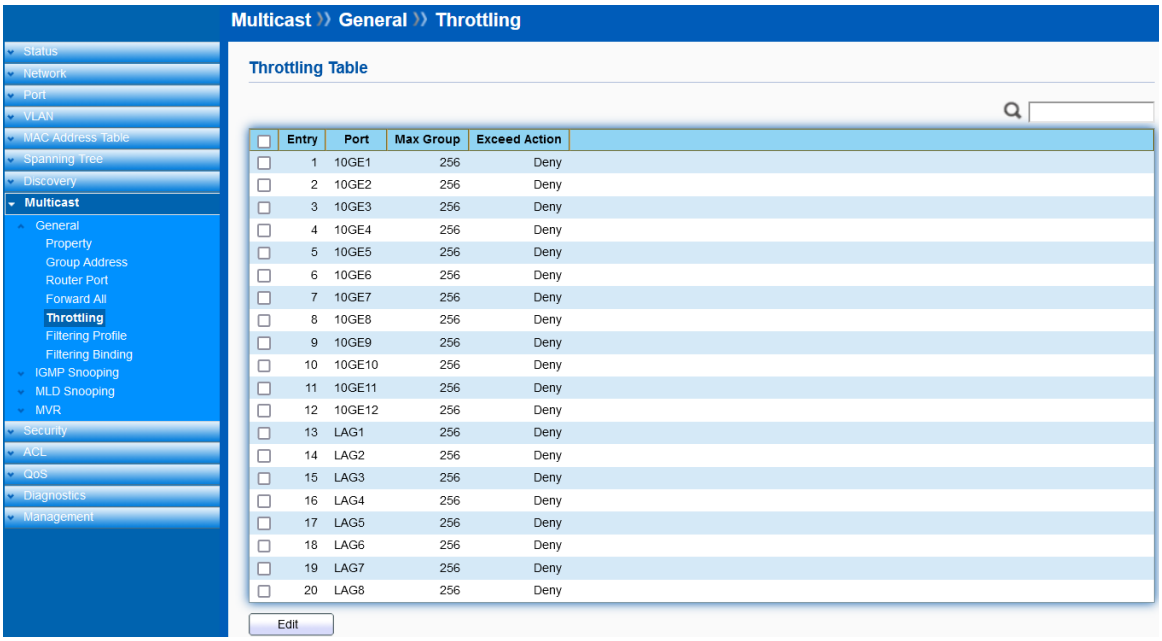


Field	Description
VLAN	Select the VLAN ID.
IP Version	IPv4 or IPv6
Type	Select the interface that is to be defined as Forward All by using the following methods: **Static**: The port receives all registered Multicast streams. **Forbidden**: The port cannot receive any registered Multicast streams, even if IGMP/MLD snooping designated the port to join a Multicast group.
Port	Select the port(s) for the Forward ALL.

10.1.5 Throttling

Click **Multicast** > **General** > **Throttling**

Use the Throttling page to configure the maximum number of Multicast groups that are allowed on each interface and specify the action when the limit reaches.



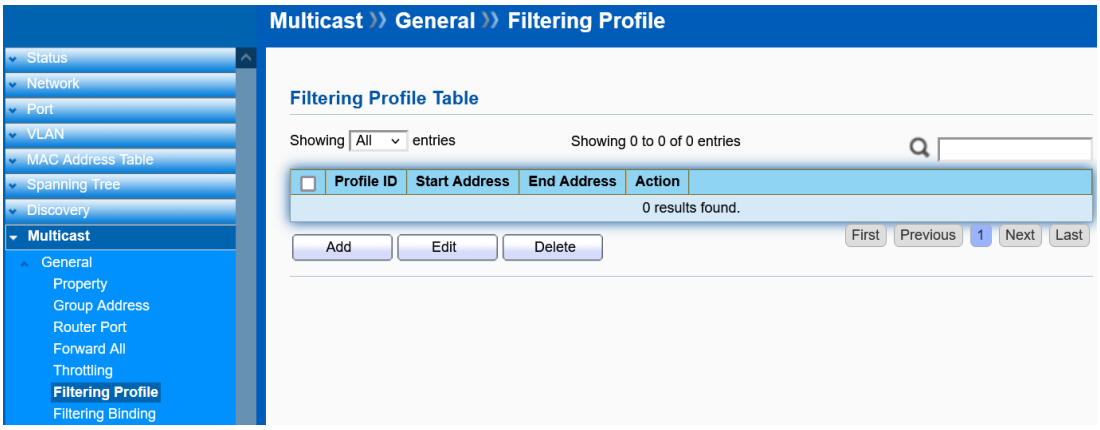
Select port and click “**Edit**” to edit Throttling.

Field	Description
Max Group	Enter the maximum number of IGMP groups that are allowed on the interface.
Exceed Action	**Deny** or **Replace** the existing group with the new group for which the IGMP report was received when the limit is reached.

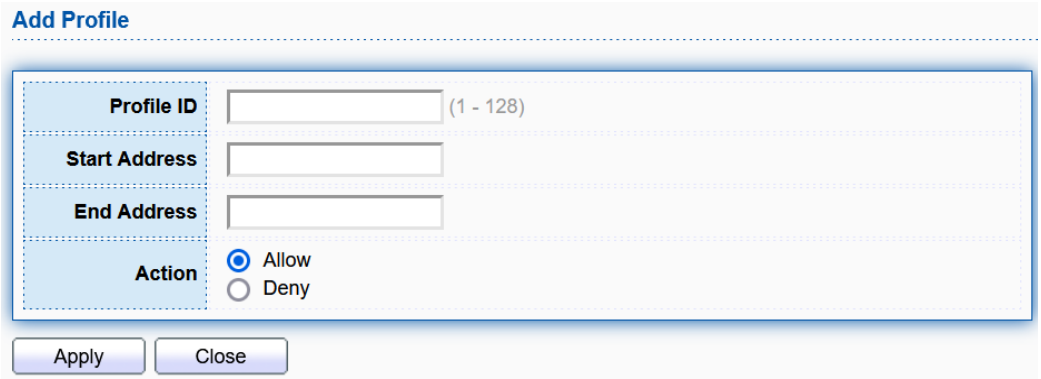
10.1.6 Filtering Protocol

Click **Multicast** > **General** > **Filtering Protocol**

A Multicast filter profile permits or denies a range of Multicast groups to be learned when the join group matches the filter profile IP group range.



Click “**Add**/**Edit**” to add/edit a filtering profile.

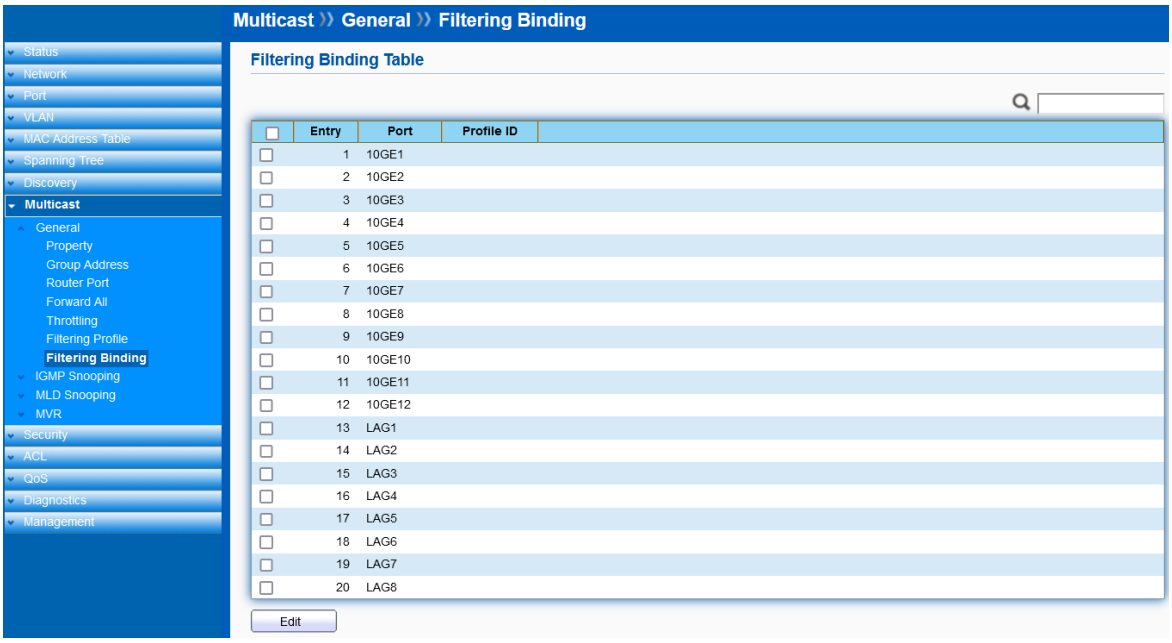


Field	Description
Profile ID	Enter the sequence number for the profile.
IP Version	Select ether IPv4 or IPv6 to apply the filter profile to IPv4 or IPv6 Multicast traffic.
Start Address	Enter the starting Multicast group address.
End Address	Enter the ending Multicast group address.
Action	**Allow** or **Deny** Multicast frames when the join group matches the profile IP group range.

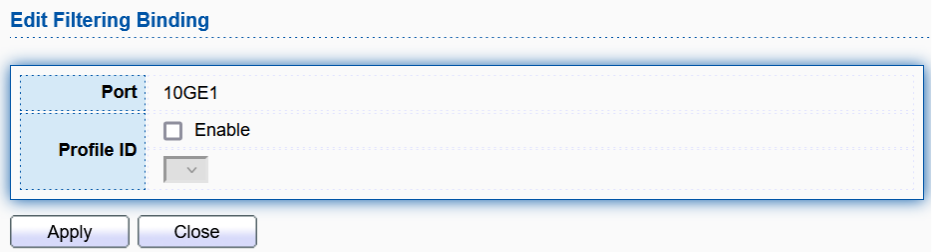
10.1.7 Filtering Binding

Click **Multicast** > **General** > **Filtering Binding**

To assign a Multicast filter profile to an interface to deny or permit the Multicast group when the join group matches the filter profile



Select port and click “**Edit**” to assign Filter profile.



Field	Description
Profile ID	Check Enable and select filter profile.

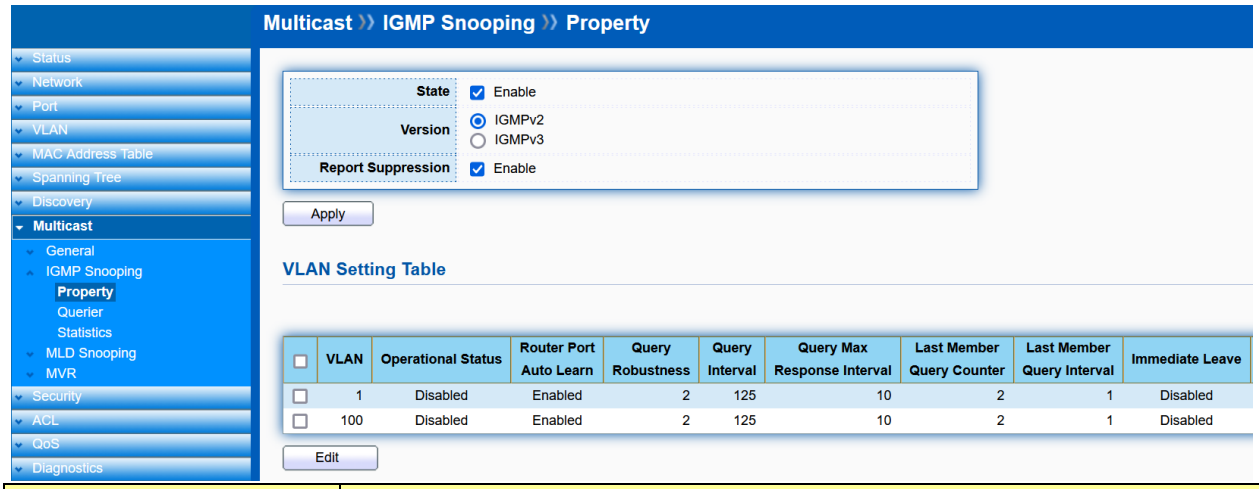
10.2 IGMP Snooping

Use the IGMP Snooping pages to configure setting of IGMP snooping function

10.2.1 Property

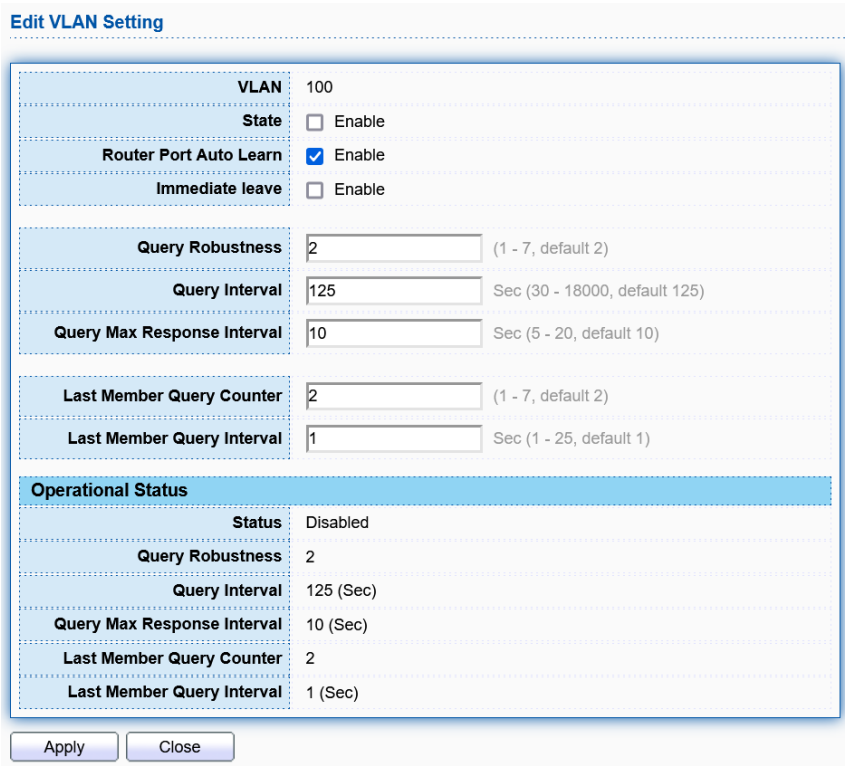
Click **Multicast** > **IGMP Snooping** > **Property**

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



Field	Description
State	Set the enabling status of IGMP Snooping functionality **Enable**: If Checked Enable IGMP Snooping, else is Disabled IGMP Snooping.
Version	Set the IGMP Snooping version **IGMPv2**: Only support process IGMP v2 packet. **IGMPv3**: Support v3 basic and v2.
Report Suppression	Set the enabling status of IGMP v2 report suppression. **Enable**: If Checked Enable IGMP Snooping v2 report suppression, else Disable the report suppression function.
VLAN	The IGMP entry VLAN ID.
Operation Status	The enable status of IGMP Snooping VLAN functionality.
Router Port Auto Learn	The enabling status of IGMP Snooping router port auto learning
Query Robustness	The Query Robustness allows tuning for the expected packet lose on a subnet.
Query Interval	The interval of query to send general query.
Query Max Response Interval	In Membership Query Messages, it specifies the maximum allowed time before sending a responding report in units of 1/10 second.
Last Member Query count	The count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Last Member Query Interval	The interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Immediate Leave	The immediate leave status of the group will immediate leave when receive IGMP Leave message.

Click “**Edit**” to edit VLAN Setting.



Field	Description
VLAN	The selected VLAN List
State	Set the enabling status of IGMP Snooping VLAN functionality **Enable**: If Checked Enable IGMP Snooping router VLAN, else is Disabled IGMP Snooping VLAN.
Router Port Auto Learn	Set the enabling status of IGMP Snooping router port learning. **Enable**: If Checked Enable learning router port by query and PIM, DVRMP, else Disable the learning router port.
Immediate Leave	Immediate Leave the group when receive IGMP Leave message. **Enable**: If Checked Enable immediate leave, else Disable immediate leave.
Query Robustness	The Admin Query Robustness allows tuning for the expected packet loss on a subnet.
Query Interval	The Admin interval of querier to send general query.
Query Max Response Interval	The Admin query max response interval, In Membership Query Messages, it specifies the maximum allowed time before sending a responding report in units of 1/10 second.
Last Member Query Counter	The Admin last member query count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Last Member Query Interval	The Admin last member query interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.

Operational Status

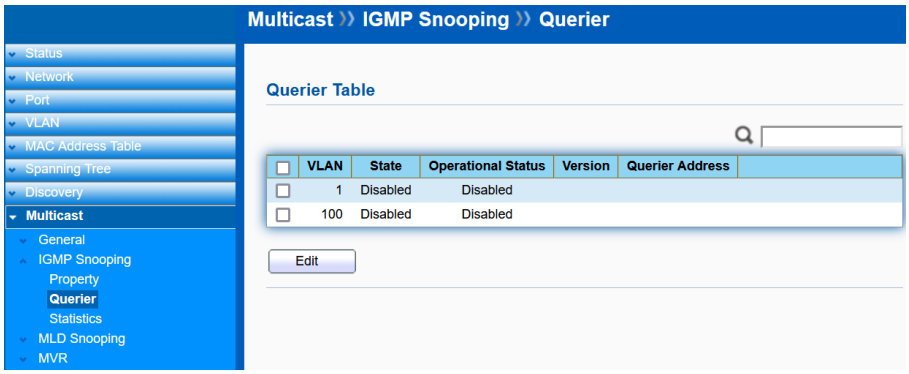
Field	Description
Status	Operational IGMP Snooping status, must both IGMP Snooping global and IGMP Snooping enable the status will be enable.
Query Robustness	Operational Query Robustness.
Query Interval	Operational Query Interval.

Query Max Response Interval	Operational Query Max Response Interval.
Last Member Query Counter	Operational Last Member Query Count.
Last Member Query Interval	Operational Last Member Query Interval.

10.2.2 Querier

Click **Multicast** > **IGMP Snooping** > **Querier**

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



Field	Description
VLAN	IGMP Snooping querier entry VLAN ID.
State	The IGMP Snooping querier Admin State.
Operational Status	The IGMP Snooping querier operational status.
Querier Version	The IGMP Snooping querier operational version.
Querier IP	The operational querier IP address on the VLAN.

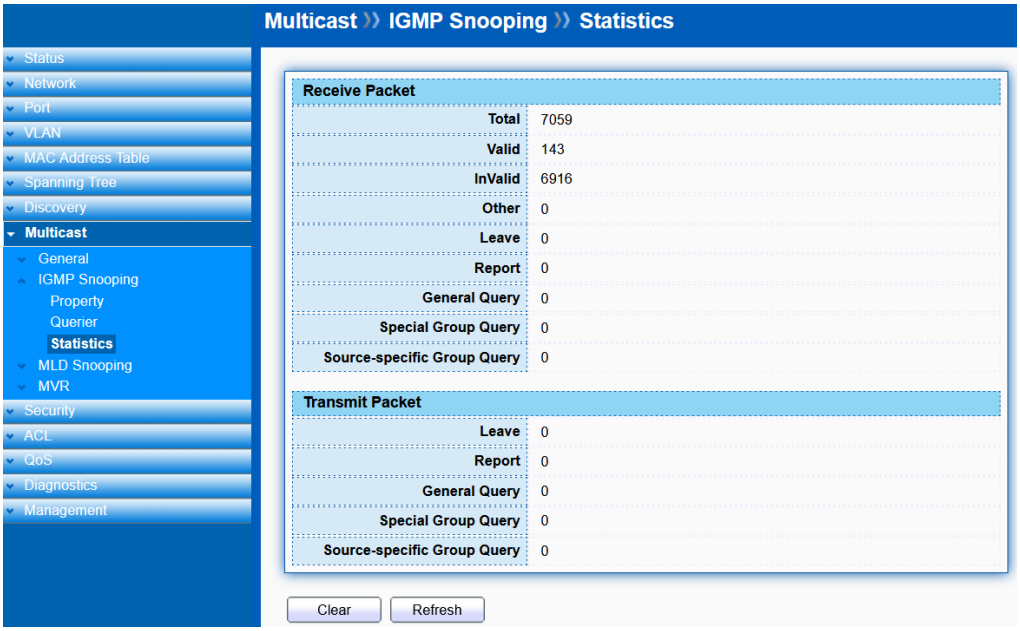
Click "**Edit**" to edit IGMP Snooping Querier.

Field	Description
VLAN	The selected Edit IGMP Snooping querier VLAN list.
State	Set the enabling status of IGMP Querier Election on the chose VLANs. **Enabled**: If checked Enable IGMP Querier, else Disable IGMP Querier.
Version	Set the query version of IGMP Querier Election on the chose VLANs. **IGMPv2**: Querier version 2 **IGMPv3**: Querier version 3. (IGMP Snooping version should be IGMPv3)

10.2.3 Statistics

Click **Multicast** > **IGMP Snooping** > **Statistics**

This page allows user to display IGMP Snooping Statistics and clear IGMP Snooping statistics.



Receive Packet

Field	Description
Total	Total RX IGMP packet, include IPv4 multicast data to CPU.
Valid	The valid IGMP Snooping process packet.
InValid	The invalid IGMP Snooping process packet.
Other	The ICMP protocol is not 2, and is not IPv4 multicast data packet.
Leave	IGMP leave packet.
Report	IGMP join and report packet.
General Query	IGMP general query packet
Special Group Query	IGMP special group general query packet
Source-specific Group Query	IGMP special source and group general query packet

Transmit Packet

Field	Description
Leave	IGMP leave packet
Report	IGMP join and report packet
General Query	IGMP general query packet includes querier transmit general query packet.
Special Group Query	IGMP special group query packet include querier transmit special group query packet.
Source-specific Group Query	IGMP special source and group general query packet.

10.3 MLD Snooping

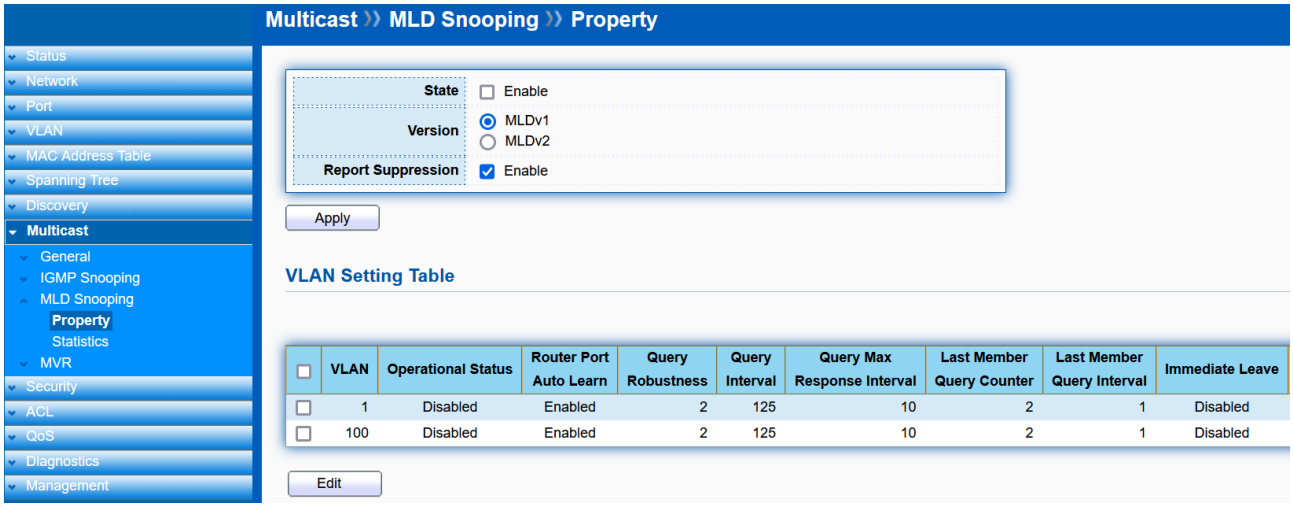
Multicast Listener Discovery (MLD) Snooping operates on the IPv6 traffic level for discovering

multicast listeners on a directly attached port and performs a similar function to IGMP Snooping for IPv4. MLD snooping allows the Switch to examine MLD packets and make forwarding decisions based on content. MLD Snooping limits IPv6 multicast traffic by dynamically configuring the Switch port so that multicast traffic is forwarded only to those ports that wish to receive it. This reduces the flooding of IPv6 multicast packets in the specified VLANs. Both IGMP and MLD Snooping can be active at the same time

10.3.1 Property

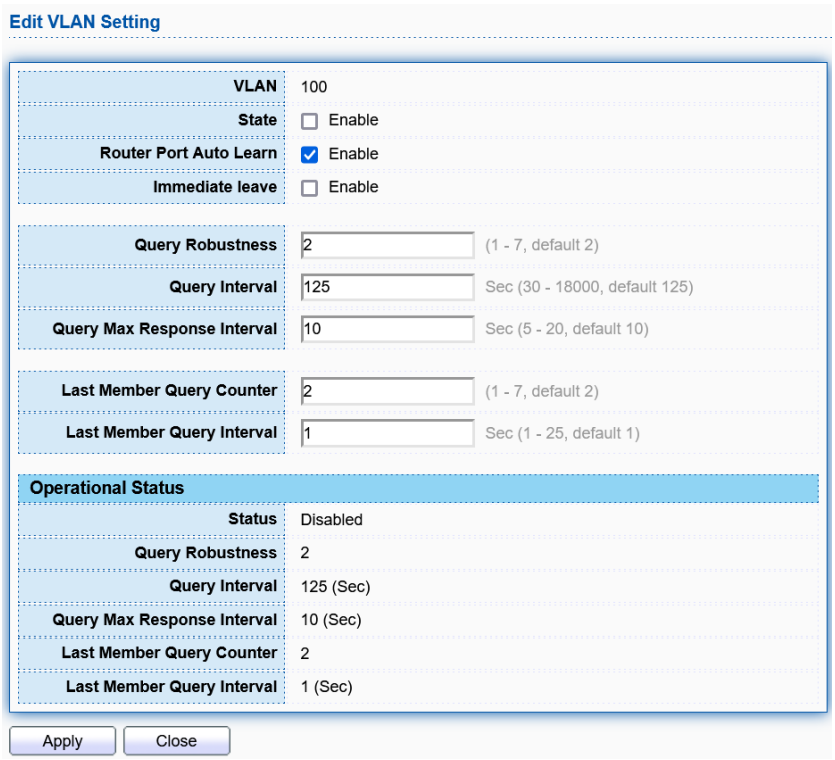
Click **Multicast** > **MLD Snooping** > **Property**

This page allows user to configure global settings of MLD snooping and configure specific VLAN settings of MLD Snooping.



Field	Description
State	Check to enable MLD Snooping.
Version	Select either MLDv1 or MLDv2.
Report Suppression	Enable or disable MLD Snooping report suppression. Disabling this feature will forward all MLDv1 reports to Multicast routers.

Click “**Edit**” to edit VLAN Setting.



Field	Description
VLAN	The selected VLAN List
State	Set the enabling status of IGMP Snooping VLAN functionality **Enable**: If checked Enable MLD Snooping router VLAN, else is Disabled MLD Snooping VLAN.
Router Port Auto Learn	Set the enabling status of MLD Snooping router port learning. **Enable**: If checked Enable learning router port by query and PIM, DVRMP, else Disable the learning router port.
Immediate Leave	Immediate Leave the group when receive MLD Leave message. **Enable**: If checked Enable immediate leave, else Disable immediate leave.
Query Robustness	The Admin Query Robustness allows tuning for the expected packet loss on a subnet.
Query Interval	The Admin interval of querier to send general query.
Query Max Response Interval	The Admin query max response interval, In Membership Query Messages, it specifies the maximum allowed time before sending a responding report in units of 1/10 second.
Last Member Query Counter	The Admin last member query count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Last Member Query Interval	The Admin last member query interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.

Operational Status.

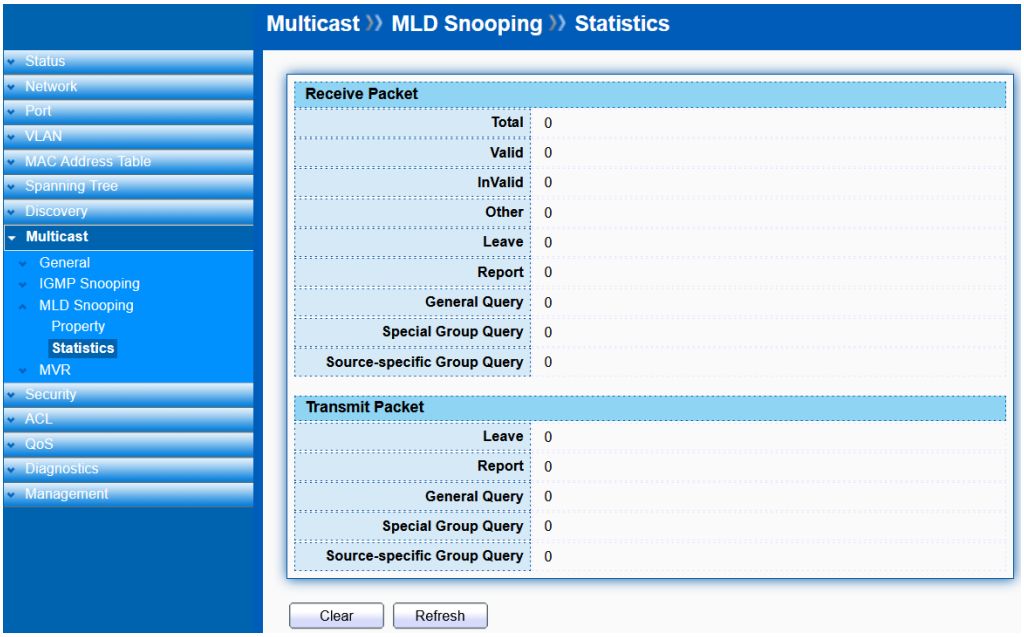
Field	Description
Status	Operational MLD Snooping status, must both MLD Snooping global and MLD Snooping enable the status will be enable.
Query Robustness	Operational Query Robustness.
Query Interval	Operational Query Interval.
Query Max Response Interval	Operational Query Max Response Interval.

Last Member Query Counter	Operational Last Member Query Count.
Last Member Query Interval	Operational Last Member Query Interval.

10.3.2 Statistics

Click **Multicast** > **MLD Snooping** > **Statistics**

This page allows user to display IMLD Snooping Statistics and clear MLD Snooping statistics.



Receive Packet

Field	Description
Total	Total RX MLD packet, include IPv6 multicast data to CPU.
Valid	The valid MLD Snooping process packet.
InValid	The invalid IMLD Snooping process packet.
Other	The ICMP protocol is not 2, and is not IPv6 multicast data packet.
Leave	MLD leave packet.
Report	MLD join and report packet.
General Query	MLD general query packet
Special Group Query	MLD special group general query packet
Source-specific Group Query	MLD special source and group general query packet

Transmit Packet

Field	Description
Leave	MLD leave packet
Report	MLD join and report packet
General Query	MLD general query packet includes querier transmit general query packet.
Special Group Query	MLD special group query packet include querier transmit special group query packet.

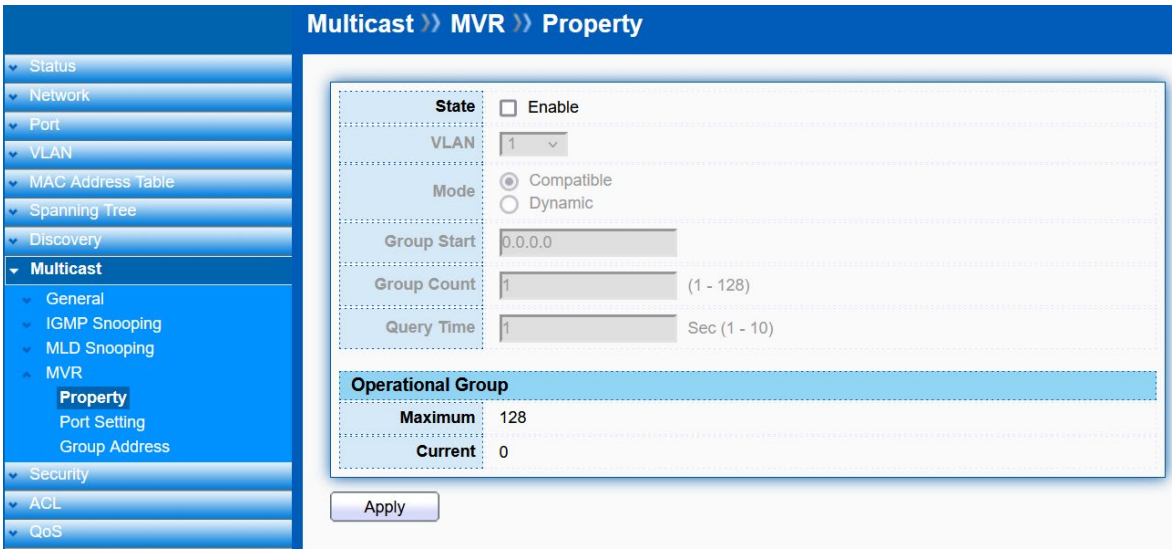
Source-specific Group Query	MLD special source and group general query packet.

10.4 MVR

10.4.1 Property

Click **Multicast** > **MVR** > **Property**

Multicast VLAN Registration (MVR) allows multicast traffic to be dedicated to a specific VLAN across a multicast domain so that receivers in other VLANs can join the sources in the dedicated VLAN and received multicast traffic.

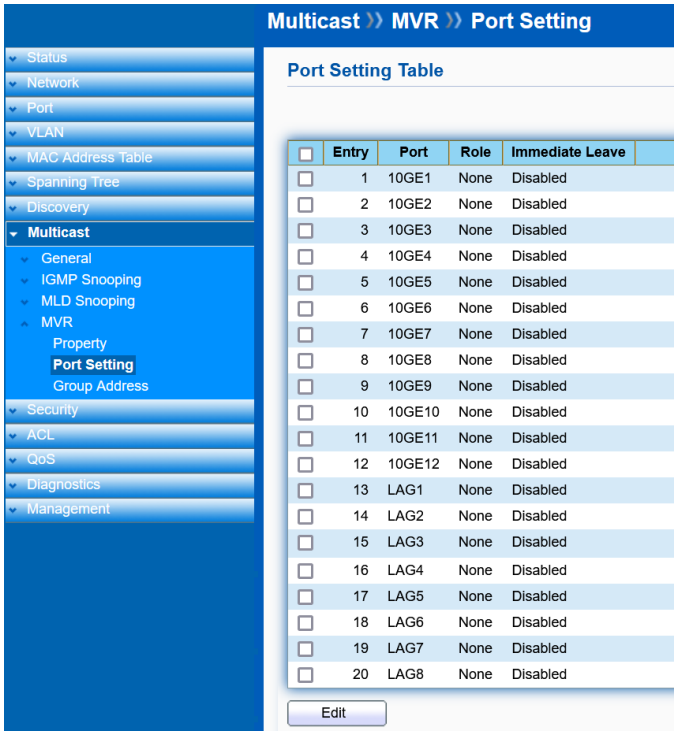


Field	Description
State	Check to enable MVR.
VLAN	Specify the Multicast VLAN ID.
Mode	Specify the MVR mode of operation. In **Compatible** mode, MVR membership reports are forbidden on source ports. In **Dynamic** mode, MVR allows dynamic MVR membership reports on source ports.
Group Start	The starting IPv4/IPv6 Multicast Group Address that will be used as a streaming channel.
Group Count	Specify the count of the multicast group.
Query Time	Defines the maximum time to wait for IGMP report memberships on a receiver port before removing the port from multicast group membership. The range is 1 to 10.

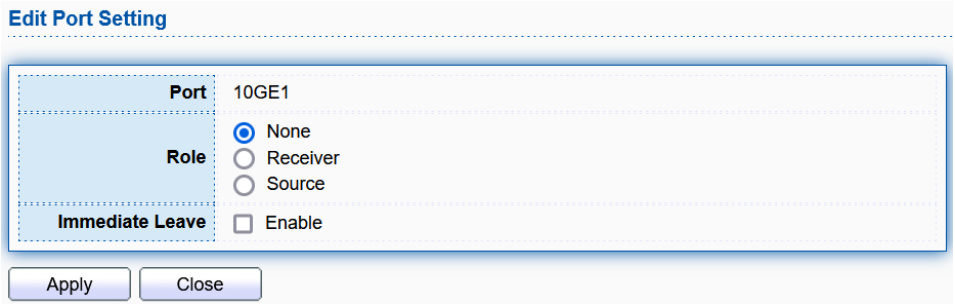
10.4.2 Port Setting

Click **Multicast** > **MVR** > **Port Setting**

This page allows user to configure MVR role in each port.



Check the port and click "**Edit**" to edit Port Setting.

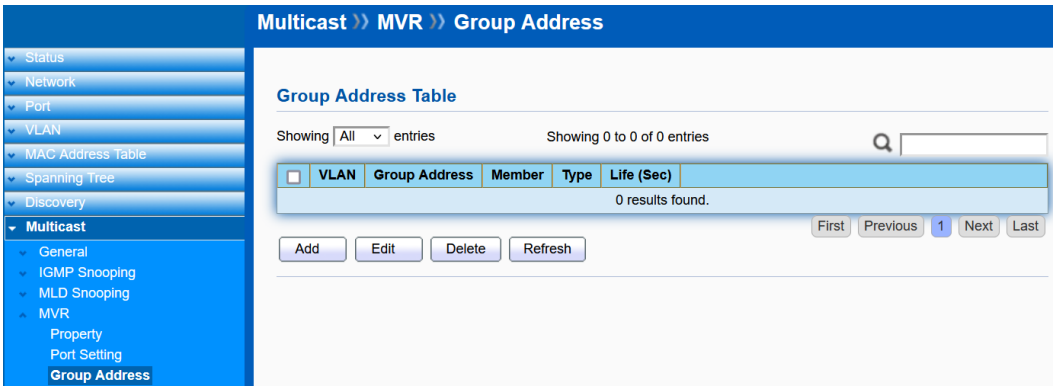


Field	Description
Port	The selected port.
Role	**None**: The designated port does not participate MVR operations. **Receiver**: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages. **Source**: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports.
Immediate Leave	Check to enable the fast leave on the port.

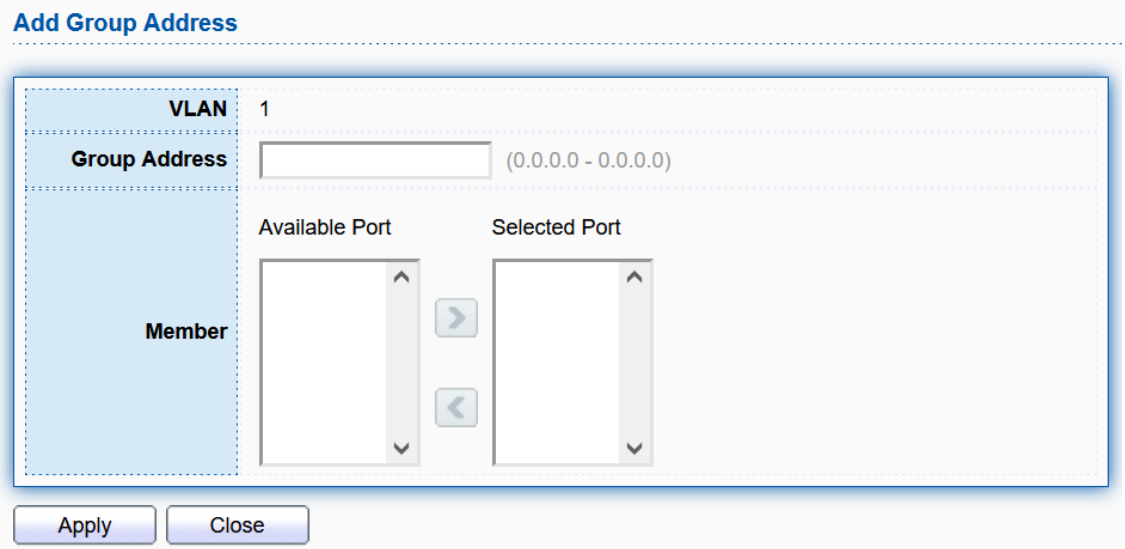
10.4.3 Group Address

Click **Multicast** > **MVR** > **Group Address**

This page allows user to assign the port(s) to group address.



Click “**Add**” or “**Edit**” to add or edit Group Address.



Field	Description
VLAN	The multicast VLAN ID.
Group Address	Specify the group address.
Member	Select the port(s) to be the group member.

Chapter 11 Security

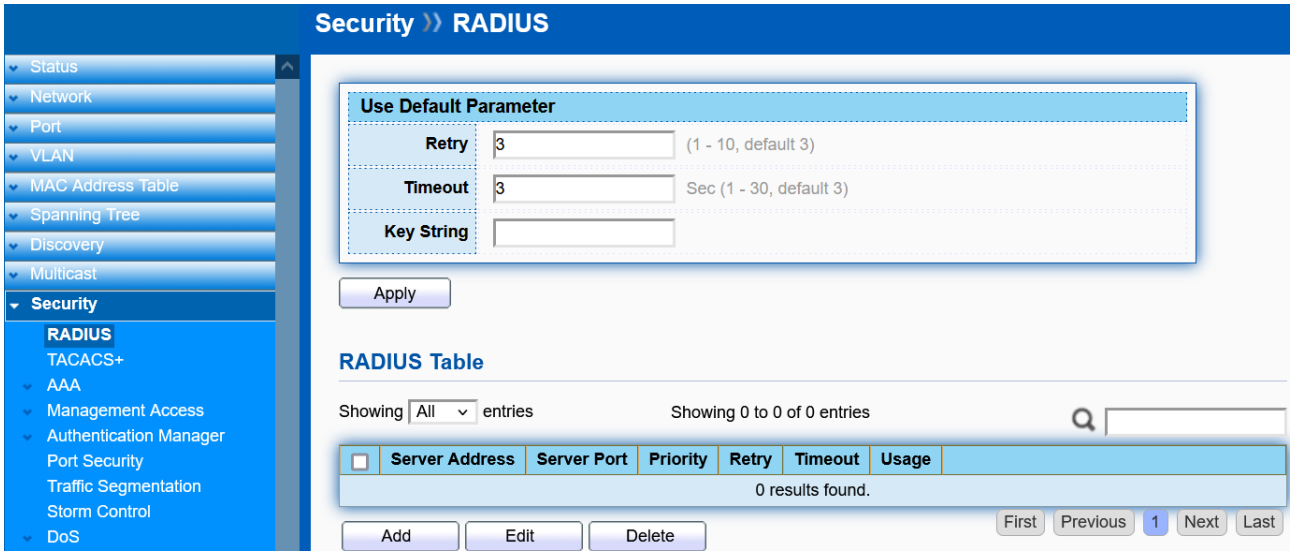
Use the security pages to configure setting for the switch security features.

11.1 RADIUS

Click **Security** > **RADIUS**

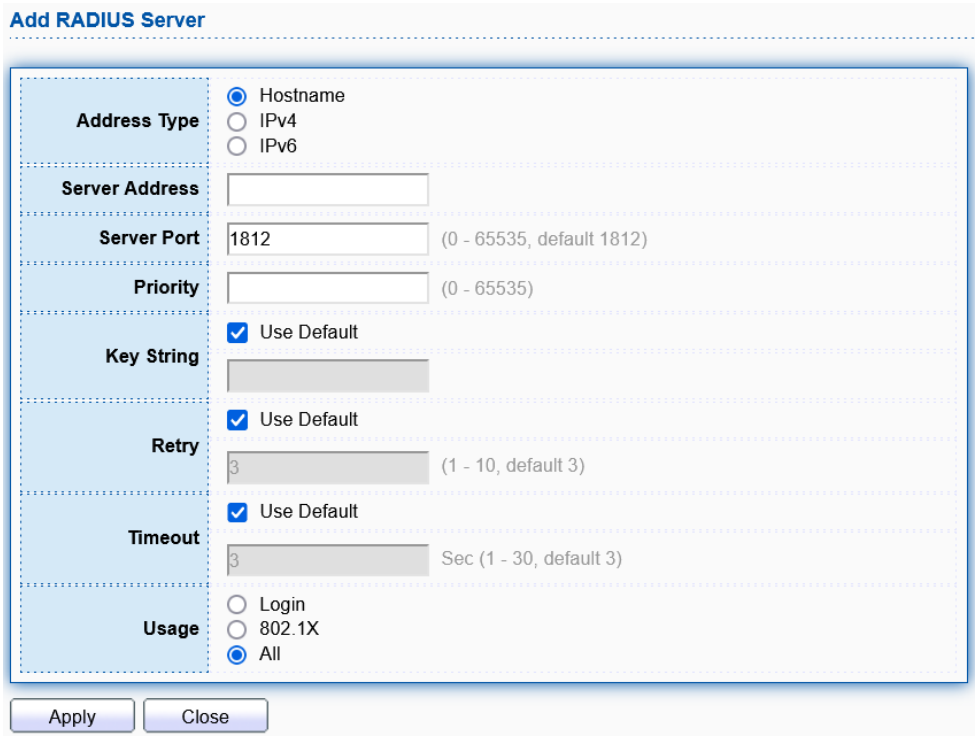
Remote Authentication Dial-In User Service (**RADIUS**) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service.

This page allows user to set up RADIUS server.



Field	Description
Retry	Enter the number of transmitted requests sent to the Radius server before a failure occurs. The default is 3.
Timeout	Enter the amount of time the device waits for an answer from the Radius Server before switching to the next server. The default value is 3.
Key String	Enter the Key String used for encrypting all Radius communication between the device and the Radius server.

Click “**Add**” or “**Edit**” to add or edit RADIUS server.



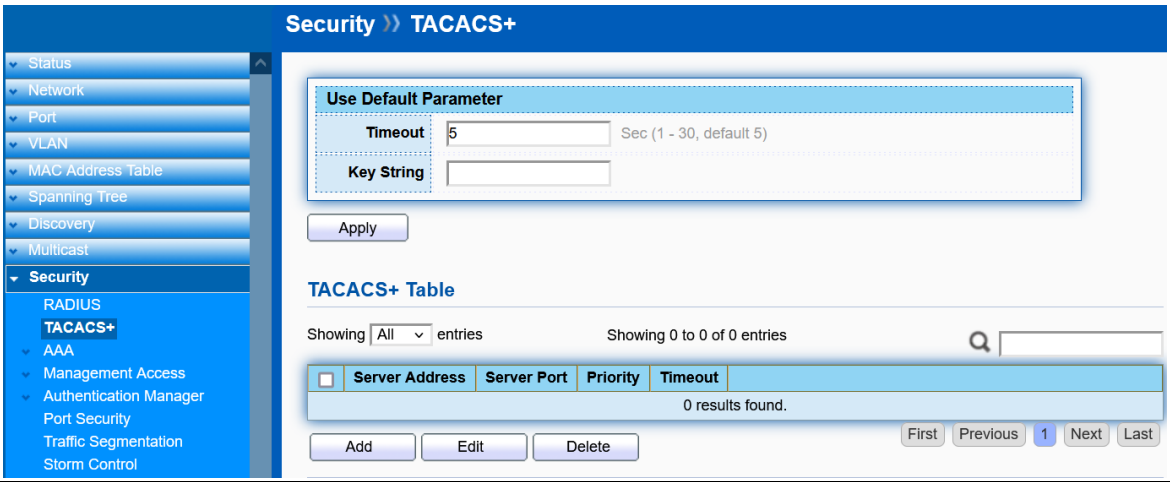
Field	Description
Address Type	Specify the address type to “Hostname”, “IPv4”, or “IPv6”.
Server Address	Specify the Hostname/IPv6/IPv4 address for the RADIUS server.
Server Port	Enter the server port number. The default port is 1812.
Key String	Enter the Key String used for encrypting all Radius communication between the device and the Radius server.
Retry	Enter the number of transmitted requests sent to the Radius server before a failure occurs. The default is 3.
Timeout	Enter the amount of time the device waits for an answer from the Radius Server before switching to the next server. The default value is 3.
Usage	Select the usage: Login, 802.1X, All.

11.2 TACACS+

Click **Security** > **TACACS+**

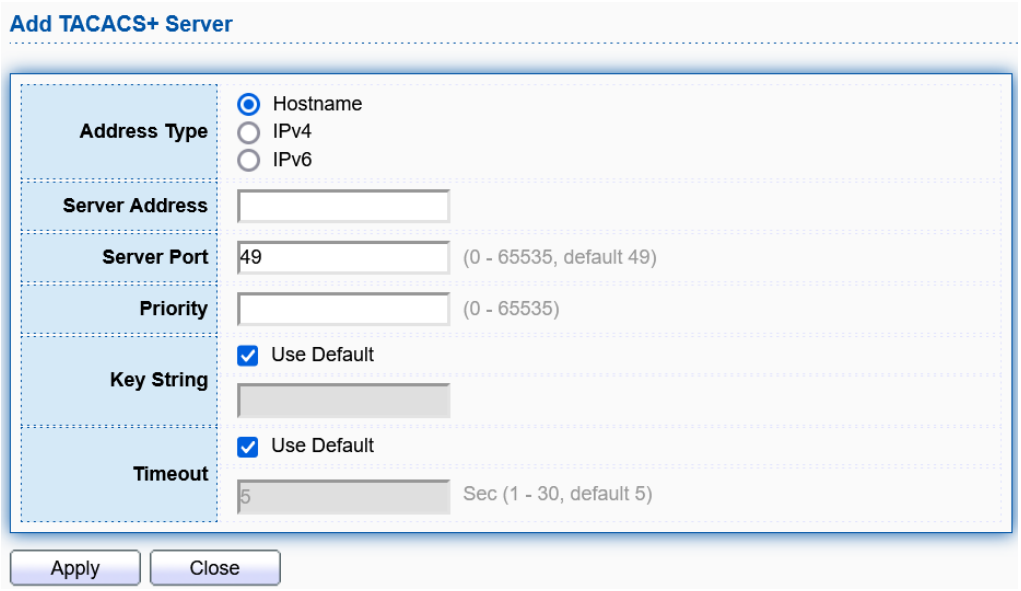
Terminal Access Controller Access-Control System Plus (**TACACS+**) is a protocol developed by Cisco. TACACS+ handles authentication, authorization, and accounting (AAA) services.

This page allows user to set up TACACS+ server.



Field	Description
Timeout	Enter the amount of time the device waits for an answer from the TACACS+ Server before switching to the next server. The default value is 3.
Key String	Enter the Key String used for encrypting all TACACS+ communication between the device and the TACACS+ server.

Click “**Add**” or “**Edit**” to add or edit TACACS+ server.



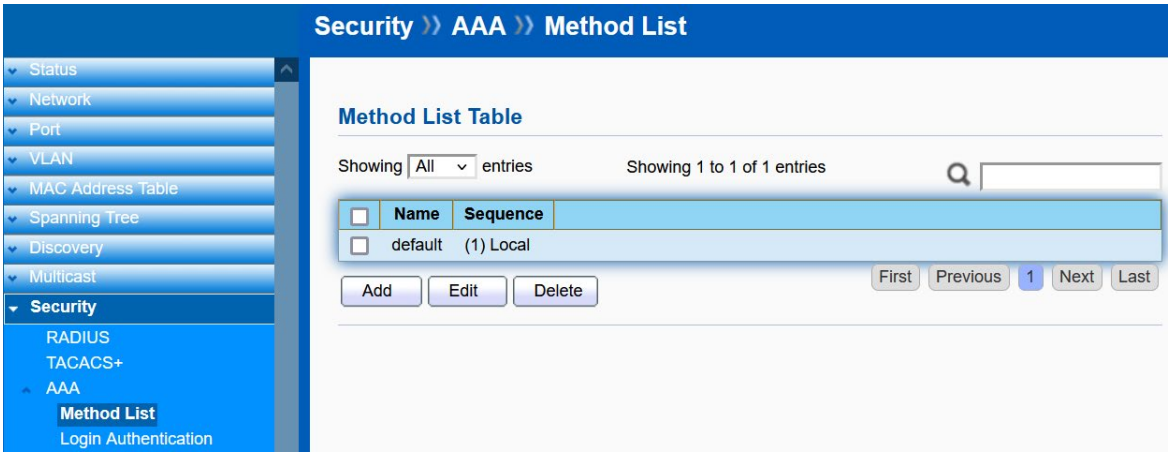
Field	Description
Address Type	Specify the address type to “Hostname”, “IPv4”, or “IPv6”.
Server Address	Specify the Hostname/IPv6/IPv4 address for the TACACS+ server.
Server Port	Enter the server port number. The default port is 49.
Key String	Enter the Key String used for encrypting all TACACS+ communication between the device and the TACACS+ server.
Timeout	Enter the amount of time the device waits for an answer from the TACACS+ Server before switching to the next server. The default value is 5.

11.3 AAA

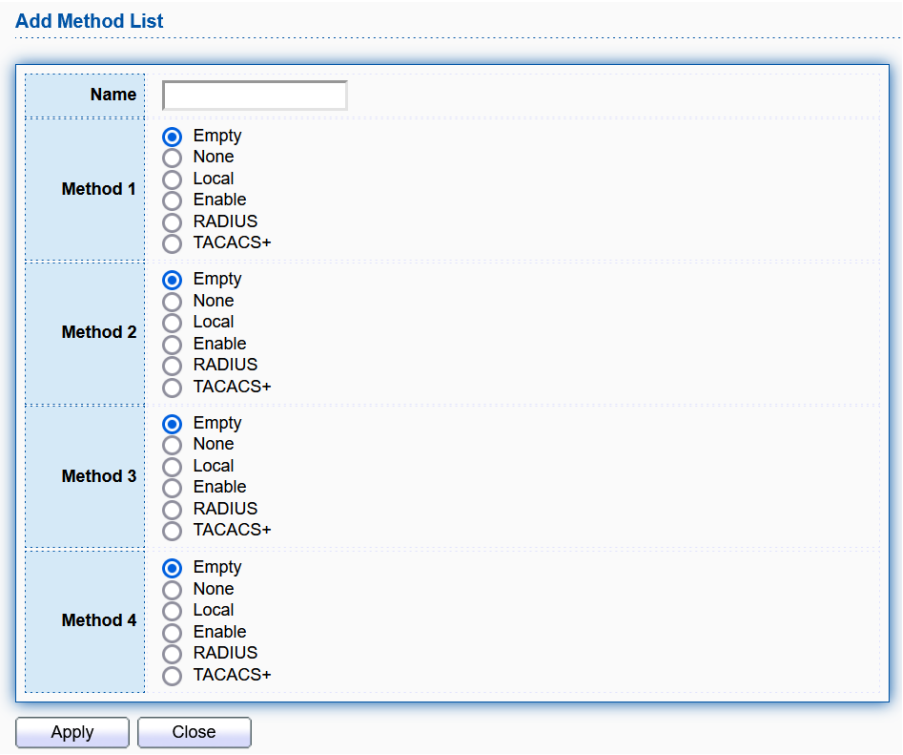
11.3.1 Method List

Click **Security** >**AAA** > **Method List**

This page allows user to change Method List.



Click “**Add**” or “**Edit**” to add or edit Method List.



11.3.2 Login Authentication

Click **Security** >**AAA** > **Login Authentication**

This page allows user to change Login Authentication. User can change the login authentication method for “Console”, “Telnet”, “SSH”, “HTTP” and “HTTPS”.

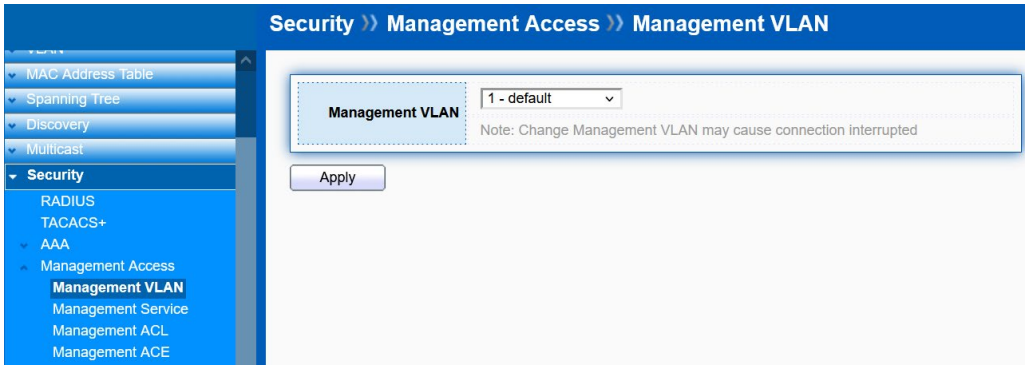
11.4 Management Access

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

11.4.1 Management VLAN

Click **Security** > **Management Access** > **Management VLAN**

This page allow user to change Management VLAN connection.

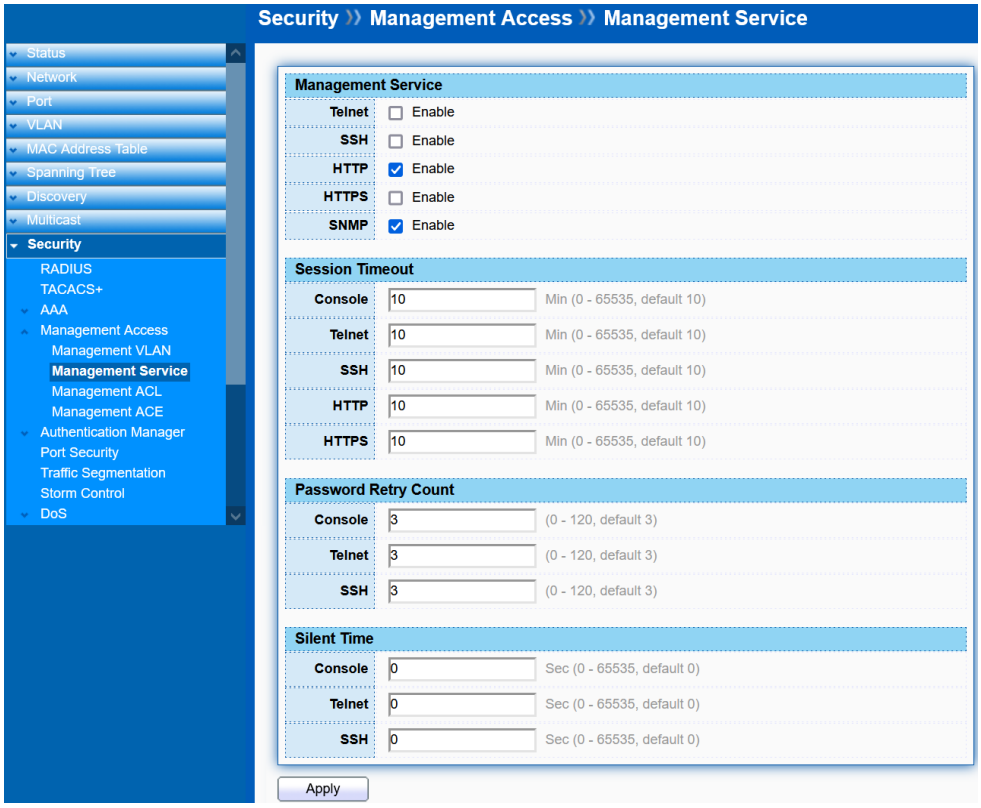


Field	Description
Management VLAN	Select management VLAN in option list. Management connection, such as http, https, SNMP etc, has the same VLAN of management VLAN are allow connecting to device. Others will be dropped.

11.4.2 Management Service

Click **Security** > **Management Access** > **Management Service**

This page allows user to change management services related configurations.

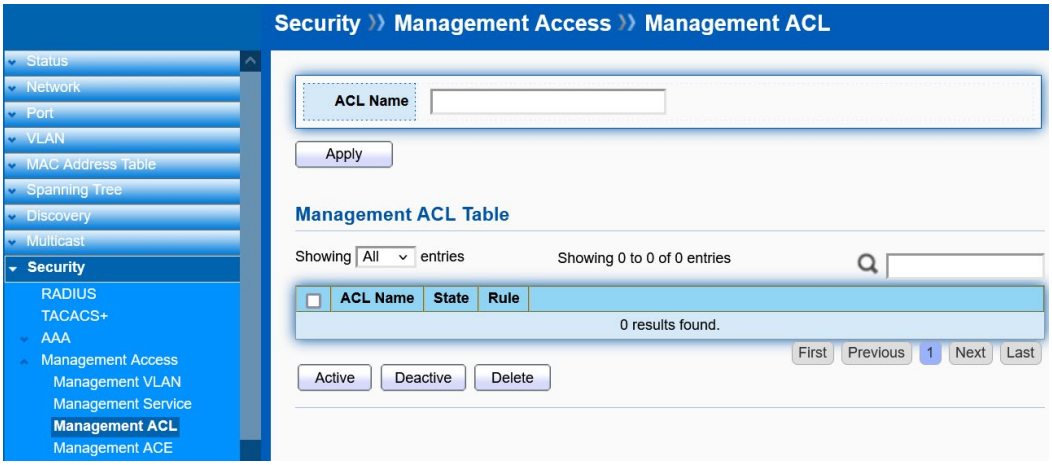


Field	Description
Management Service	Management Service admin state. **Telnet**: Connect CLI through Telnet. **SSH**: Connect CLI through SSH. **HTTP**: Connect Web UI through HTTP. **HTTPS**: Connect Web UI through HTTPS. **SNMP**: Manage switch through SNMP.
Session Timeout	Set session timeout minutes for user access to user interface. 0 minute means never timeout.
Password Retry Count	Set password retry count for user access to user interface.
Silent Time	Set silent time for user access to user interface.

11.4.3 Management ACL

Click **Security** > **Management Access** > **Management ACL**

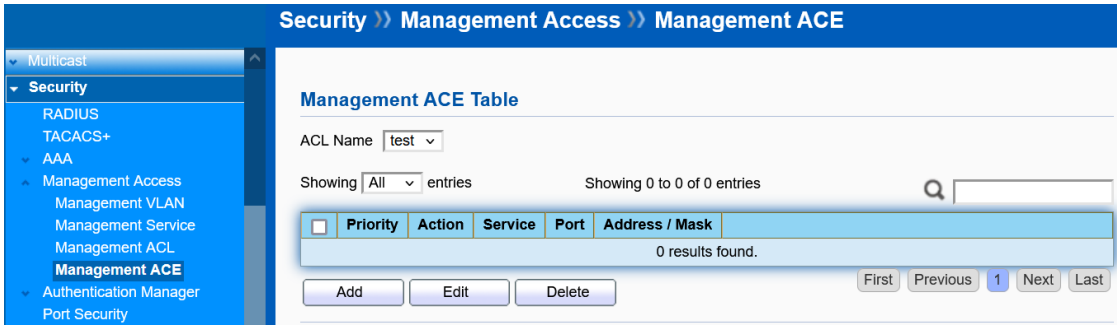
This page displays the currently-defined Management ACLs profiles. To add a new ACL, enter the name of the new ACL and click **Apply**.



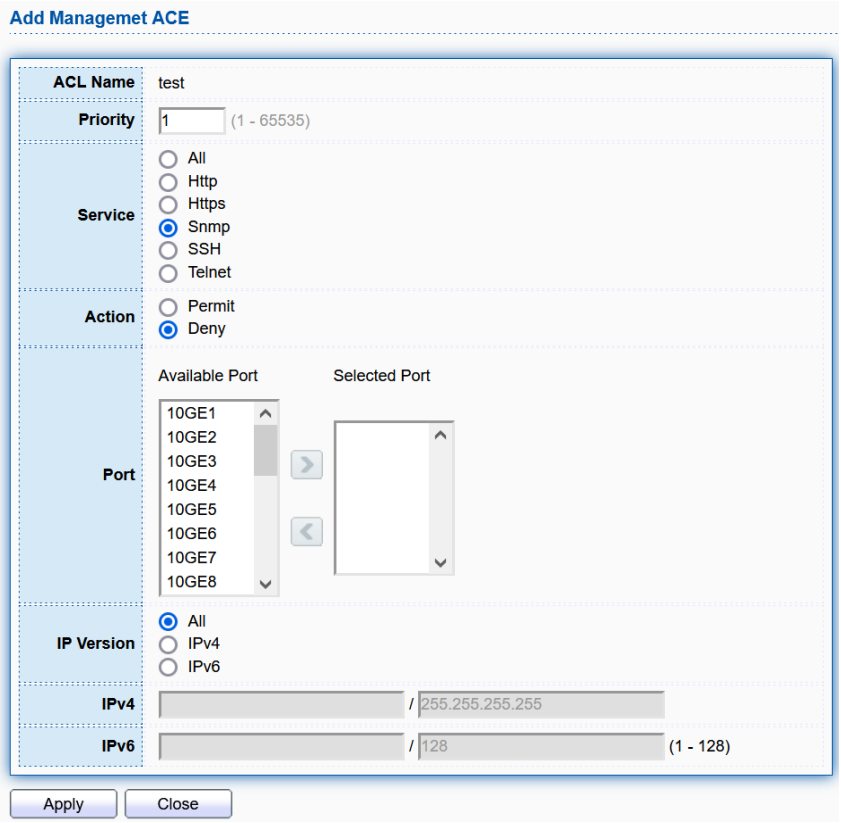
11.4.4 Management ACE

Click **Security** > **Management Access** > **Management ACE**

Use this page to view and add rules to Management ACLs



Select an **ACL Name** and click "**Add**/**Edit**" to add/edit ACE. Check and click **Delete** to delete ACEs.



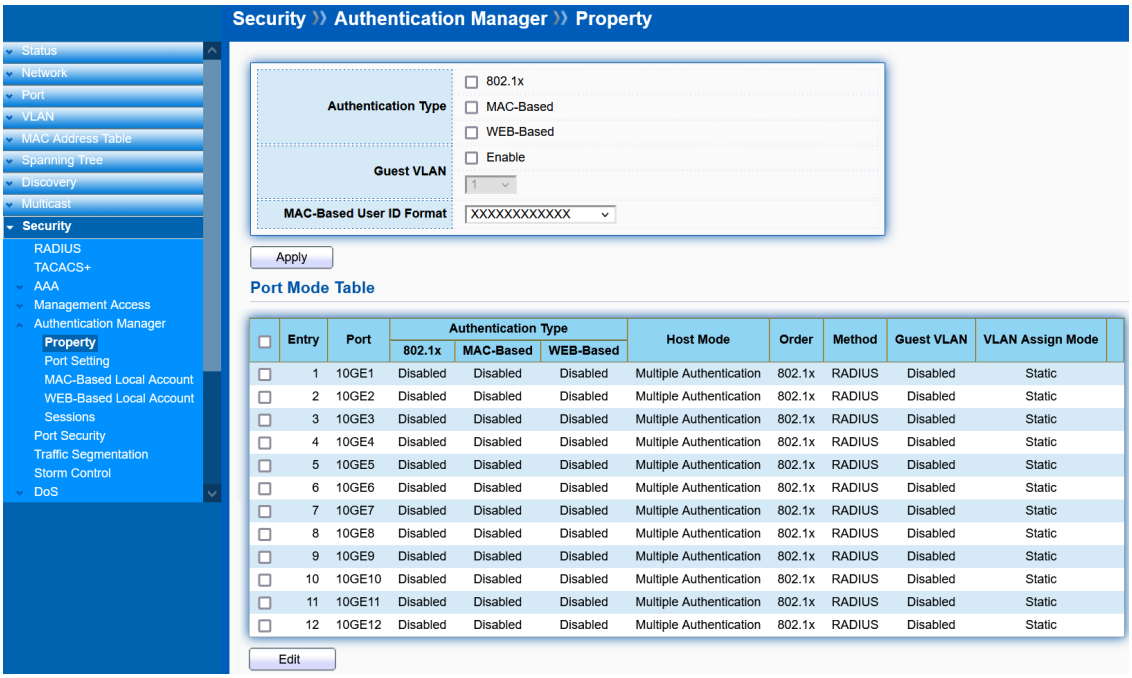
Field	Description
ACL Name	The selected ACL.
Priority	Set priority for the rule.
Service	Select service.
Action	Select the action: Permit or Deny.
Port	Select the port.
IP Version	Select the IP version.

11.5 Authentication Manager

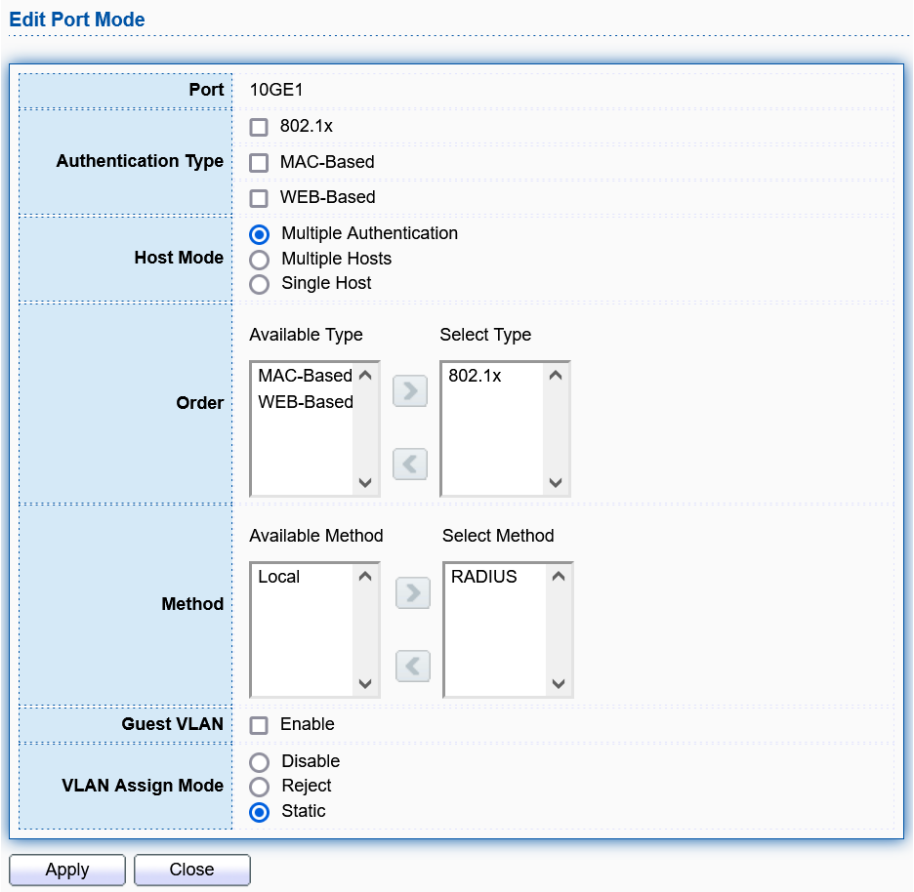
11.5.1 Property

Click **Security** > **Authentication Manager** > **Property**

This page allows user to change Authentication Type and Property.



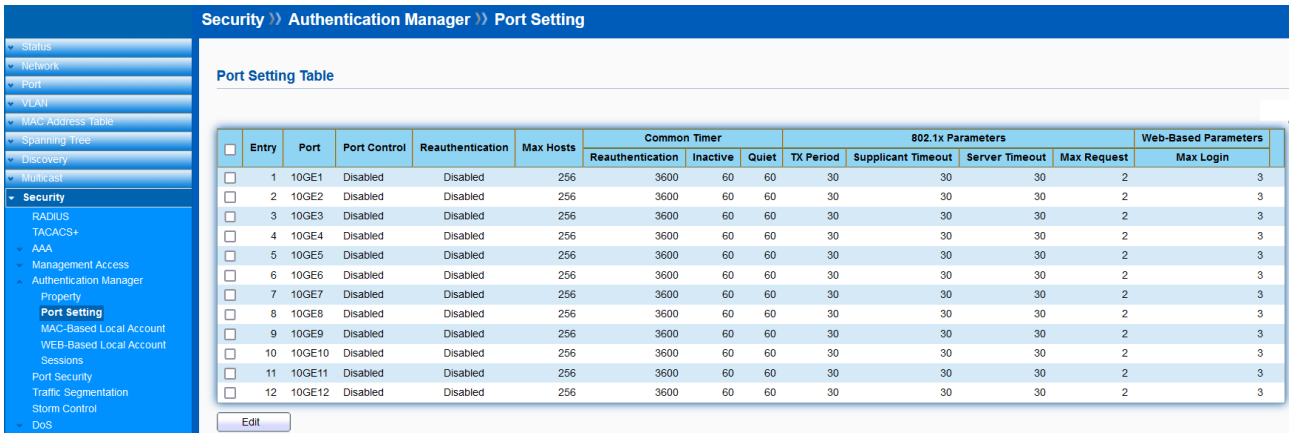
Select the ports in Port Mode Table and click “**Edit**” to edit Property.



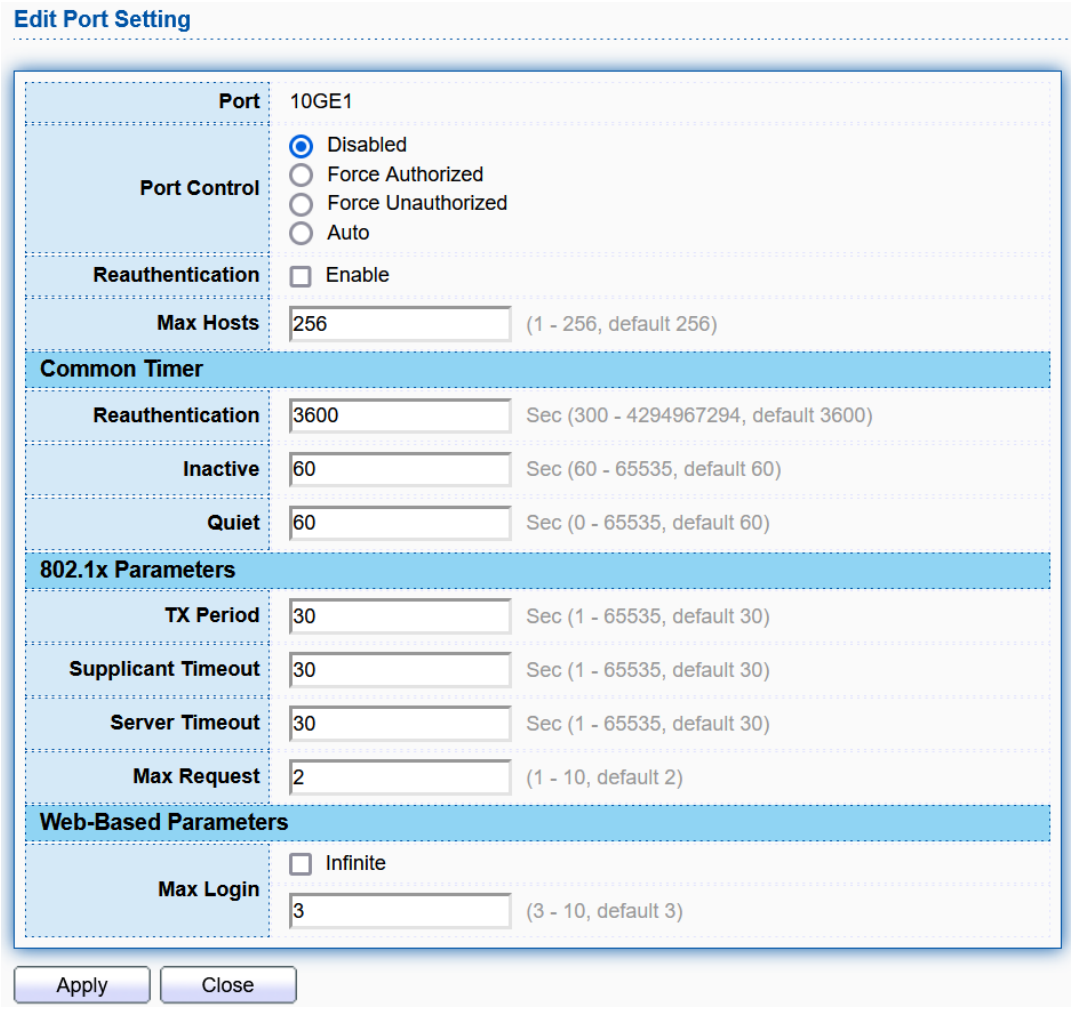
11.5.2 Port Setting

Click **Security** > **Authentication Manager** > **Port Setting**

This page allows user to change Port Setting.



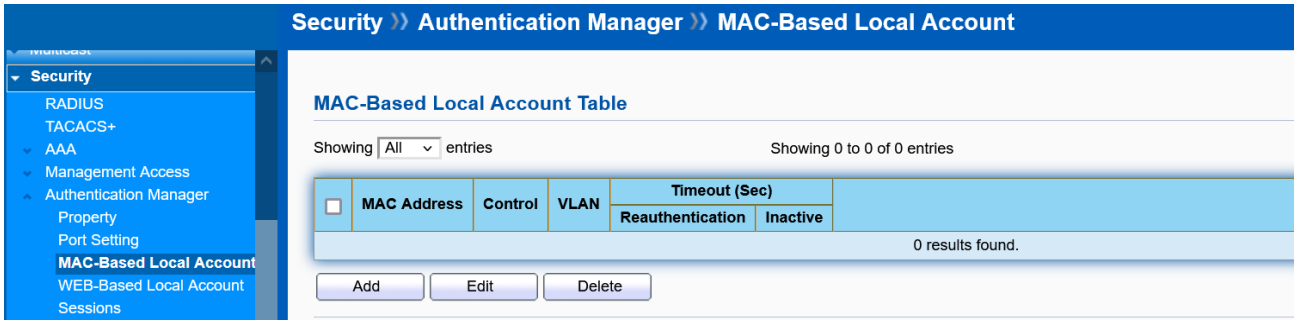
Select the ports in Port Setting Table and click “**Edit**” to edit Port Setting.



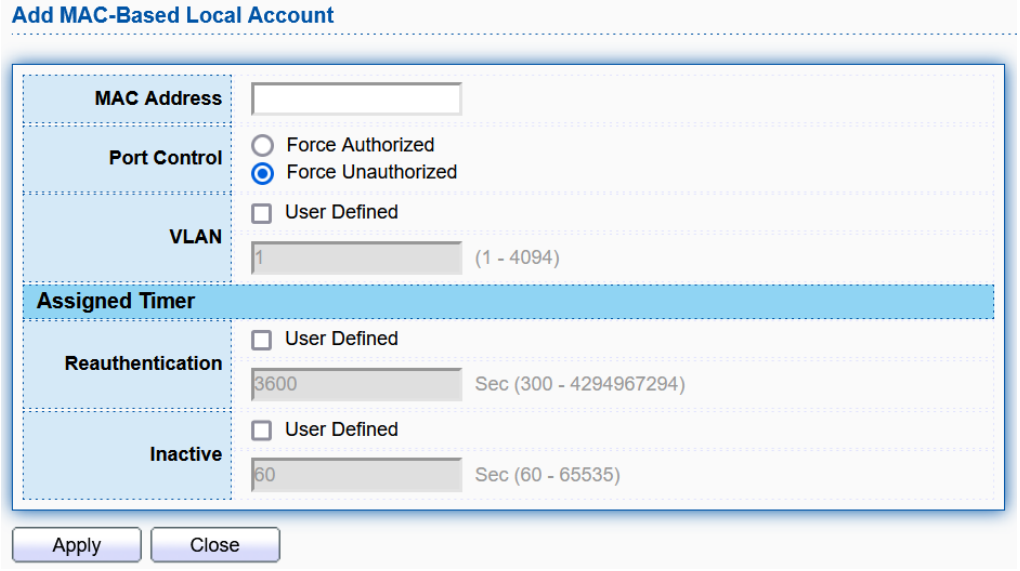
11.5.3 MAC-Based Local Account

Click **Security** > **Authentication Manager** > **MAC-Based Local Account**

This page allows user to add MAC-Based account.



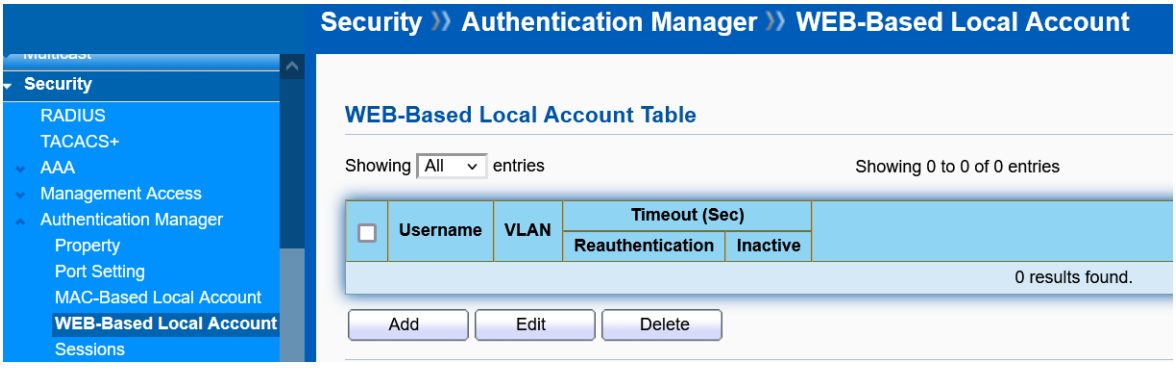
Click “**Add**” or “**Edit**” to add or edit a MAC-based account.



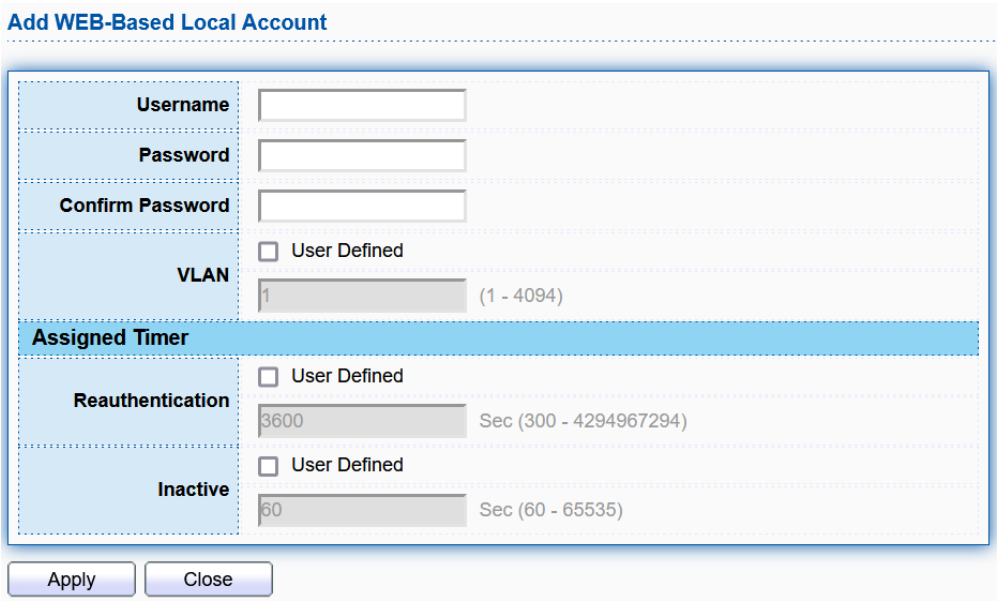
11.5.4 WEB-Based Local Account

Click **Security** > **Authentication Manager** > **WEB-Based Local Account**

This page allows user to add WEB-Based account.



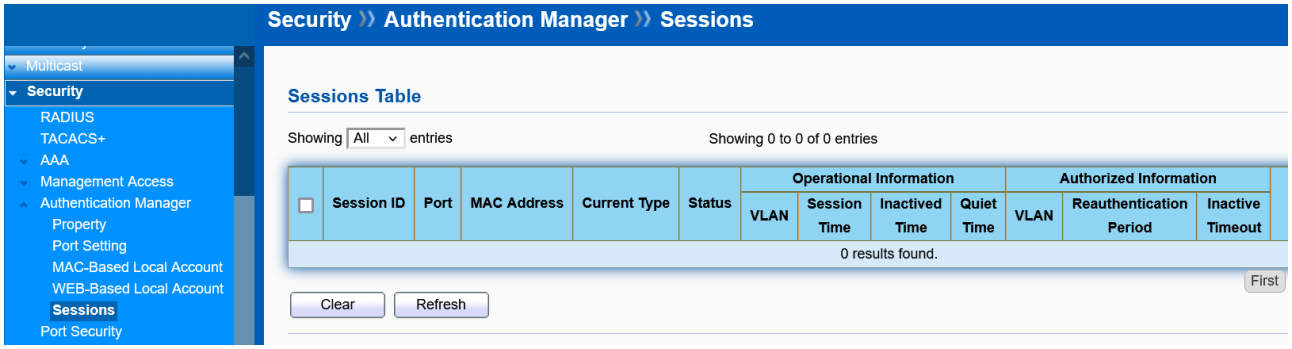
Click “**Add**” or “**Edit**” to add or edit a WEB-based account.



11.5.5 Sessions

Click **Security** > **Authentication Manager** > **Sessions**

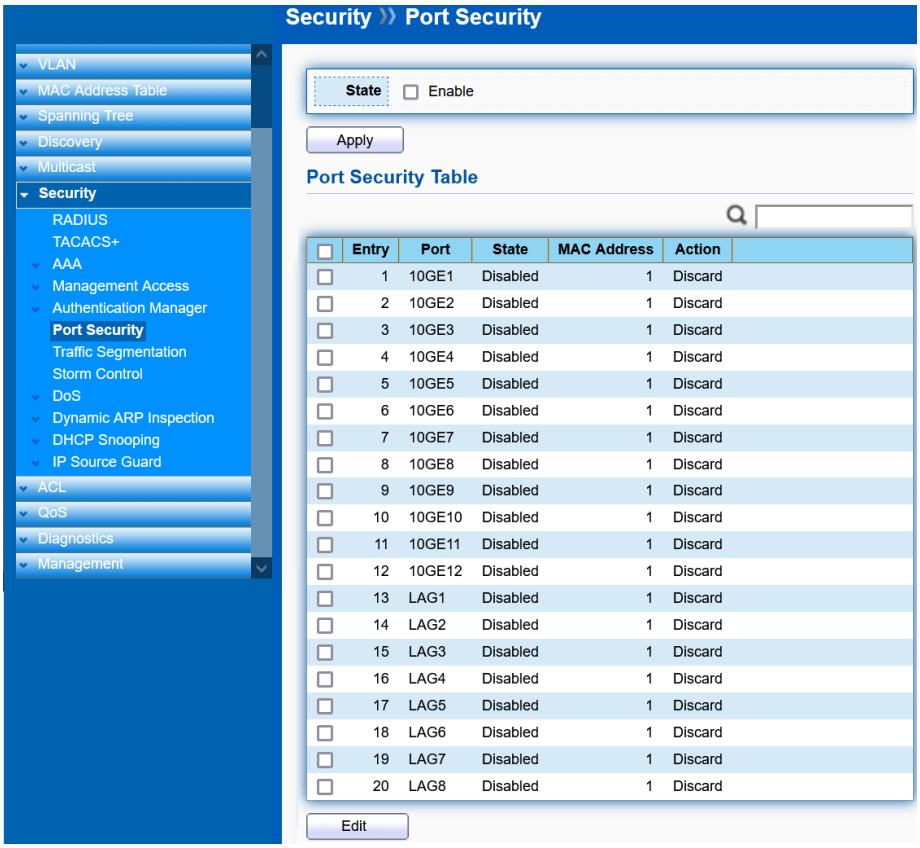
This page allows user to monitor Sessions.



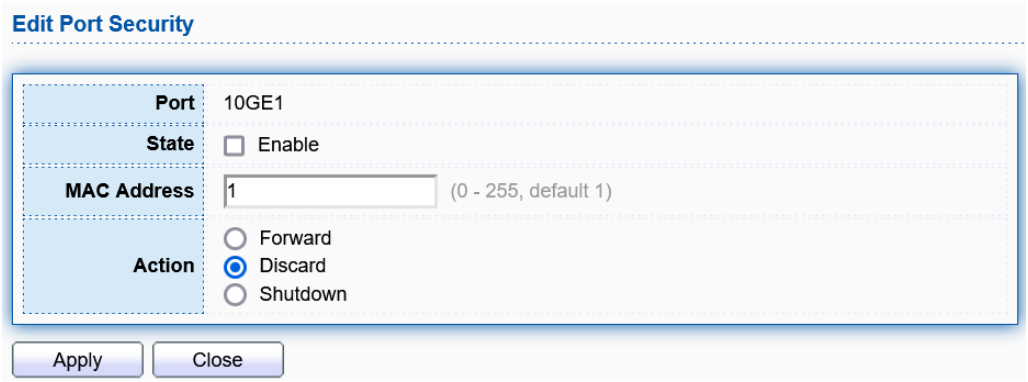
11.6 Port Security

Click **Security** > **Port Security**

Network security can be increased by limiting access on a specific port to users with specific MAC addresses. Port Security prevents unauthorized device to the Switch prior to stopping auto-learning processing.



Select port and click "**Edit**" to edit port security.

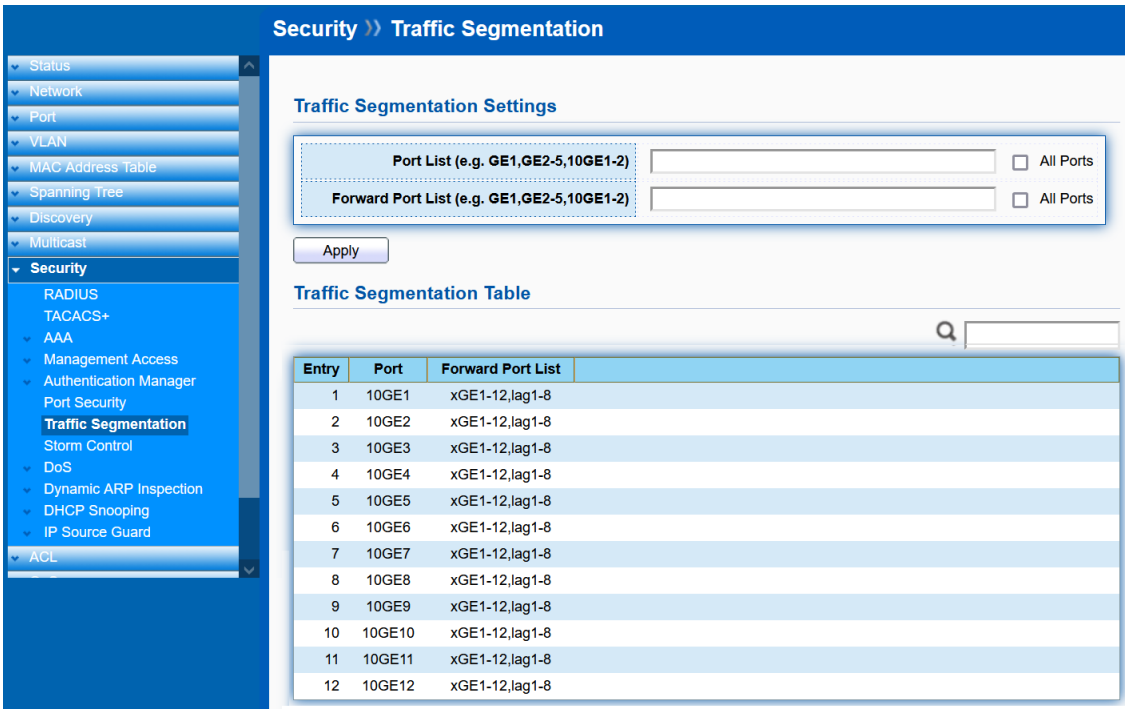


Field	Description
Port	The selected port.
State	Check to **Enable** for the port security feature for the selected port
MAC Address	Enter the maximum number of MAC Address that can be learned on the port. The range is from 0-255.
Action	Select the action: **Forward**, **Discard** or **Shutdown** when exceeded the maximum number of MAC Address.

11.7 Traffic Segmentation

Click **Security** > **Traffic Segmentation**

Traffic Segmentation prohibits ports to communicate with each other directly, on other manufacturers' switches, this function is called Protected Ports, Port Isolation, etc.

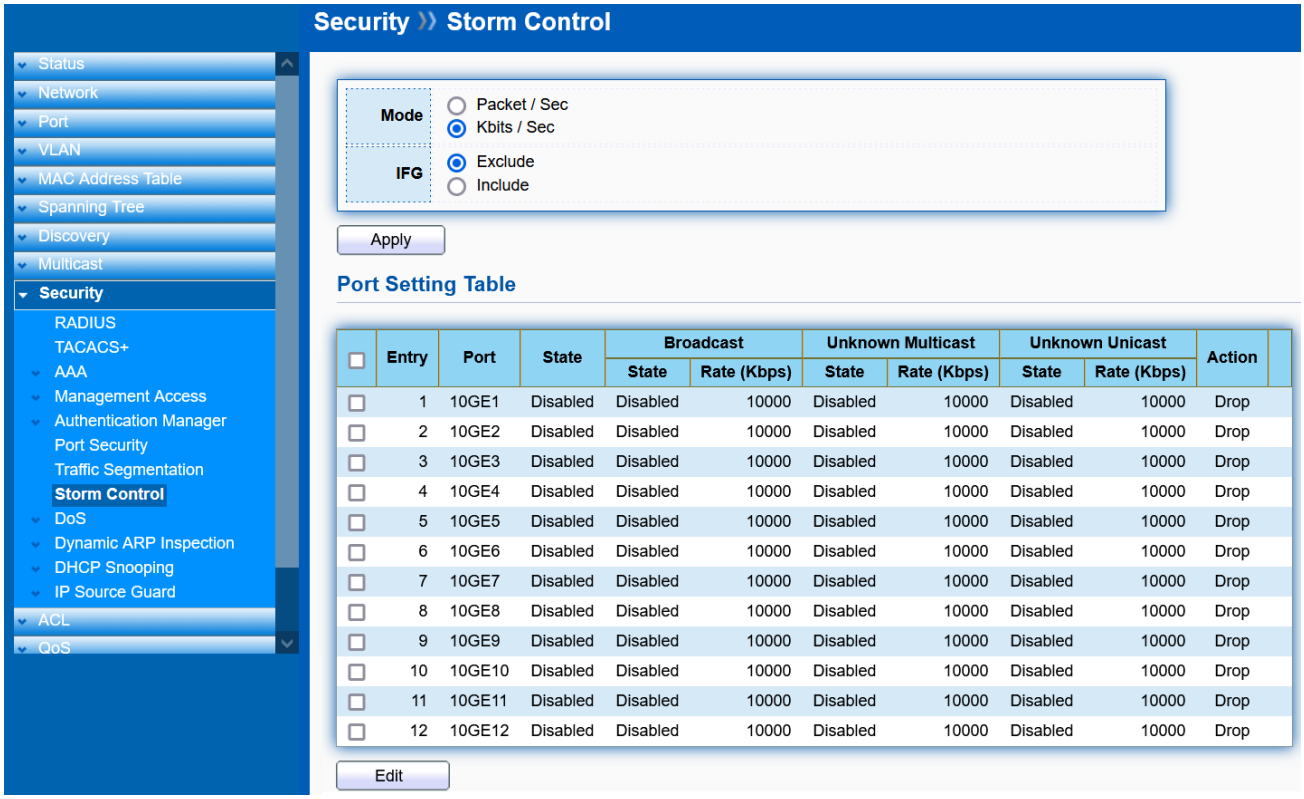


Field	Description
Port List	Enter the source port (eg. xGE1, xGE2–xGE12)
Forward Port List	Enter the forwarding ports (eg. xGE1, xGE2–xGE12, LAG1-LAG8)

11.8 Storm Control

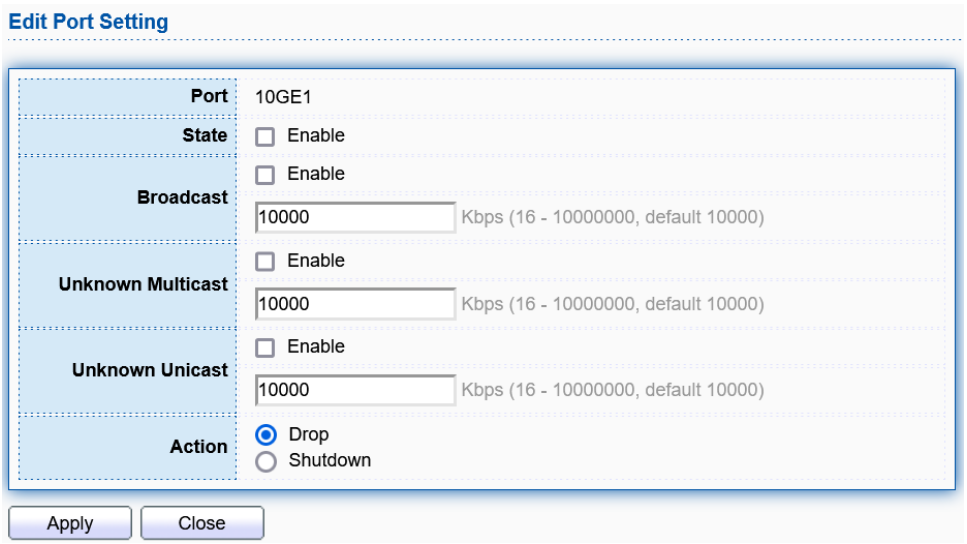
Click **Security** > **Storm Control**

To display Storm Control global setting web page.



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

Click "**Edit**" to edit the storm control port setting web page.



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

11.9 DoS

A Denial of Service (DoS) attack is a hacker attempt to make a device unavailable to its users. DoS

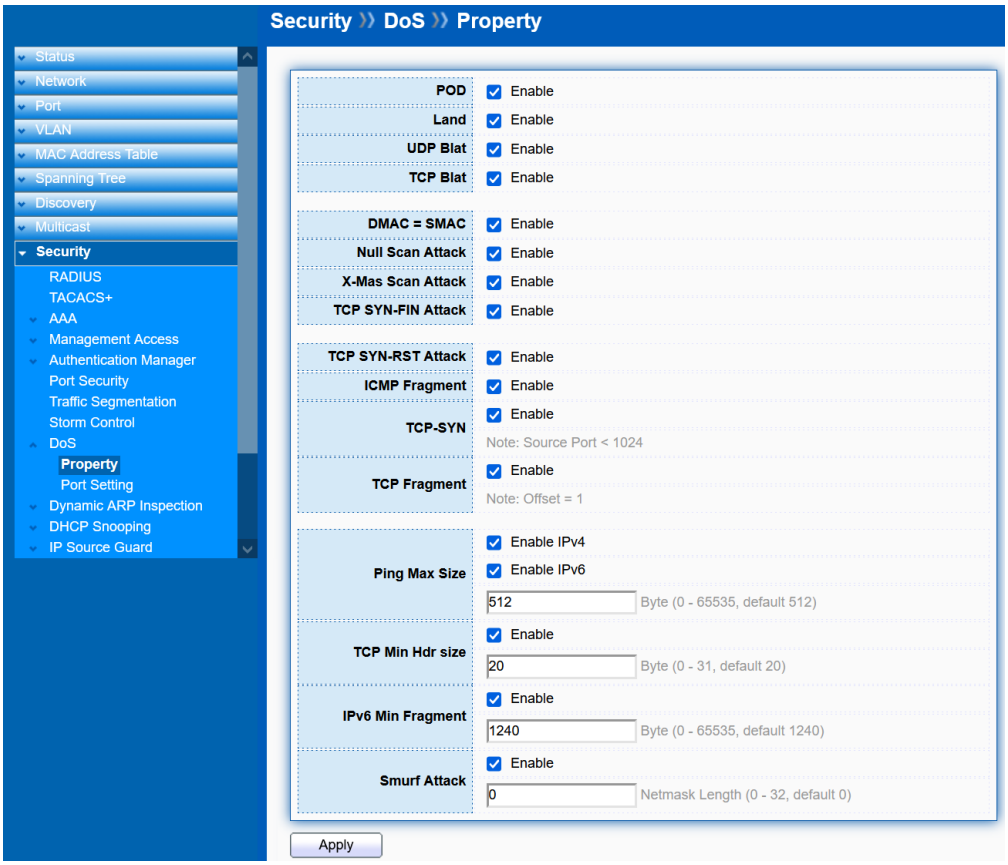
attacks saturate the device with external communication requests, so that it cannot respond to legitimate traffic. These attacks usually lead to a device CPU overload.

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

11.9.1 Property

Click **Security** > **DoS** > **Property**

To display DoS Global Setting web page.



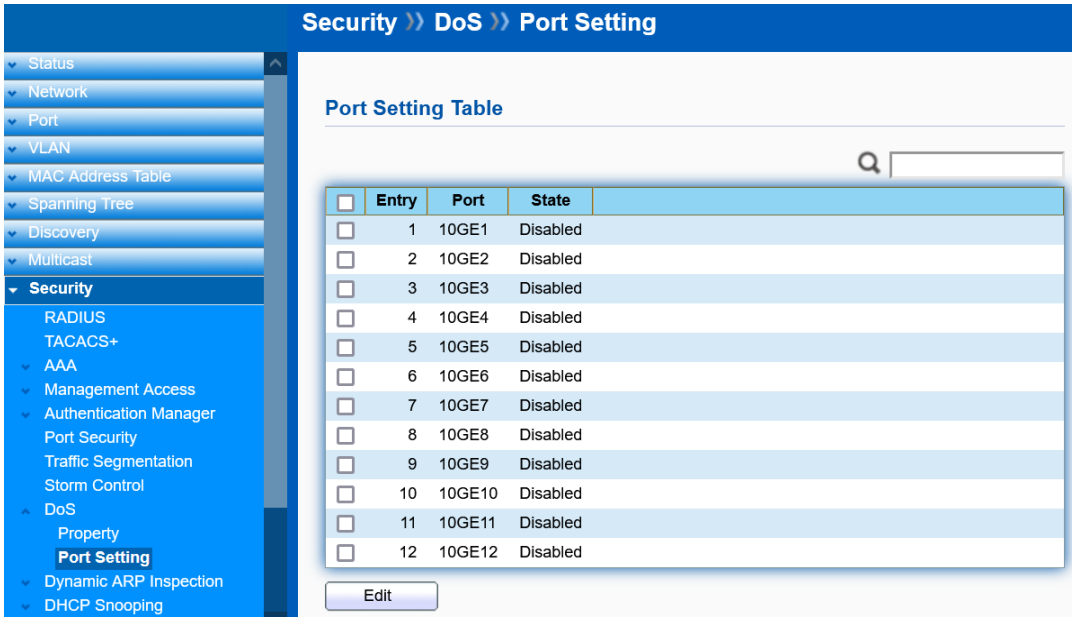
Field	Description
POD	Avoids ping of death attack.
Land	Drops the packets if the source IP address is equal to the destination IP address.
UDP Blat	Drops the packets if the UDP source port equals to the UDP destination port.
TCP Blat	Drops the packages if the TCP source port is equal to the TCP destination port.
DMAC=SMAC	Drops the packets if the destination MAC address is equal to the source MAC address.
Null Scan Attack	Drops the packets with NULL scan.
X-Mas Scan Attack	Drops the packets if the sequence number is zero, and the FIN, URG and PSH bits are set.
TCP SYN-FIN Attack	Drops the packets with SYN and FIN bits set.
TCP SYN-RST Attack	Drops the packets with SYN and RST bits set.
ICMP Fragment	Drops the fragmented ICMP packets.

TCP-SYN(SPORT <1024)	Drops SYN packets with sport less than 1024.
TCP Fragment (Offset=1)	Drops the TCP fragment packets with offset equals to one.
Ping Max Size	Specify the maximum size of the ICMPv4/ICMPv6 ping packets. The valid range is from 0 to 65535 bytes, and the default value is 512 bytes.
IPv4 Ping Max Size	Checks the maximum size of ICMP ping packets, and drops the packets larger than the maximum packet size.
IPv6 Ping Max Size	Checks the maximum size of ICMPv6 ping packets, and drops the packets larger than the maximum packet size
TCP Min Hdr Size	Checks the minimum TCP header and drops the TCP packets with the header smaller than the minimum size. The length range is from 0 to 31 bytes, and default length is 20 bytes.
IPv6 Min Fragment	Checks the minimum size of IPv6 fragments, and drops the packets smaller than the minimum size. The valid range is from 0 to 65535 bytes, and default value is 1240 bytes.
Smurf Attack	Avoid smurf attack. The length range of the netmask is from 0 to 323 bytes, and default length is 0 bytes.

11.9.2 Port Setting

Click **Security** > **DoS** > **Port Setting**

To configure and display the state of DoS protection for interfaces.



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

11.10 Dynamic ARP Inspection

Dynamic ARP inspection (DAI) protects switching devices against ARP spoofing.

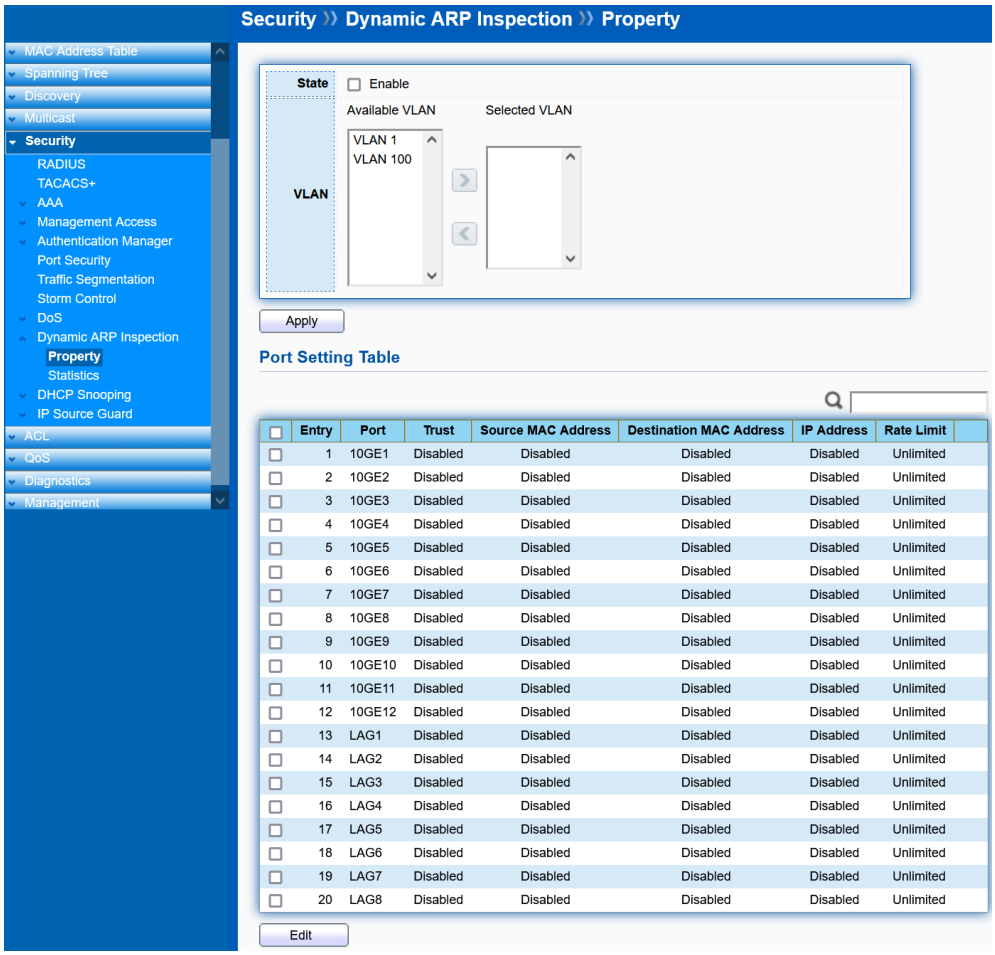
DAI inspects Address Resolution Protocol (ARP) packets on the LAN and uses the information in the DHCP snooping database on the switch to validate ARP packets and to protect against ARP

spoofing (also known as ARP poisoning or ARP cache poisoning). ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made based on the results of those comparisons. When an attacker tries to use a forged ARP packet to spoof an address, the switch compares the address with entries in the database. If the MAC address or IP address in the ARP packet does not match a valid entry in the DHCP snooping database, the packet is dropped.

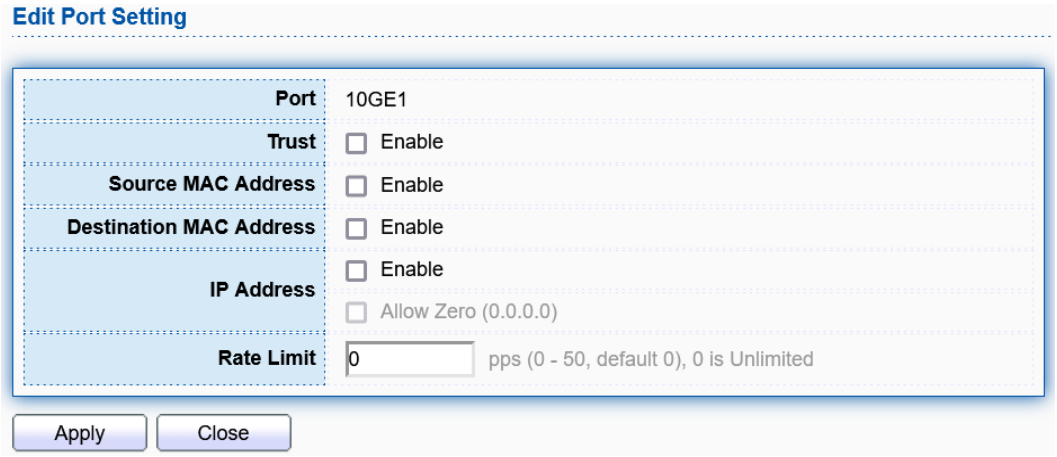
11.10.1 Property

Click **Security** > **Dynamic ARP Inspection** > **Property**

To configure and display the state of Dynamic ARP Inspection for interfaces.



Select port and click “**Edit**” to edit DAI for that port.

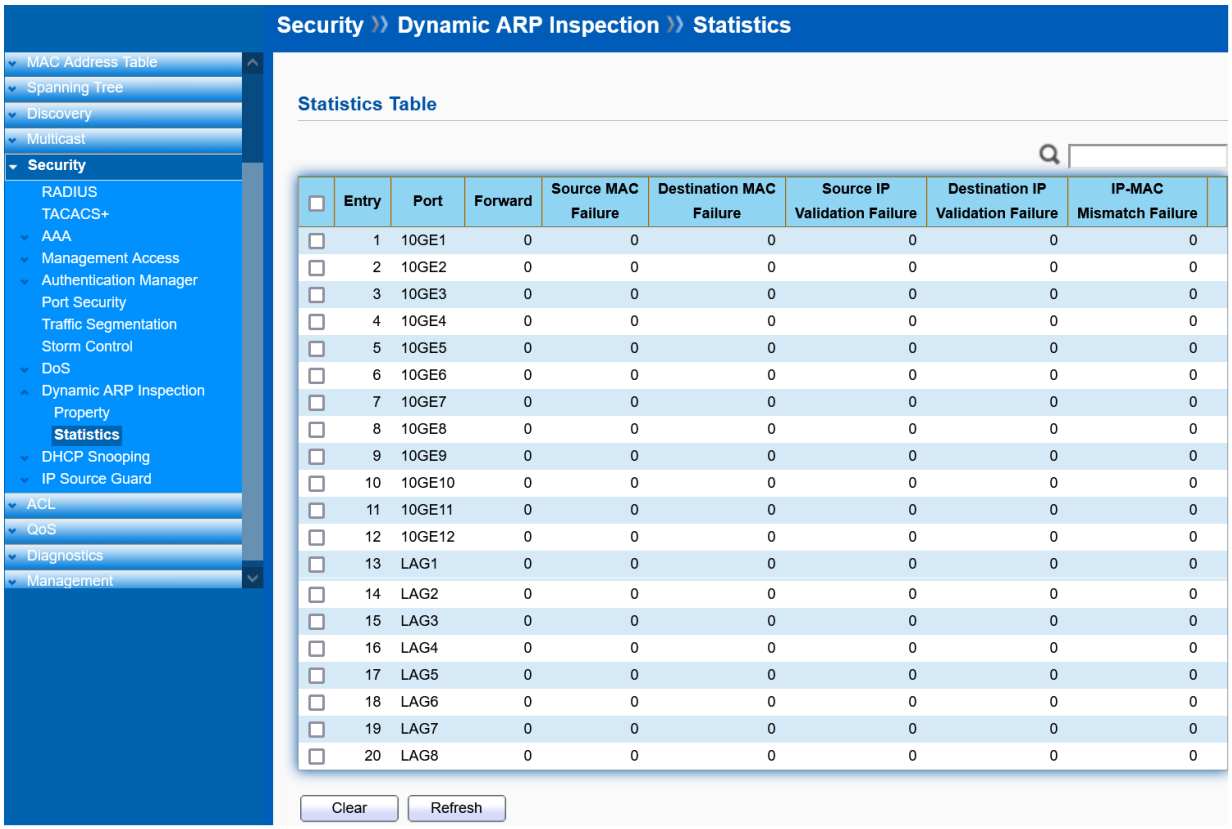


Field	Description
Port	The selected port.
Trust	Check to set the port to **Trust** state. DAI associates a trust state with each interface on the switch. Packets arriving on trusted interfaces bypass all DAI validation checks, and those arriving on untrusted interfaces undergo the DAI validation process.
Source MAC Address	Check this option; DAI will check Source MAC Address.
Destination MAC Address	Check this option; DAI will check Destination MAC Address.
IP Address	Check this option; DAI will check IP Address. And if check Allow Zero, DAI will allow 0.0.0.0 IP address to pass through.
Rate Limit	Set the rate limit on untrusted interfaces. The rate is unlimited on all trusted interfaces.

11.10.2 Statistics

Click **Security** > **Dynamic ARP Inspection** > **Statistics**

To display the statistics of Dynamic ARP Inspection.



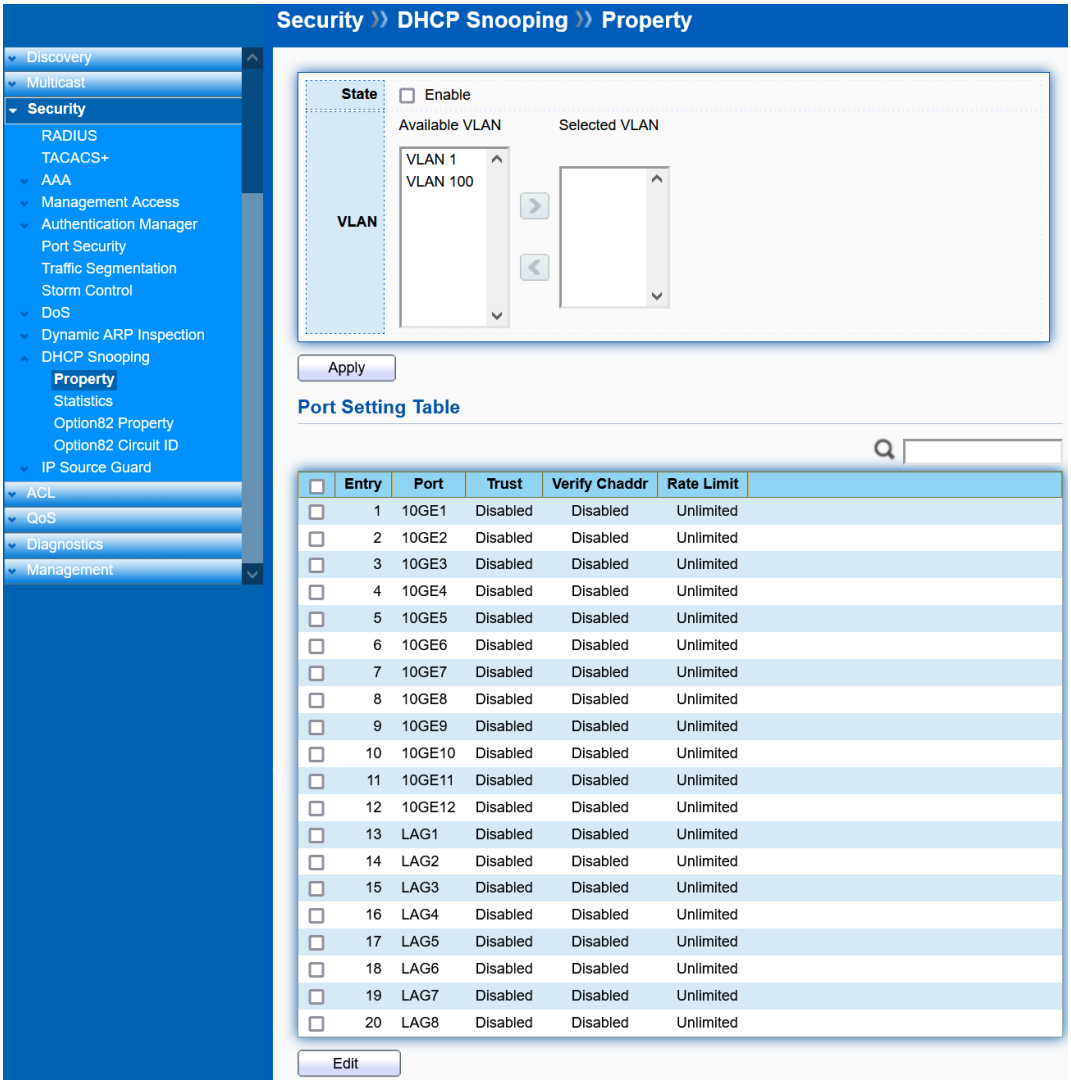
11.11 DHCP Snooping

You can use DHCP snooping to help avoid the Denial of Service attacks that result from unauthorized users adding a DHCP server to the network that then provides invalid configuration data to other DHCP clients on the network. DHCP snooping accomplishes this by allowing you to distinguish between trusted ports connected to a DHCP server or switch and untrusted ports connected to end-users. DHCP packets are forwarded between trusted ports without inspection. DHCP packets received on other switch ports are inspected before being forwarded. Packets from untrusted sources are dropped.

11.11.1 Property

Click **Security** > **DHCP Snooping** > **Property**

To configure and display the state of DHCP Snooping for interfaces.



Select port and click "**Edit**" to edit DHCP Snooping for that port.

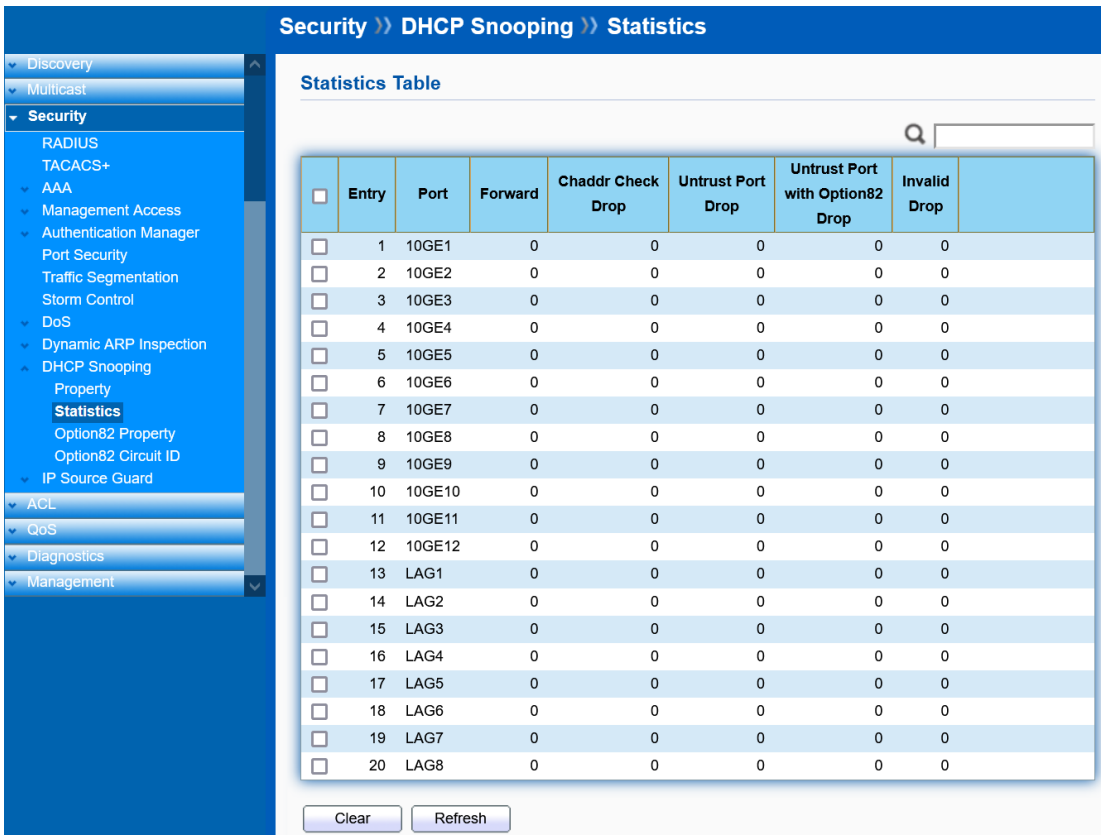
Field	Description
Port	The selected port.
Trust	Check to set the port to **Trust** state. The DHCP snooping feature determines whether traffic sources are trusted or untrusted. An untrusted source may initiate traffic attacks or other hostile actions. To prevent such attacks, the DHCP snooping feature filters messages and rate-limits traffic from untrusted sources.
Verify Chaddr	Check to enable **Verify Chaddr**. DHCP snooping drops DHCP packets received on untrusted ports when the check address (chaddr) field in the DHCP header does not match the source MAC address of the packet.

Rate Limit	Set the rate limit on untrusted interfaces. The rate is unlimited on all trusted interfaces.

11.11.2 Statistics

Click **Security** > **DHCP Snooping** > **Statistics**

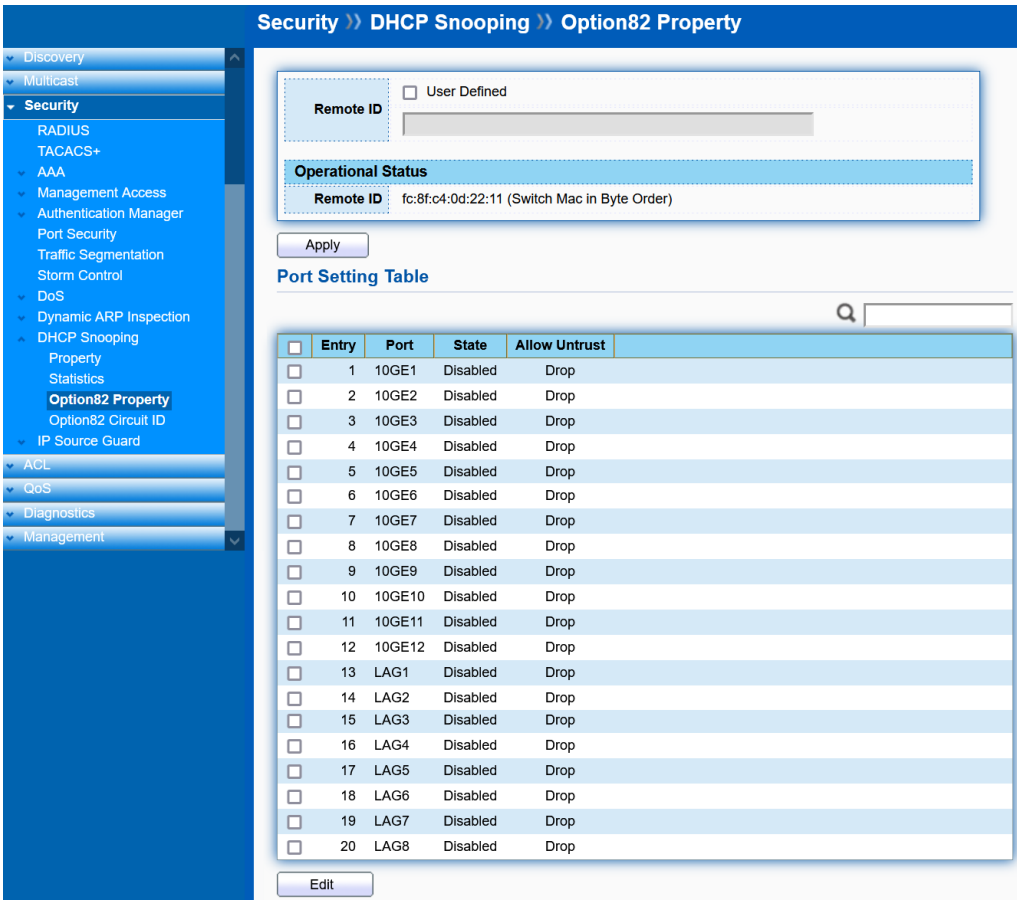
To display the statistics of DHCP Snooping.



11.11.3 Option82 Property

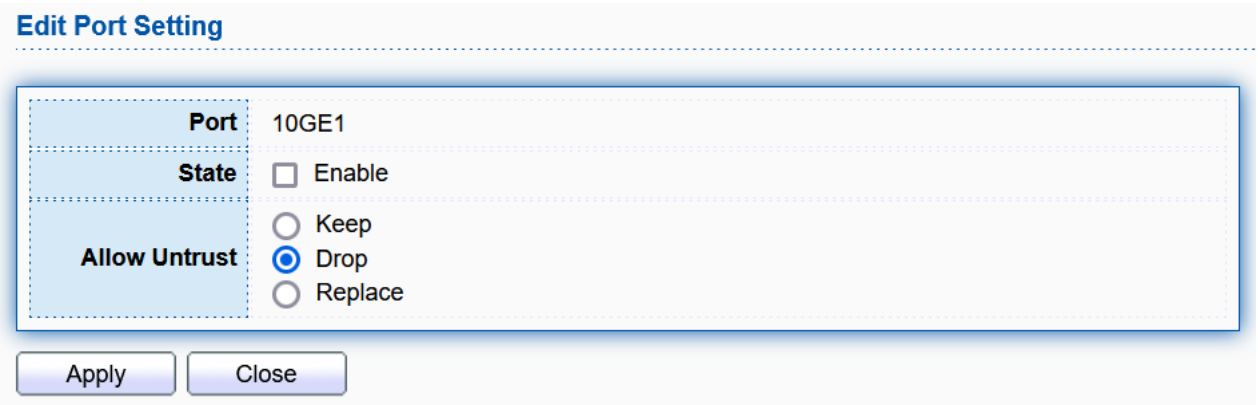
Click **Security** > **DHCP Snooping** > **Option82 Property**

To configure and display Option82 property.



Field	Description
Remote ID	Used for defining the MAC address of the switch that added the Option 82 information.

Select port and click "**Edit**" to edit Option82 property for that port.

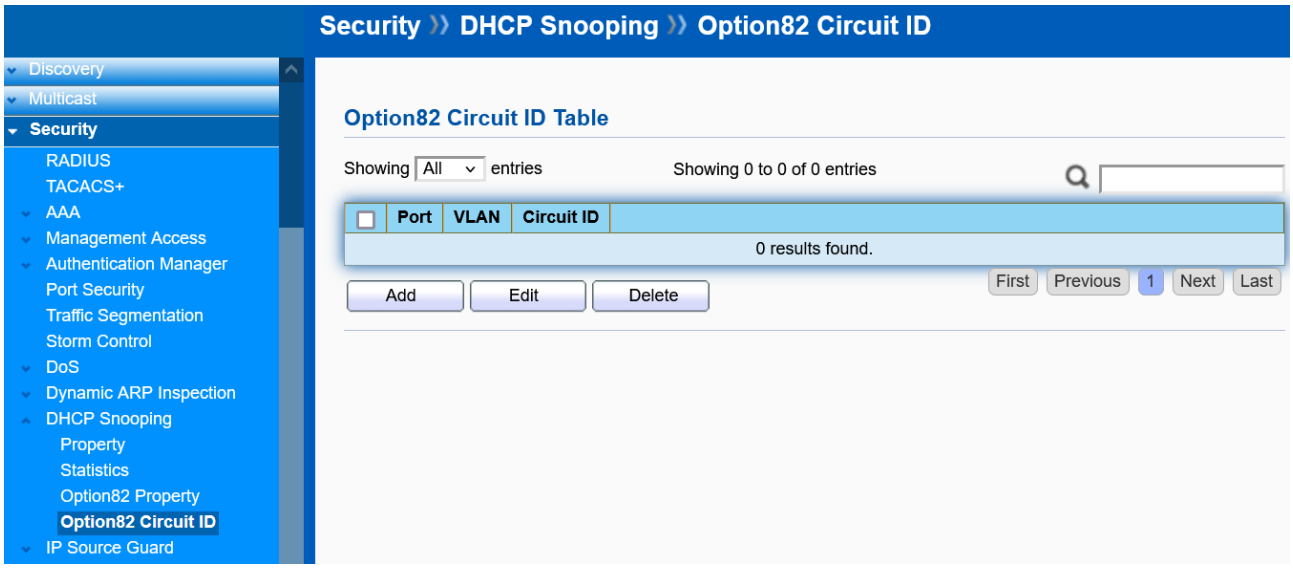


Field	Description
Port	The selected port.
State	Check to set the port to **Trust** state.
Allow Untrust	Configures DHCP snooping behavior when forwarding a DHCP packet from an untrusted port that already contains DHCP relay information (Option 82). **Keep**: The packet is forwarded without replacing the option information. **Drop**: The packet is dropped. **Replace**: The existing option is replaced with a new Option 82 generated by the switch.

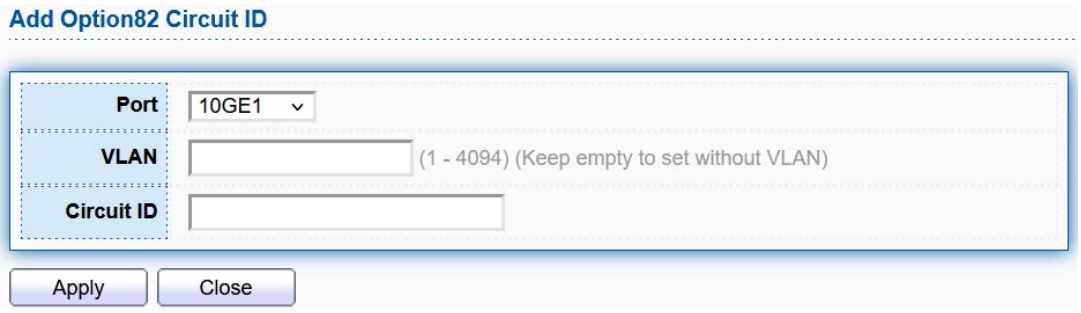
11.11.4 Option82 Circuit ID

Click **Security** > **DHCP Snooping** > **Option82 Circuit ID**

To configure and display Option82 Circuit ID.



Click "**Add**" or "**Edit**" to add or edit an Option82 Circuit ID.



Field	Description
Port	Select the port to add Circuit ID.
VLAN	Specify the VLAN ID.
Circuit ID	Used for defining the switch port and VLAN number of the port user(s)

11.12 IP Source Guard

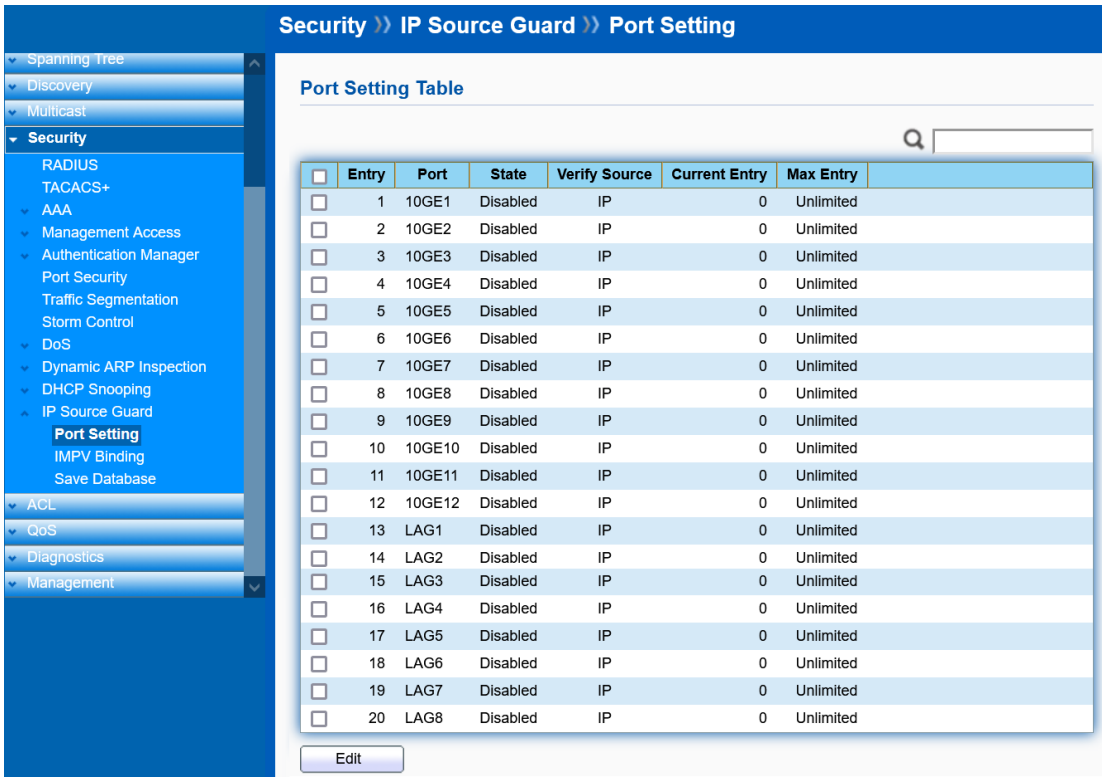
IP Source Guard is a security feature that restricts IP traffic on untrusted Layer 2 ports by filtering traffic based on the DHCP snooping binding database or manually configured IP source bindings. This feature helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host. Any IP traffic coming into the interface with a source IP address other than that assigned (via DHCP or static configuration) will be filtered out on the untrusted Layer 2 ports.

The IP Source Guard feature is enabled in combination with the DHCP snooping feature on untrusted Layer 2 interfaces. It builds and maintains an IP source binding table that is learned by DHCP snooping or manually configured (static IP source bindings). An entry in the IP source binding table contains the IP address and the associated MAC and VLAN numbers. The IP Source Guard is

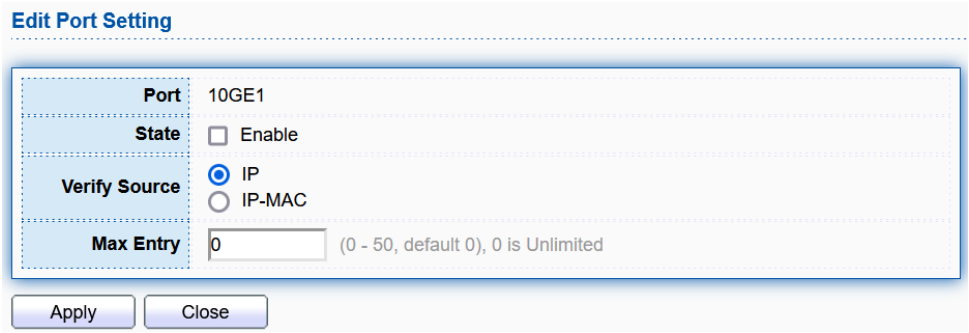
supported on Layer 2 ports only, including access and trunk ports.

11.12.1 Port Setting

Click **Security** > **IP Source Guard** > **Port Setting**



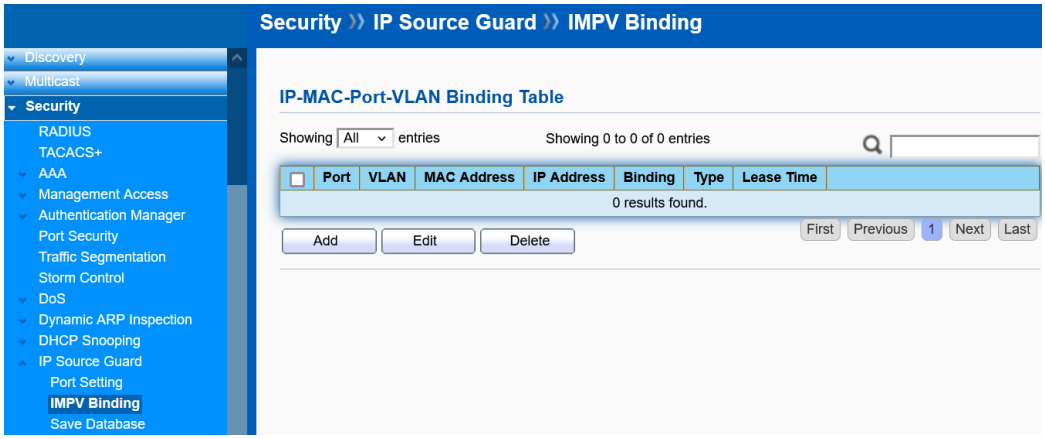
Check the port and click "**Edit**" to edit IP Source Guard for that port.



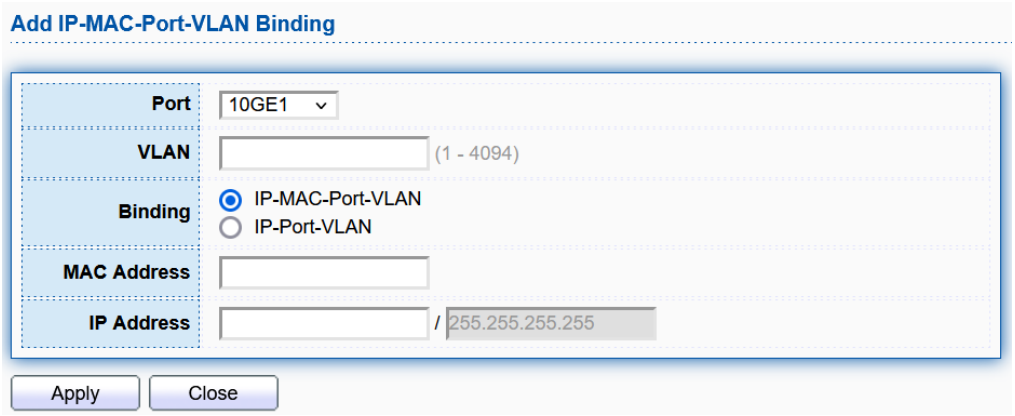
Field	Description
Port	Selected port.
State	Check to Enable IP Source Guard.
Verify Source	Select method: **IP** or **IP-MAC**.
Max Entry	Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0-50 (0 means unlimited).

11.12.2 IMPV Binding

Click **Security** > **IP Source Guard** > **IMPV Binding**



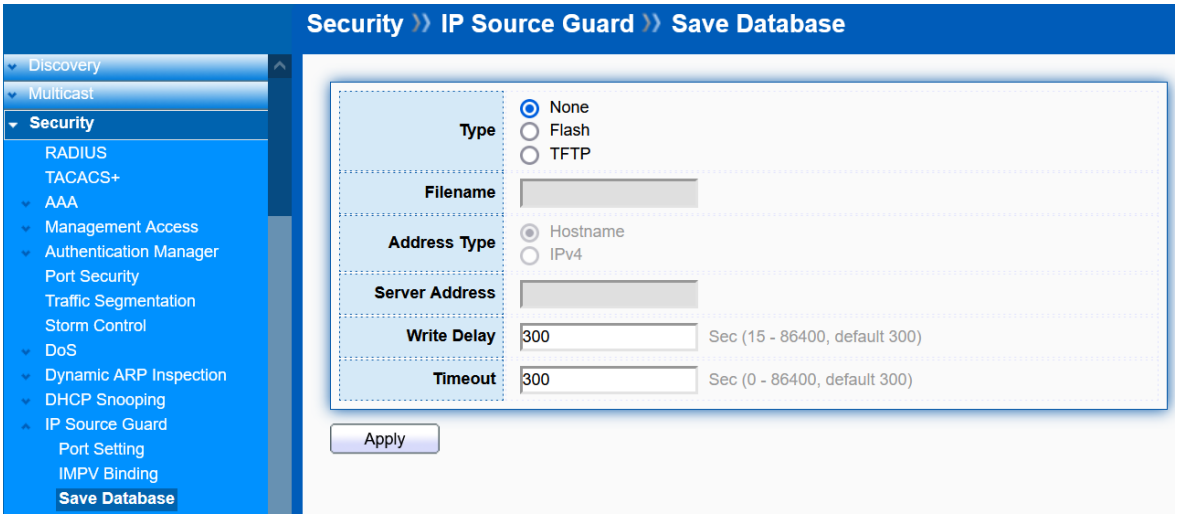
Click “**Add**” or “**Edit**” to add or edit a Binding rule.



Field	Description
Port	Select the port.
VLAN	The VLAN ID for the settings.
Binding	Select the binding method: **IP-MAC-Port-VLAN** or **IP-Port-VLAN**.
MAC Address	Allowed Source MAC address.
IP Address	Allowed Source IP address.

11.12.3 Save Database

Click **Security** > **IP Source Guard** > **Save Database**



Field	Description
Type	Select type: None, Flash or TFTP.
Filename	Enter the filename to save database If using TFTP method.
Address Type	Enter the address type to save database If using TFTP method.
Server Address	Enter the server address to save database If using TFTP method.
Write Delay	Specify the write delay time.
Timeout	Specify the timeout.

Chapter 12 ACL

An Access Control List (ACL) allows you to define classification rules or establish criteria to provide security to your network by blocking unauthorized users and allowing authorized users to access specific areas or resources. ACLs can provide basic security for access to the network by controlling whether packets are forwarded or blocked at the Switch ports. Access Control Lists (ACLs) are filters that allow you to classify data packets according to a particular content in the packet header, such as the source address, destination address, source port number, destination port number, and more. Packet classifiers identify flows for more efficient processing.

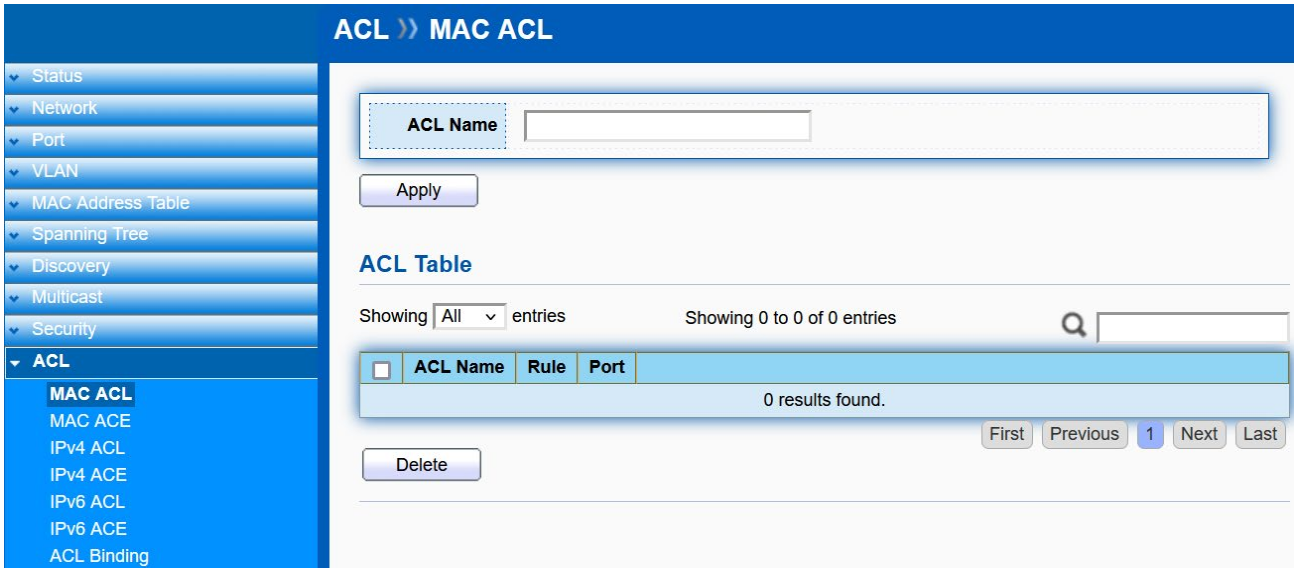
Each filter defines the conditions that must match for inclusion in the filter. ACLs (Access Control Lists) provide packet filtering for IP frames (based on the protocol, TCP/UDP port number or frame type) or layer 2 frames (based on any destination MAC address for unicast, broadcast, or multicast, or based on VLAN ID or VLAN tag priority). ACLs can be used to improve performance by blocking unnecessary network traffic or to implement security controls by restricting access to specific network resources or protocols.

Policies can be used to differentiate service for client ports, server ports, network ports, or guest ports. They can also be used to strictly control network traffic by only allowing incoming frames that match the source MAC and source IP address on a specific port. ACLs are composed of Access Control Entries (ACEs), which are rules that determine traffic classifications. Each ACE is a considered as a single rule, and up to 512 rules may be defined on ACLs. ACLs are used to provide traffic flow control, restrict contents of routing updates, and determine which types of traffic are forwarded or blocked. This criterion can be specified on a basis of the MAC address or IP address.

12.1 MAC ACL

Click **ACL** > **MAC ACL**

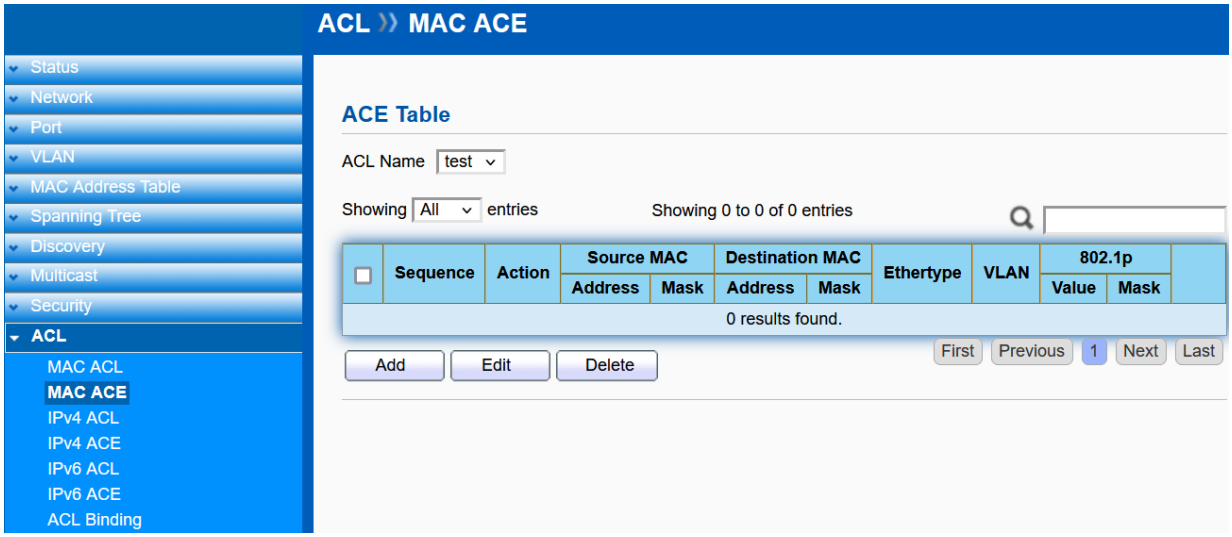
This page displays the currently-defined MAC-based ACLs profiles. To add a new ACL, enter the name of the new ACL and click **Apply**.



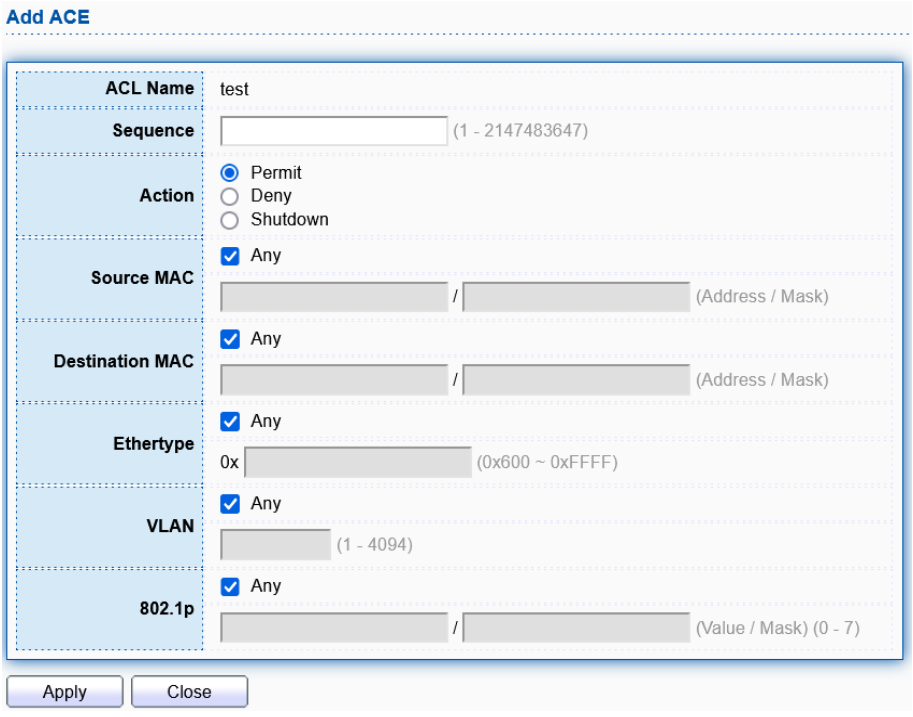
12.2 MAC ACE

Click **ACL** > **MAC ACE**

Use this page to view and add rules to MAC-based ACLs



Select an **ACL Name** and click "**Add**/**Edit**" to add/edit ACE. Check and click **Delete** to delete ACEs.



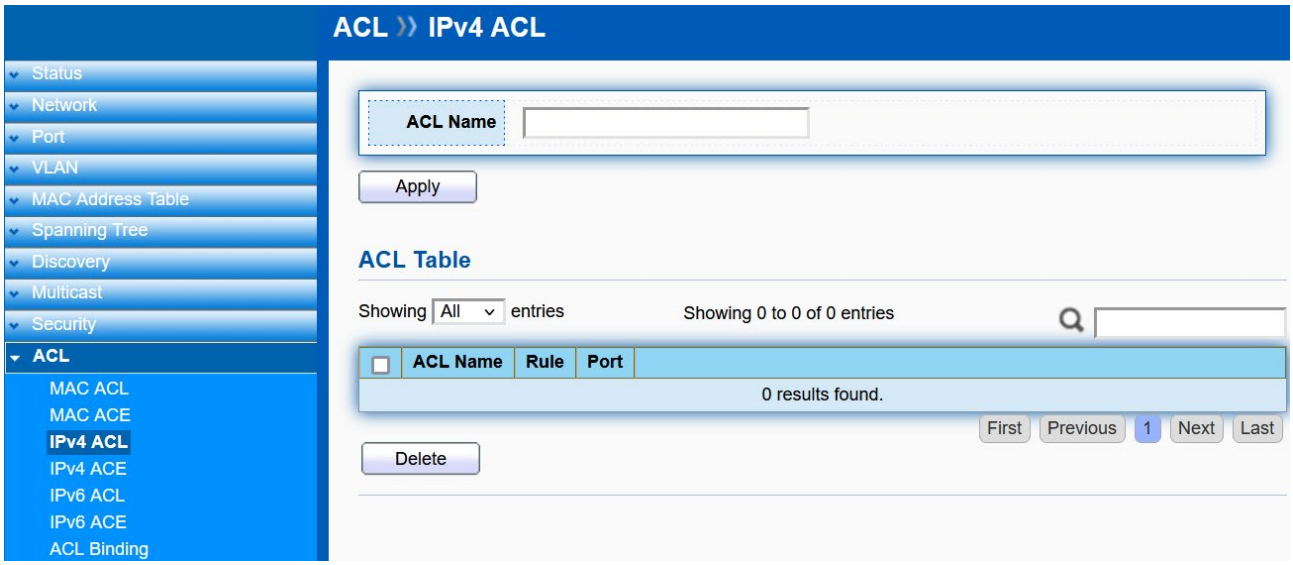
Field	Description
ACL Name	The ACL name
Sequence	Enter the sequence number which signifies the order of the specified ACL relative to other ACLs assigned to the selected interface. The valid range is from 1-2147483647, 1 being processed first.
Action	Select what action taken if a packet matches the criteria.

	•Permit – Forward packets that meet the ACL criteria. •Deny – Drops packets that meet the ACL criteria. •Shutdown – Shutdown the port that meet the ACL criteria.
Source MAC	Enter a MAC address mask for the source MAC address. A mask of 00:00:00:00:00:00 means the bits must be matched exactly; ff:ff:ff:ff:ff:ff means the bits are irrelevant. Any combination of 0s and ffs can be used.
Destination MAC	Enter a MAC address mask for the destination MAC address. A mask of 00:00:00:00:00:00 means the bits must be matched exactly; ff:ff:ff:ff:ff:ff means the bits are irrelevant. Any combination of 0s and ffs can be used.
Ethertype	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header. This option can only be used to filter Ethernet II formatted packets. A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), and 8137 (IPX).
VLAN	Enter the VLAN ID to which the MAC address is attached in MAC ACE. The range is from 1-4094.
802.1p	Enter the 802.1p value. The range is from 0-7.

12.3 IPv4 ACL

Click **ACL** > **IPv4 ACL**

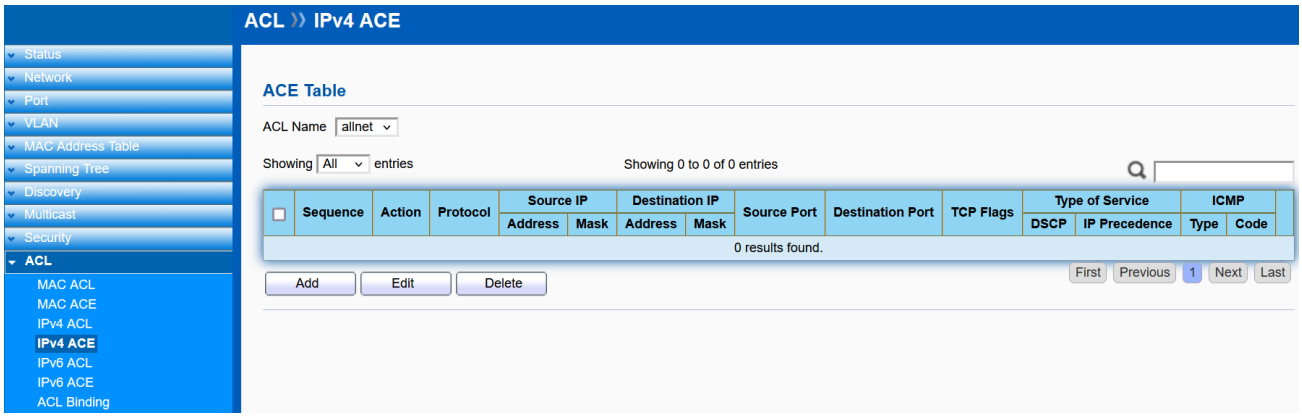
This page displays the currently-defined IPv4-based ACLs profiles. To add a new ACL, enter the name of the new ACL and click **Apply**.



12.4 IPv4 ACE

Click **ACL** > **IPv4 ACE**

Use this page to view and add rules to IPv4-based ACLs.



Select an **ACL Name** and click “**Add**/**Edit**” to add/edit ACE. Check and click **Delete** to delete ACEs.

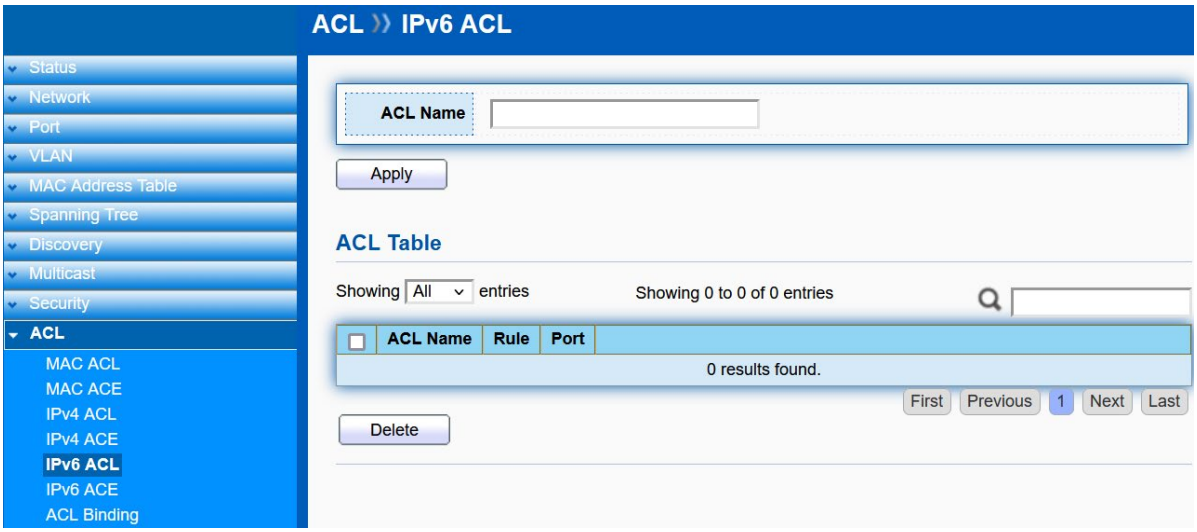
Field	Description
ACL Name	The ACL name
Sequence	Enter the sequence number which signifies the order of the specified ACL relative to other ACLs assigned to the selected interface. The valid range is from 1-2147483647, 1 being processed first.
Action	Select what action taken if a packet matches the criteria. •**Permit** – Forward packets that meet the ACL criteria. •**Deny** – Drops packets that meet the ACL criteria. •**Shutdown** – Shutdown the port that meet the ACL criteria.
Protocol	Select Any, Define, or from the list in the drop down menu. •**Any** – Check **Any** to use any protocol. •**Define** – Enter the protocol in the ACE to which the packet is matched.

	•**ICMP** – Internet Control Message Protocol (ICMP). The ICMP enables the gateway or destination host to communicate with the source host. •**IP in IP** – Encapsulates IP packets to create tunnels between two routers. This ensures that IP in IP tunnel appears as a single interface, rather than several separate interfaces. IP in IP enables tunnel intranets occur the internet, and provides an alternative to source routing. •**TCP** – Transmission Control Protocol (TCP) enables two hosts to communicate and exchange data streams. TCP guarantees packet delivery, and guarantees that packets are transmitted and received in the order they are sent. •**EGP** – Exterior Gateway Protocol (EGP) permits exchanging routing information between two neighboring gateway hosts in an autonomous systems network. •**IGP** – Interior Gateway Protocol (IGP) enables a routing information exchange between gateways within an autonomous network. •**UDP** – User Datagram Protocol (UDP) is a communication protocol that transmits packets but does not guarantee their delivery. •**HMP** – The Host Mapping Protocol (HMP) collects network information from various networks hosts. HMP monitors hosts spread over the internet as well as hosts in a single network. •**RDP** – Reliable Data Protocol (RDP) provides a reliable data transport service for packet-based applications. •**IPv6** – Matches the packet to the IPV6 protocol. •**IPv6: ROUT** – Routing Header for IPv6. •**IPv6: FRAG** – Fragment Header for IPv6. •**RVSP** – Matches the packet to the ReSerVation Protocol(RSVP). •**IPv6: ICMP** – The Internet Control Message Protocol (ICMP) allows the gateway or destination host to communicate with the source host. •**OSPF** – The Open Shortest Path First (OSPF) protocol is a link-state hierarchical interior gateway protocol (IGP) for network routing Layer Two (2) Tunneling Protocols. It is an extension to the PPP protocol that enables ISPs operate Virtual Private Networks (VPNs). •**PIM** – Matches the packet to Protocol Independent Multicast (PIM). •**L2TP** – Matches the packet to Internet Protocol (L2TP).
Source IP	Enter the source IP address.
Destination IP	Enter the destination IP address.
Type of Service	Select **Any**, **DSCP** or **IP Precedence** from the list. The **DSCP** range is from 0-63. The **IP Precedence** range is from 0-7.
Source Port	Select **Any**, **Single** or **Range** from the list. Enter the source port that is matched to packets. The range is from 0-65535.
Destination Port	Select **Any**, **Single** or **Range** from the list. Enter the destination port that is matched to packets. The range is from 0-65535.
TCP Flags	Set the TCP Flags.
ICMP Type	Select the ICMP Type.
ICMP Code	Enter the ICMP code. The range is from 0-255.

12.5 IPv6 ACL

Click **ACL** > **IPv6 ACL**

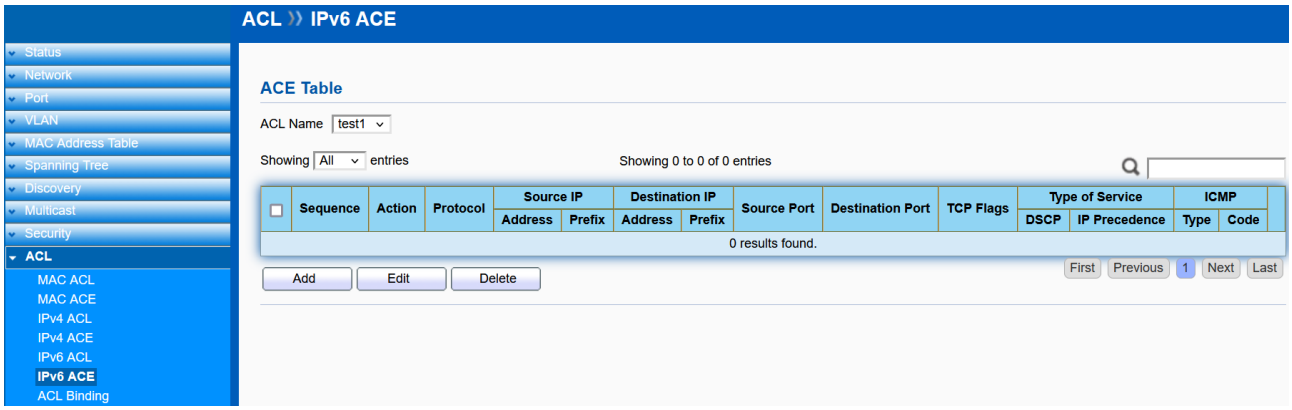
This page displays the currently-defined IPv6-based ACLs profiles. To add a new ACL, enter the name of the new ACL and click **Apply**.



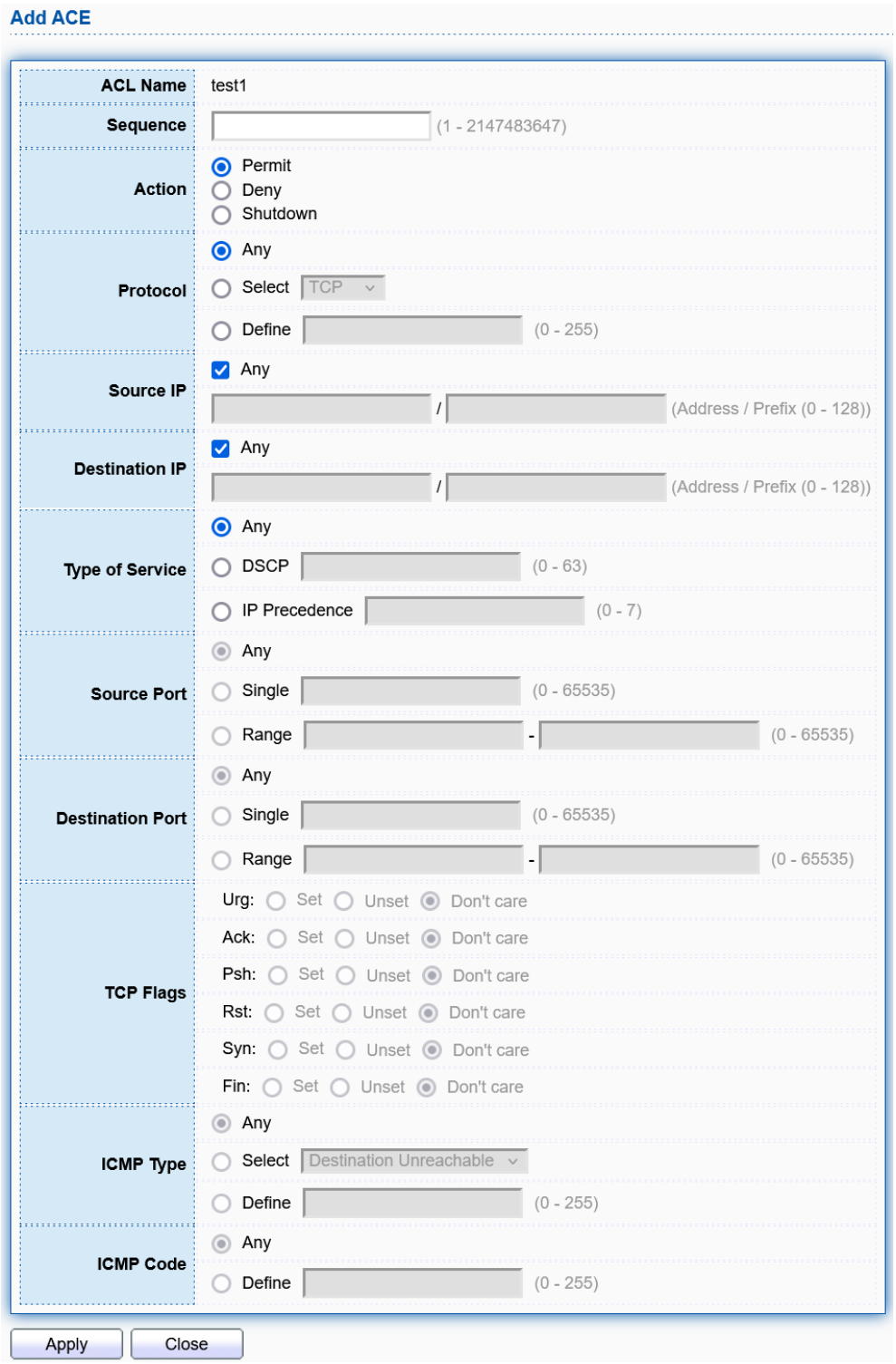
12.6 IPv6 ACE

Click **ACL** > **IPv6 ACE**

Use this page to view and add rules to IPv6-based ACLs.



Select an **ACL Name** and click "**Add**/**Edit**" to add/edit ACE. Check and click **Delete** to delete ACEs.



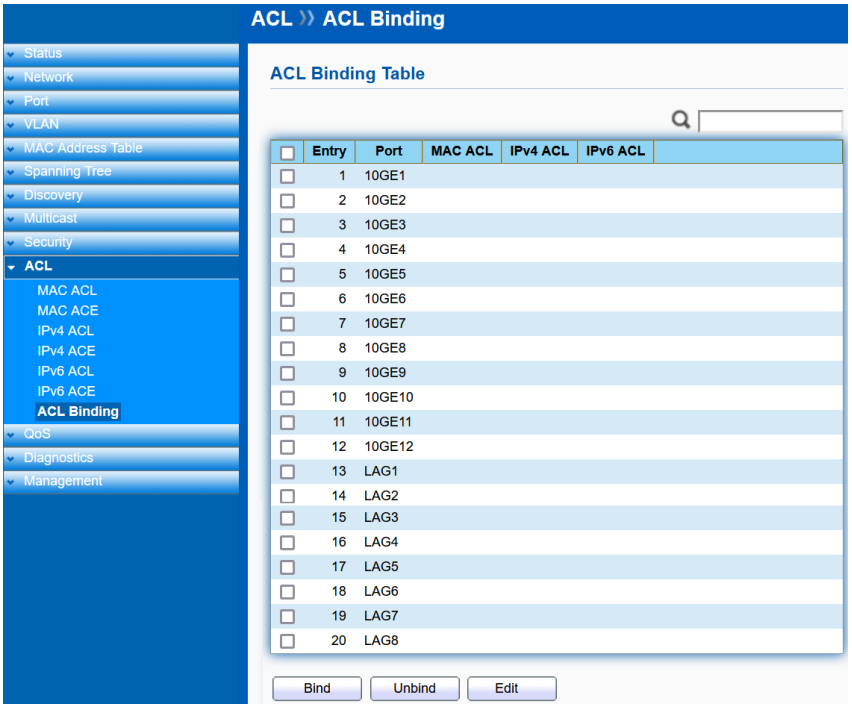
Field	Description
ACL Name	The ACL name
Sequence	Enter the sequence number which signifies the order of the specified ACL relative to other ACLs assigned to the selected interface. The valid range is from 1-2147483647, 1 being processed first.
Action	Select what action taken if a packet matches the criteria. •**Permit** – Forward packets that meet the ACL criteria. •**Deny** – Drops packets that meet the ACL criteria. •**Shutdown** – Shutdown the port that meet the ACL criteria.

Protocol	Select **Any**, **Define**, or from the list in the drop down menu. •**Any** – Check **Any** to use any protocol. •**Define** – Enter the protocol in the ACE to which the packet is matched.
Source IP	Enter the source IP address.
Destination IP	Enter the destination IP address.
Type of Service	Select **Any**, **DSCP** or **IP Precedence** from the list. The DSCP range is from 0-63. The IP Precedence range is from 0-7.
Source Port	Select **Any**, **Single** or **Range** from the list. Enter the source port that is matched to packets. The range is from 0-65535.
Destination Port	Select **Any**, **Single** or **Range** from the list. Enter the destination port that is matched to packets. The range is from 0-65535.
TCP Flags	Set the TCP Flags.
ICMP Type	Select the ICMP Type.
ICMP Code	Enter the ICMP code. The range is from 0-255.

12.7 ACL Binding

Click **ACL** > **ACL Binding**

When an ACL is bound to an interface, all the rules that have been defined for the ACL are applied to that interface. Whenever an ACL is assigned on a port or LAG, flows from that ingress or egress interface that do not match the ACL, are matched to the default rule of dropping unmatched packets. To bind an ACL to an interface, simply select an interface and select the ACL(s) you wish to bind.



Field	Description
Port	Select the port for which the ACLs are bound to.
MAC ACL	The ACL is MAC address based.
IPv4 ACL	The ACL is IPv4 based.
IPv6 ACL	The ACL is IPv6 based.

Chapter 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

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

13.1.1 Property

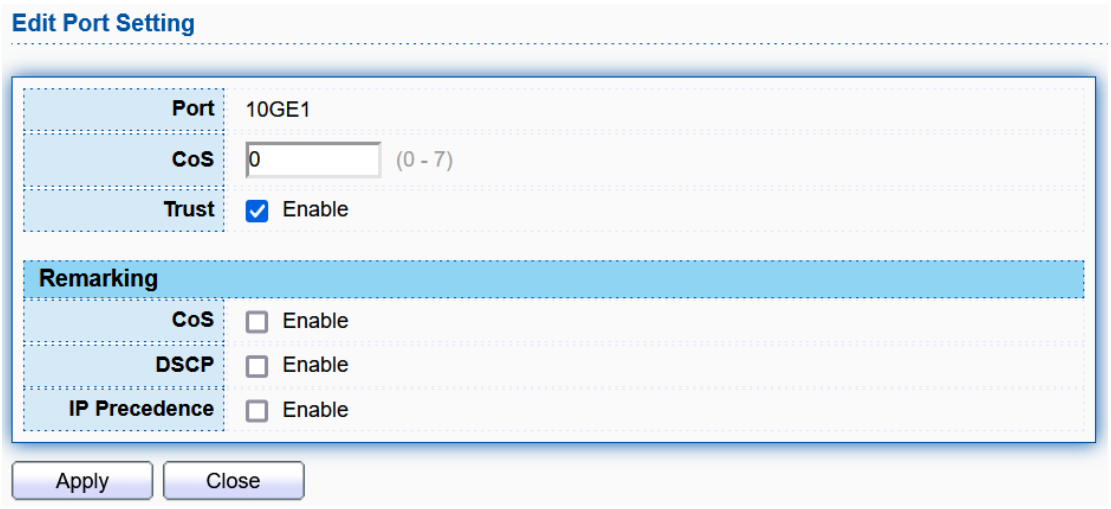
Click **QoS** > **General** > **Property**

To display QoS property web page.

Field	Description
State	Set checkbox to enable/disable QoS.

Trust Mode	Select QoS trust mode. **CoS**: Traffic is mapped to queues based on the CoS field in the VLAN tag, or based on the per-port default CoS value (if there is no VLAN tag on the incoming packet), the actual mapping of the CoS to queue can be configured on port setting dialog. **DSCP**: All IP traffic is mapped to queues based on the DSCP field in the IP header. The actual mapping of the DSCP to queue can be configured on the DSCP mapping page. If traffic is not IP traffic, it is mapped to the best effort queue. **CoS-DSCP**: Uses the trust CoS mode for non-IP traffic and trust DSCP mode for IP traffic. IP Precedence: Traffic is mapped to queues based on the IP precedence. The actual mapping of the IP precedence to queue can be configured on the IP Precedence mapping page.
Field	**Description**
Port	Port name
CoS	Port default CoS priority value for the selected ports.
Trust	Port trust state **Enable**: Traffic will follow trust mode in global setting. **Disable**: Traffic will always use best efforts.
Remarking (CoS)	Port CoS remarking admin state. **Enable**: CoS remarking is enabled **Disable**: CoS remarking is disabled
Remarking (DSCP)	Port DSCP remarking admin state. **Enable**: DSCP remarking is enabled **Disable**: DSCP remarking is disabled
Remarking (IP Precedence)	Port IP Precedence remarking admin state. **Enable**: IP Precedence remarking is enabled **Disable**: IP Precedence remarking is disabled

Click “**Edit**” to edit the QoS port setting.



Field	Description
Port	Select port list
CoS	Set default CoS priority value for the selected ports.
Trust	Set checkbox to enable/disable port trust state.
Remarking (CoS)	Set checkbox to enable/disable port CoS remarking.
Remarking (DSCP)	Set checkbox to enable/disable port DSCP remarking.

Remarking (IP Precedence)	Set checkbox to enable/disable port IP Precedence remarking.

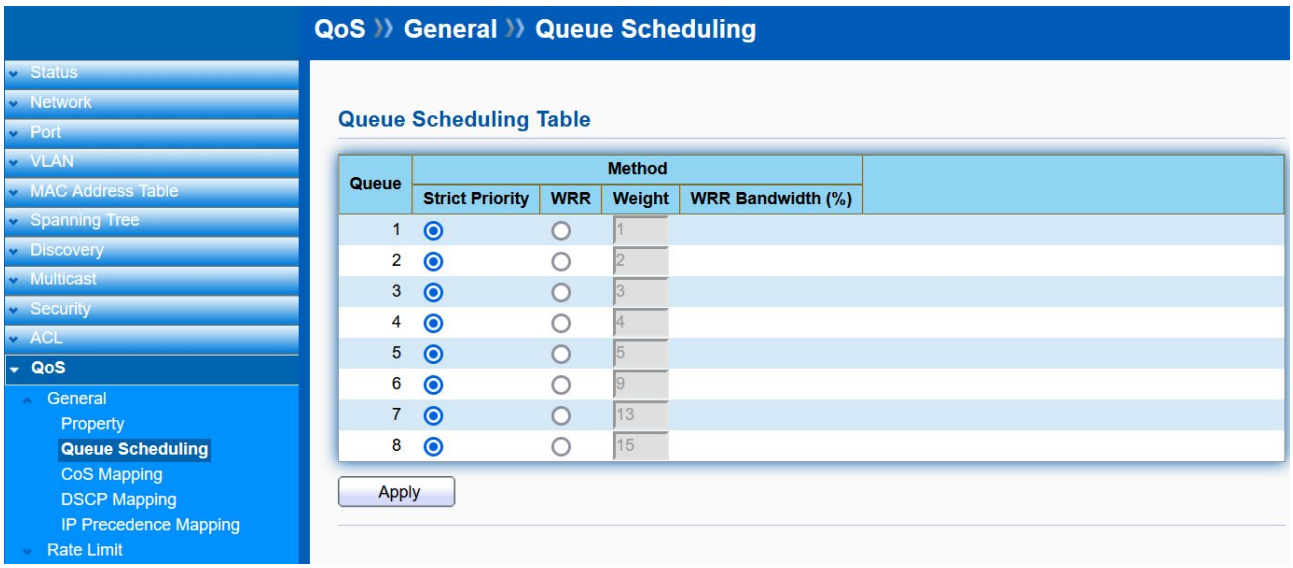
13.1.2 Queue Scheduling

Click **QoS** > **General** > **Queue Scheduling**

To display Queue Scheduling web page.

The switch supports eight queues for each interface. Queue number 8 is the highest priority queue. Queue number 1 is the lowest priority queue. There are two ways of determining how traffic in queues is handled, **Strict Priority (SP)** and **Weighted Round Robin (WRR)**.
Strict Priority (SP): Egress traffic from the highest priority queue is transmitted first. Traffic from the lower queues is processed only after the highest queue has been transmitted, which provide the highest level of priority of traffic to the highest numbered queue.
Weighted Round Robin (WRR): In WRR mode the number of packets sent from the queue is proportional to the weight of the queue (the higher the weight, the more frames are sent).

The queuing mode can be selected on the Queue page. When the queuing mode is by Strict Priority, the priority sets the order in which queues are serviced, starting with queue_8 (the highest priority queue) and going to the next lower queue when each queue is completed.
When the queuing mode is Weighted Round Robin, queues are serviced until their quota has been used up and then another queue is serviced. It is also possible to assign some of the lower queues to WRR, while keeping some of the higher queues in Strict Priority. In this case traffic for the SP queues is always sent before traffic from the WRR queues. After the SP queues have been emptied, traffic from the WRR queues is forwarded. (The relative portion from each WRR queue depends on its weight).



Field	Description
Queue	Queue ID to configure
Strict Priority	Set queue to strict priority type
WRR	Set queue to Weight Round Robin type.
Weight	If the queue type is WRR, set the queue weight for the queue.

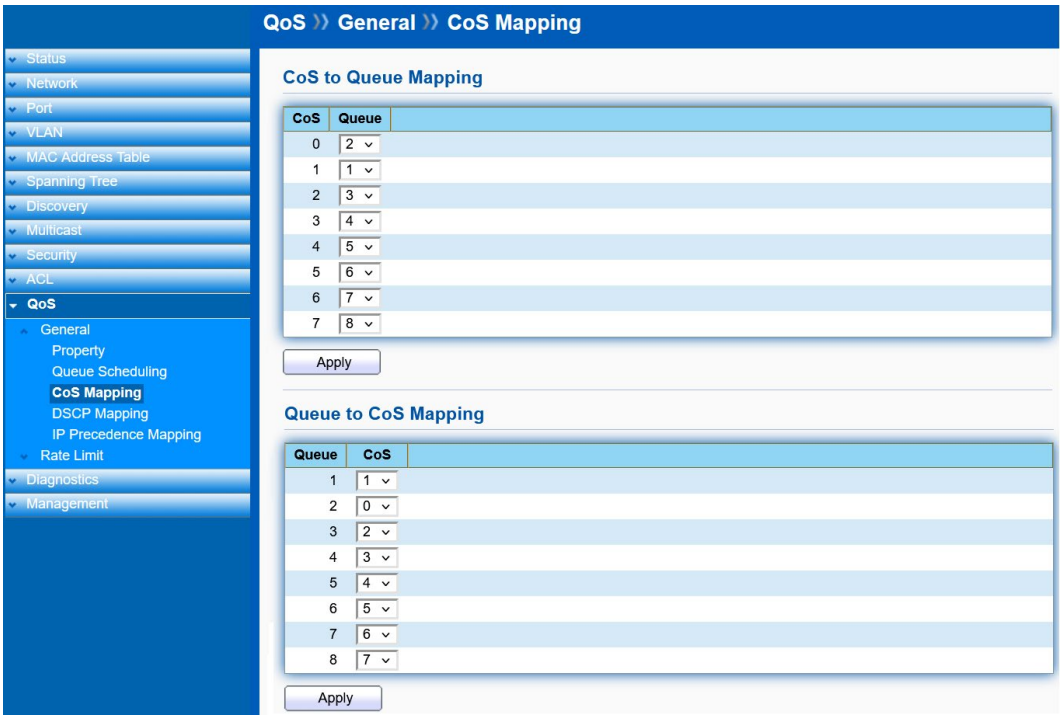
WRR Bandwidth	Percentage of WRR queue bandwidth.

13.1.3 CoS Mapping

Click **QoS** > **General** > **CoS Mapping**

To display CoS Mapping web page.

The CoS to Queue table determines the egress queues of the incoming packets based on the 802.1p priority in their VLAN tags. For incoming untagged packets, the 802.1p priority will be the default CoS/802.1p priority assigned to the ingress ports.
Use the Queues to CoS table to remark the CoS/802.1p priority for egress traffic from each queue.



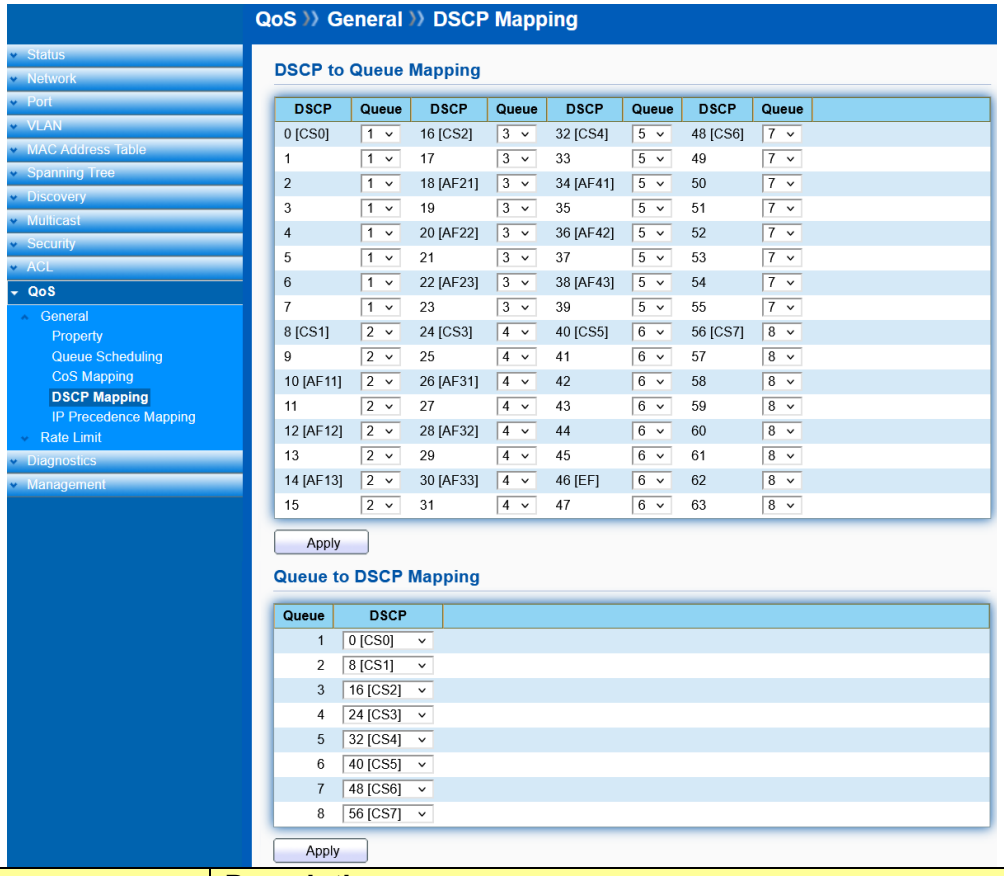
Field	Description
CoS	CoS value
Queue	Select queue ID for the CoS value
Field	**Description**
Queue	Queue ID
CoS	Select CoS value for the queue ID.

13.1.4 DSCP Mapping

Click **QoS** > **General** > **DSCP Mapping**

To display DSCP Mapping web page.

The DSCP to Queue table determines the egress queues of the incoming IP packets based on their DSCP values. The original VLAN Priority Tag (VPT) of the packet is unchanged.
Use the Queues to DSCP page to remark DSCP value for egress traffic from each queue.



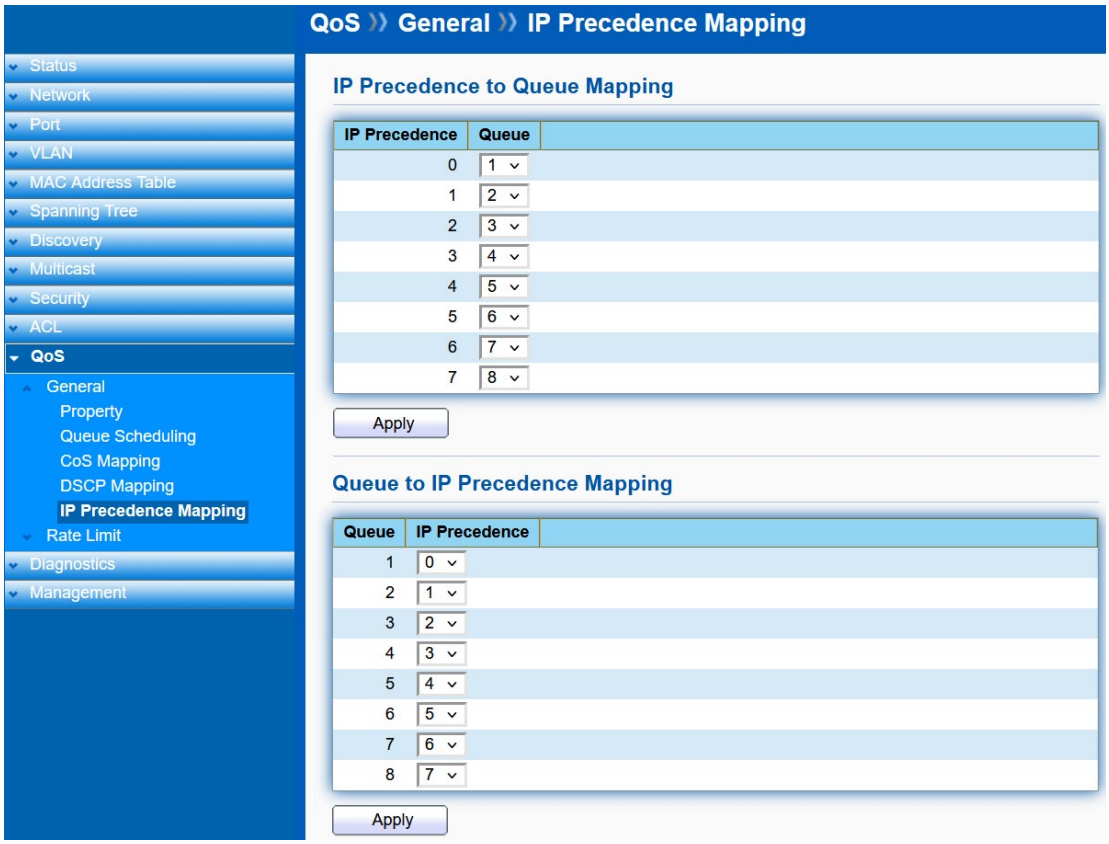
Field	Description
DSCP	DSCP value
Queue	Select Queue ID for DSCP value.
Field	**Description**
Queue	Queue ID
DSCP	Select DSCP value for Queue ID.

13.1.5 IP Precedence Mapping

Click **QoS** > **General** > **IP Precedence Mapping**

To display IP Precedence Mapping web page.

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



Field	Description
IP Precedence	IP Precedence value
Queue	Queue value which IP Precedence is mapped.
Field	**Description**
Queue	Queue ID
IP Precedence	IP Precedence value which queue is mapped.

13.2 Rate Limit

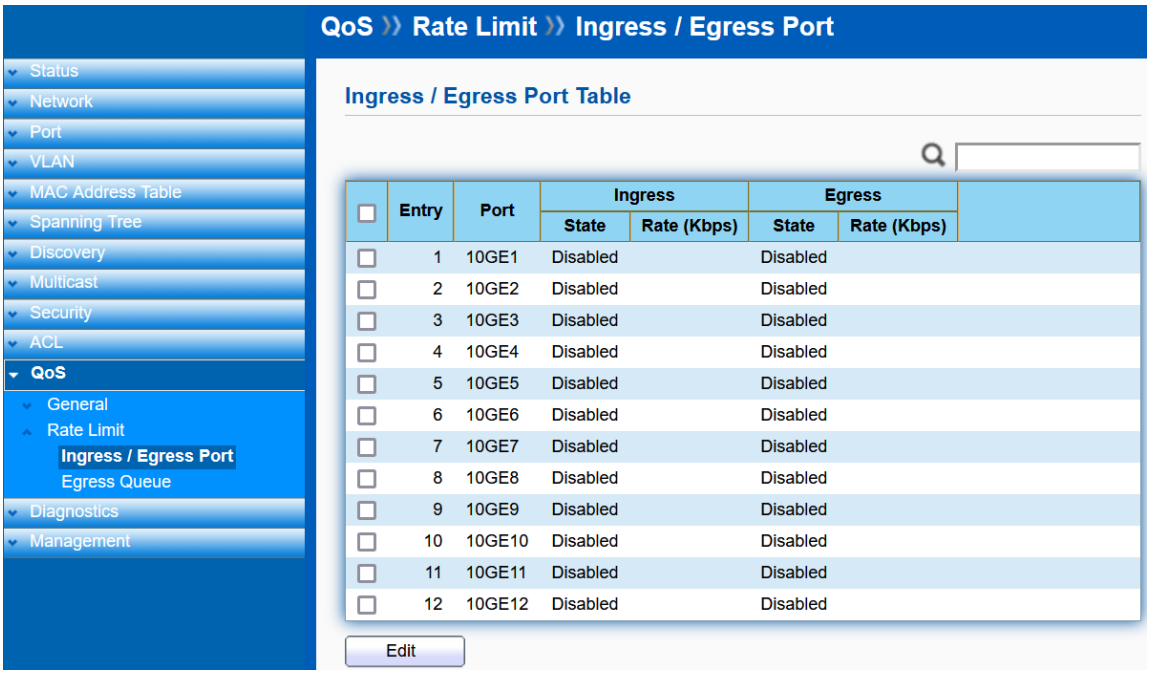
Use the Rate Limit pages to define values that determine how much traffic the switch can receive and send on specific port or queue.

13.2.1 Ingress / Egress Port

Click **QoS** > **Rate Limit** > **Ingress/Egress**

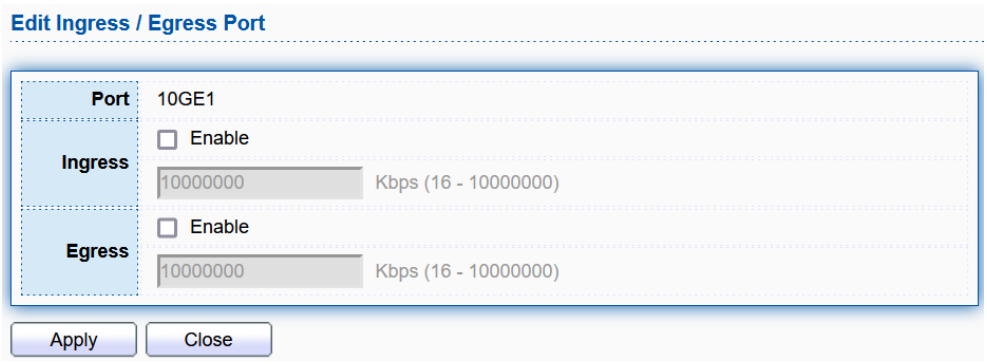
To display Ingress/Egress Port web page.

This page allow user to configure ingress port rate limit and egress port rate limit. The ingress rate limit is the number of bits per second that can be received from the ingress interface. Excess bandwidth above this limit is discarded.



Field	Description
Port	Port name
Ingress (State)	Port ingress rate limit state Enable: Ingress rate limit is enabled. Disable: Ingress rate limit is disabled.
Ingress (Rate)	Port ingress rate limit value if ingress rate state is enabled.
Egress (State)	Port egress rate limit state Enable: Egress rate limit is enabled. Disable: Egress rate limit is disabled.
Egress (Rate)	Port egress rate limit value if egress rate state is enabled.

Click "**Edit**" to edit Ingress/Egress Port.



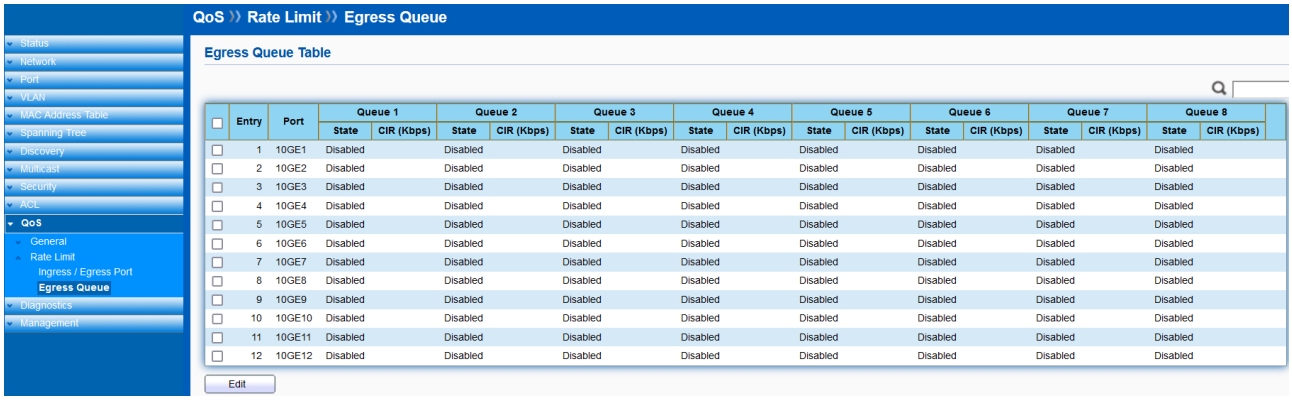
Field	Description
Port	Select Port list
Ingress	Set checkbox to enable/disable ingress rate limit. If ingress rate limit is enabled, rate limit value need to be assigned.
Egress	Set checkbox to enable/disable egress rate limit. If egress rate limit is enabled, rate limit value need to be assigned.

13.2.2 Egress Queue

Click **QoS** > **Rate Limit** > **Egress Queue**

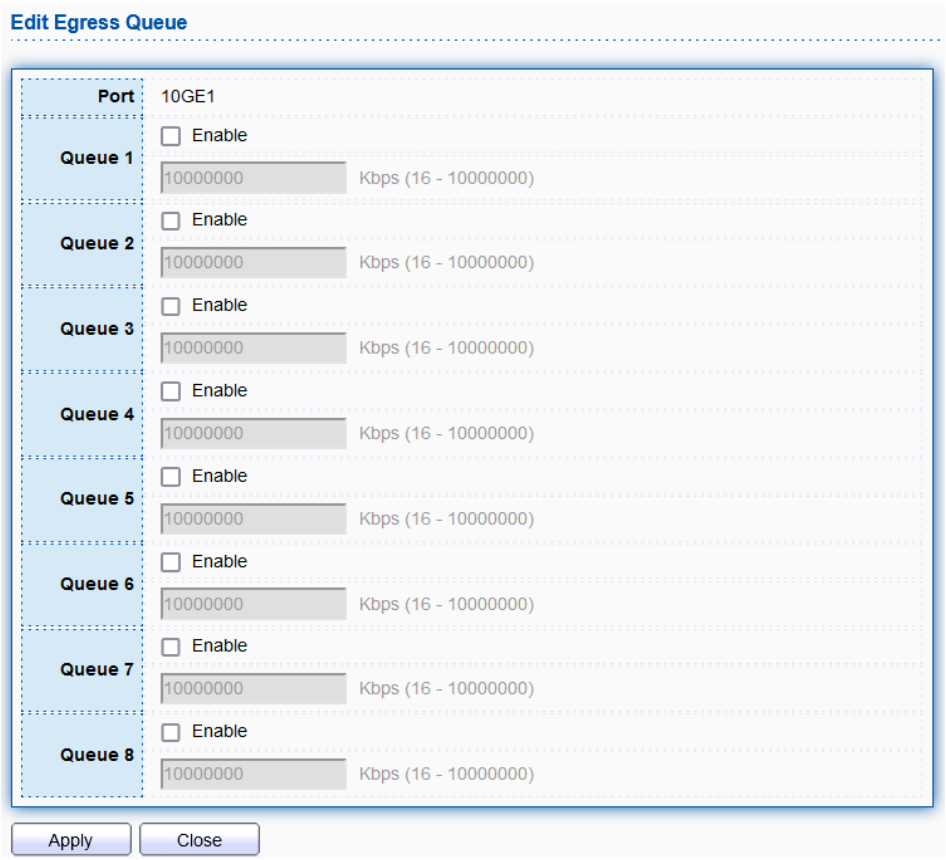
To display Egress Queue web page.

Egress rate limiting is performed by shaping the output load.



Field	Description
Port	Port name
Queue 1 (State)	Port egress queue 1 rate limit state. **Enable**: Egress queue rate limit is enable. **Disable**: Egress queue rate limit is disable.
Queue 1 (CIR)	Queue 1 egress committed information rate.
Queue 2 (State)	Port egress queue 2 rate limit state. **Enable**: Egress queue rate limit is enable. **Disable**: Egress queue rate limit is disable.
Queue 2 (CIR)	Queue 2 egress committed information rate.
Queue 3 (State)	Port egress queue 3 rate limit state. **Enable**: Egress queue rate limit is enable. **Disable**: Egress queue rate limit is disable.
Queue 3 (CIR)	Queue 3 egress committed information rate.
Queue 4 (State)	Port egress queue 4 rate limit state. **Enable**: Egress queue rate limit is enable. **Disable**: Egress queue rate limit is disable.
Queue 4 (CIR)	Queue 4 egress committed information rate.
Queue 5 (State)	Port egress queue 5 rate limit state. **Enable**: Egress queue rate limit is enable. **Disable**: Egress queue rate limit is disable.
Queue 5 (CIR)	Queue 5 egress committed information rate.
Queue 6 (State)	Port egress queue 6 rate limit state. **Enable**: Egress queue rate limit is enable. **Disable**: Egress queue rate limit is disable.
Queue 6 (CIR)	Queue 6 egress committed information rate.
Queue 7 (State)	Port egress queue 7 rate limit state. **Enable**: Egress queue rate limit is enable. **Disable**: Egress queue rate limit is disable.
Queue 7 (CIR)	Queue 7 egress committed information rate.
Queue 8 (State)	Port egress queue 8 rate limit state. **Enable**: Egress queue rate limit is enable. **Disable**: Egress queue rate limit is disable.
Queue 8 (CIR)	Queue 8 egress committed information rate.

Click “**Edit**” to edit Egress Queue



Field	Description
Port	Select port list
Queue 1	Set checkbox to enable/disable egress queue 1 rate limit. If egress rate limit is enabled, rate limit value need to be assigned.
Queue 2	Set checkbox to enable/disable egress queue 2 rate limit. If egress rate limit is enabled, rate limit value need to be assigned.
Queue 3	Set checkbox to enable/disable egress queue 3 rate limit. If egress rate limit is enabled, rate limit value need to be assigned.
Queue 4	Set checkbox to enable/disable egress queue 4 rate limit. If egress rate limit is enabled, rate limit value need to be assigned.
Queue 5	Set checkbox to enable/disable egress queue 5 rate limit. If egress rate limit is enabled, rate limit value need to be assigned.
Queue 6	Set checkbox to enable/disable egress queue 6 rate limit. If egress rate limit is enabled, rate limit value need to be assigned.
Queue 7	Set checkbox to enable/disable egress queue 7 rate limit. If egress rate limit is enabled, rate limit value need to be assigned.
Queue 8	Set checkbox to enable/disable egress queue 8 rate limit. If egress rate limit is enabled, rate limit value need to be assigned.

Chapter 14 Diagnostics

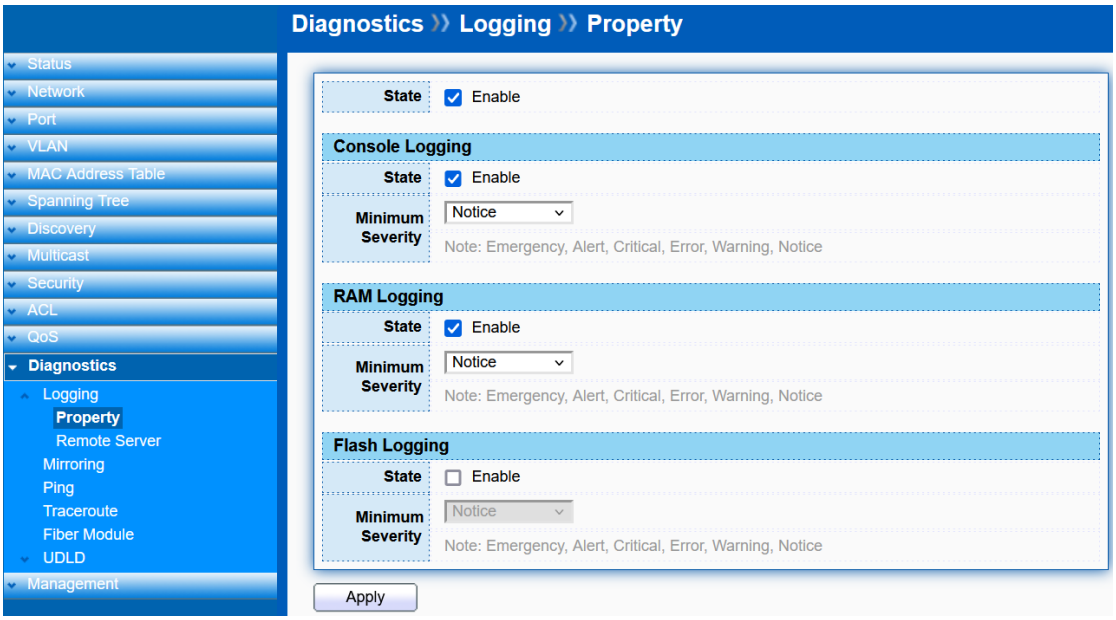
Use the Diagnostic pages to configure settings for the switch diagnostics feature or operating diagnostic utilities.

14.1 Logging

14.1.1 Property

Click **Diagnostics** > **Logging** > **Property**

To display the Logging Service web page.



Field	Description
State	Enable/Disable the global logging services. When the logging service is enabled, logging configuration of each destination rule can be individually configured. If the logging service is disabled, no messages will be sent to these destinations.

Console Logging

Field	Description
State	Enable/Disable the console logging service.
Minimum Severity	The minimum severity for the console logging.

RAM Logging

Field	Description
State	Enable/Disable the RAM logging service.
Minimum Severity	The minimum severity for the RAM logging.

Flash Logging

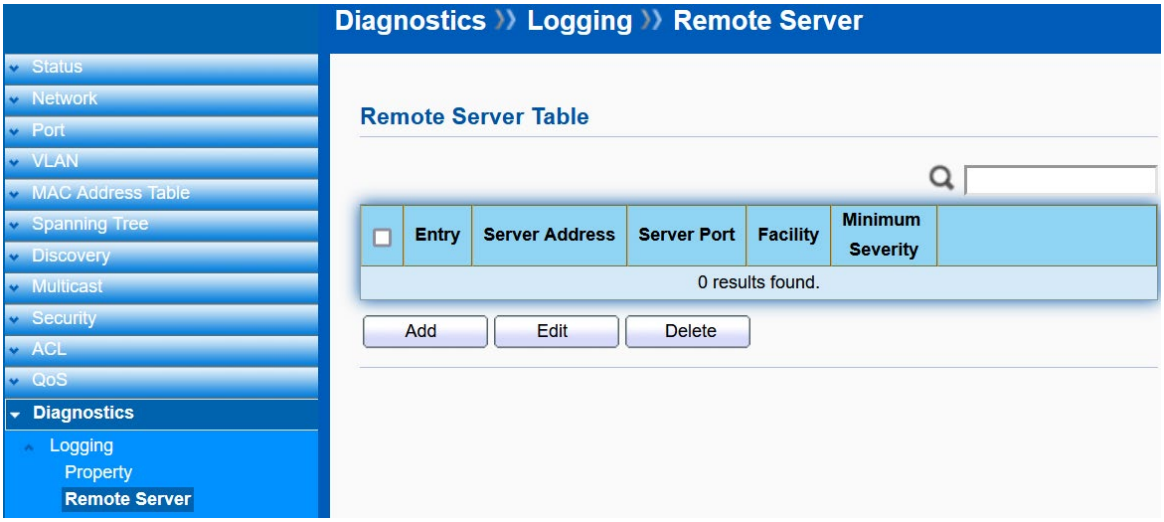
Field	Description

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

14.1.2 Remote Server

Click **Diagnostics** > **Logging** > **Remote Server**

To display the Remote Logging Server web page.

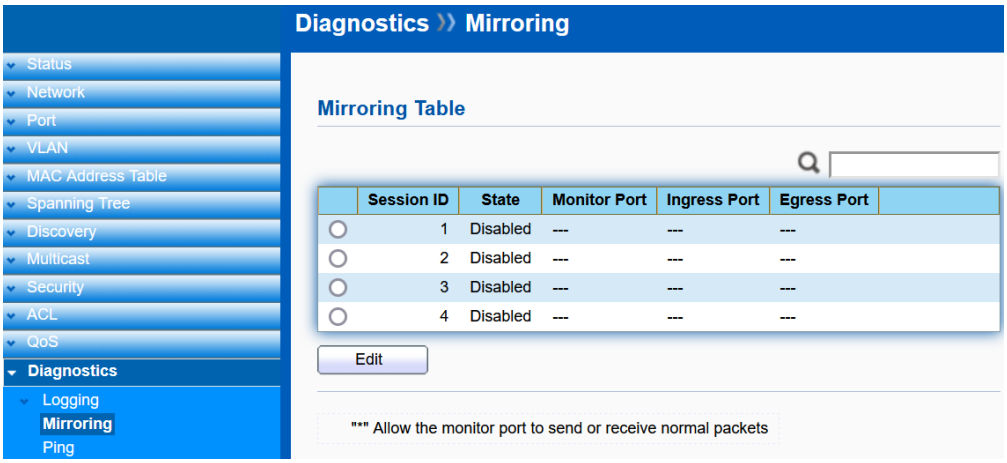


Field	Description
Server Address	The IP address of the remote logging server.
Server Ports	The port number of the remote logging server.
Facility	The facility of the logging messages. It can be one of the following values: local0, local1, local2, local3, local4, local5, local6, and local7.
Severity	The minimum severity **Emergence**: System is not usable. **Alert**: Immediate action is needed. **Critical**: System is in the critical condition. **Error**: System is in error condition. **Warning**: System warning has occurred. **Notice**: System is functioning properly, but a system notice has occurred. **Informational**: Device information. **Debug**: Provides detailed information about an event.

14.2 Mirroring

Click **Diagnostics** > **Mirroring**

To display the Port Mirroring web page.

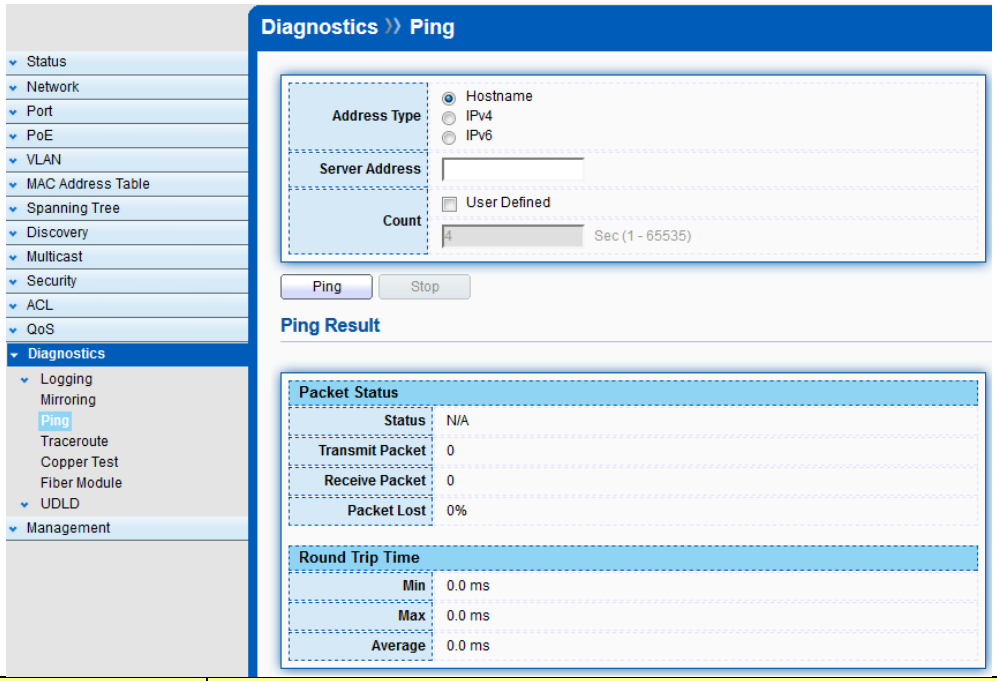


Field	Description
Session ID	Select mirror session ID
State	Select mirror session state : port-base mirror or disable **Enabled** : Enable port based mirror **Disabled** : Disable mirror
Monitor Port	Select mirror session monitor port, and select. Whether normal packet could be sent or received by monitor port.
Ingress Port	Select mirror session source RX ports.
Egress Port	Select mirror session source TX ports.

14.3 Ping

Click **Diagnostics** > **Ping**

To display the Diagnostic Ping functionality web page.

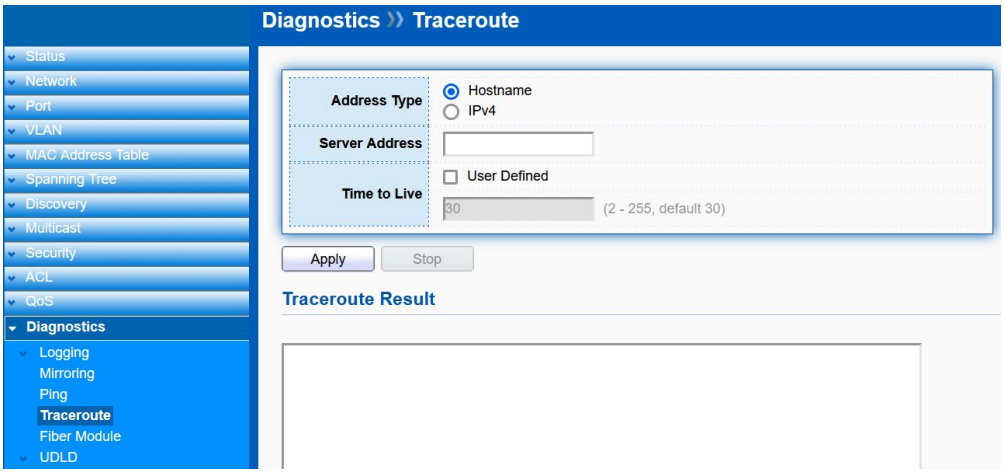


Field	Description
Address Type	Specify the address type to “Hostname”, “IPv4”, or “IPv6”.
Server Address	Specify the Hostname/IPv4/IPv6 address for ping diagnostics.
Count	Specify the numbers of each ICMP ping request.

14.4 Traceroute

Click **Diagnostics** > **Traceroute**

To display the Diagnostic Traceroute functionality web page.

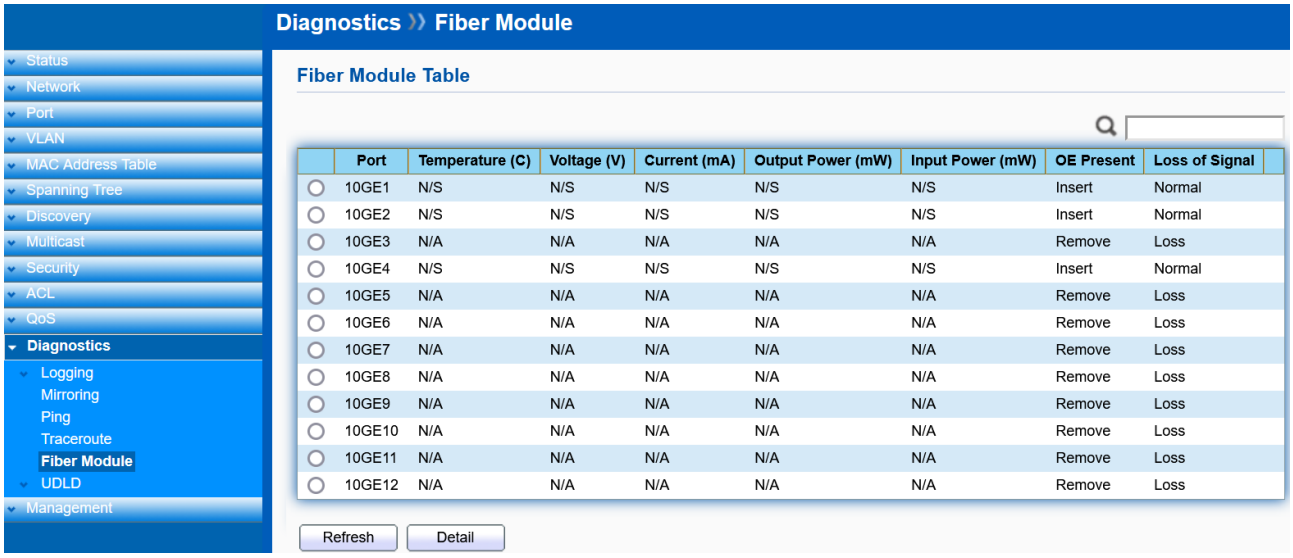


Field	Description
Address Type	Specify the address type to “Hostname” or “IPv4”.
Server Address	Specify the Hostname/IPv4 address for traceroute diagnostics.
Time to Live	Specify the numbers of Time to Live.

14.5 Fiber Module

Click **Diagnostics** > **Fiber Module**

To display the fiber module.



Click “**Detail**” to display the detail information.

14.6 UDLD

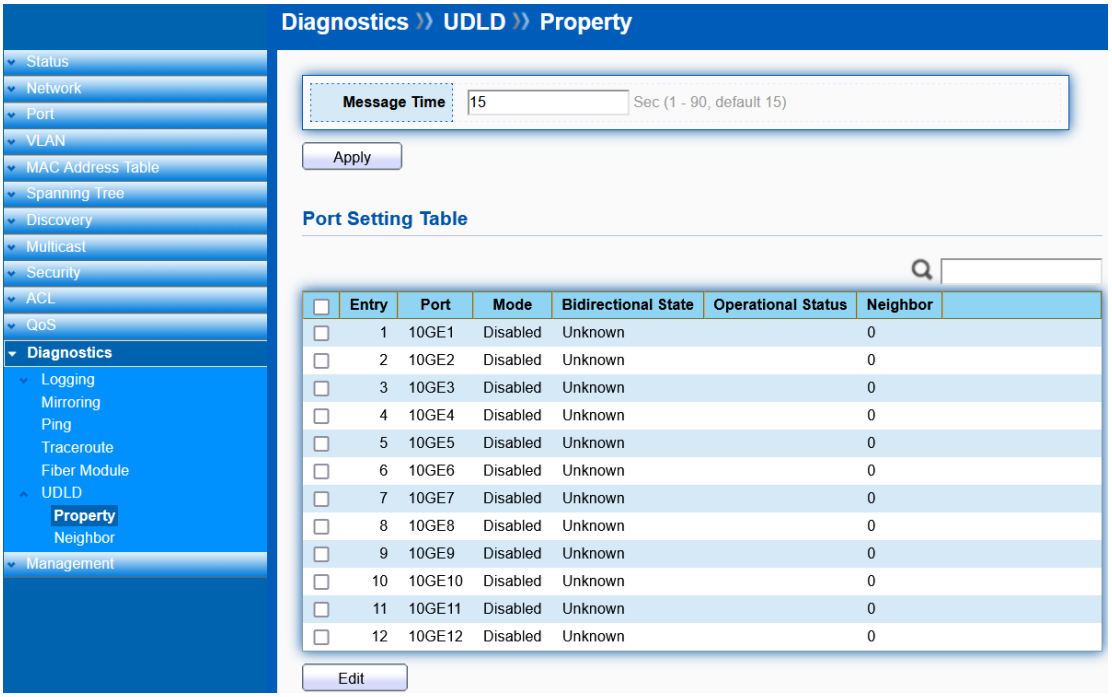
Unidirectional Link Detection (**UDLD**) is a data link layer protocol from Cisco Systems to monitor the physical configuration of the cables and detect unidirectional links.

Unidirectional Link failure can cause "traffic blackholing" and loop in the Switch topology.
In order to detect the unidirectional links before the forwarding loop is created, UDLD works by exchanging protocol packets between the neighboring devices. In order for UDLD to work, both switch devices on the link must support UDLD and have it enabled on respective ports.

14.6.1 Property

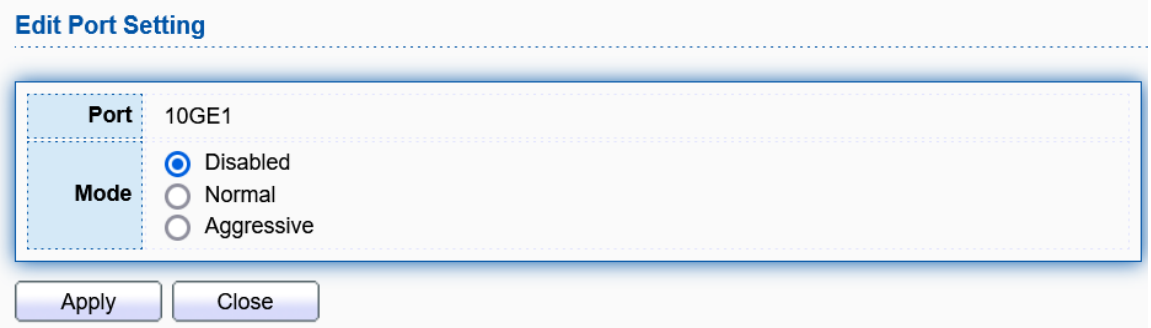
Click **Diagnostics** > **UDLD** > **Property**

To view the UDLD status and set up UDLD mode.



Field	Description
Message Time	Aging of UDLD information happens when the port that runs UDLD does not receive UDLD packets from the neighbor port for duration of hold time. The hold time for the port is dictated by the remote port and depends on the **Message Time** at the remote side. The shorter the Message Time, the shorter the hold time and the faster the detection. The range of Message Time is from 1-90. Default is 15 seconds.

Check and click "**Edit**" to edit UDLD mode.



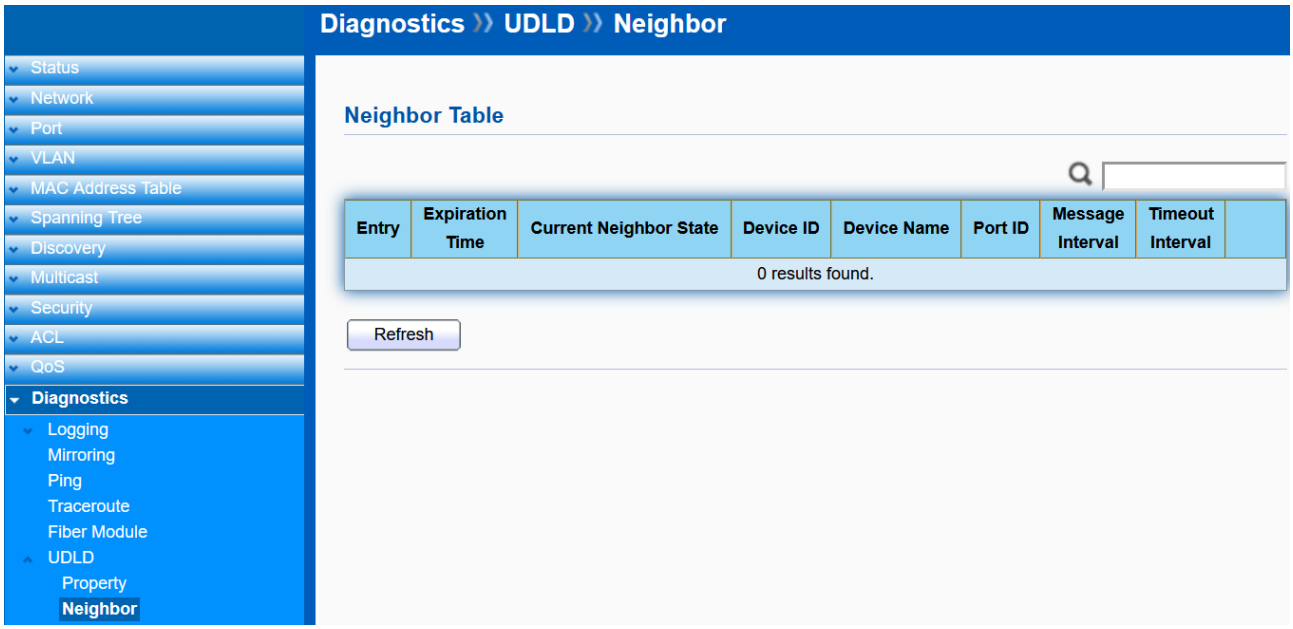
Field	Description
Port	The interface for UDLD.

Mode	**Disabled**: The UDLD function is disabled. **Normal**: In normal mode, if the link state of the port was determined to be bi-directional and the UDLD information times out, no action is taken by UDLD. The port state for UDLD is marked as undetermined. The port behaves according to its STP state. **Aggressive**: In aggressive mode, if the link state of the port is determined to be bi-directional and the UDLD information times out while the link on the port is still up, UDLD tries to re-establish the state of the port. If not successful, the port is put into the Error Disabled state.

14.6.2 Neighbor

Click **Diagnostics** > **UDLD** > **Neighbor**

To view the UDLD neighbor status.



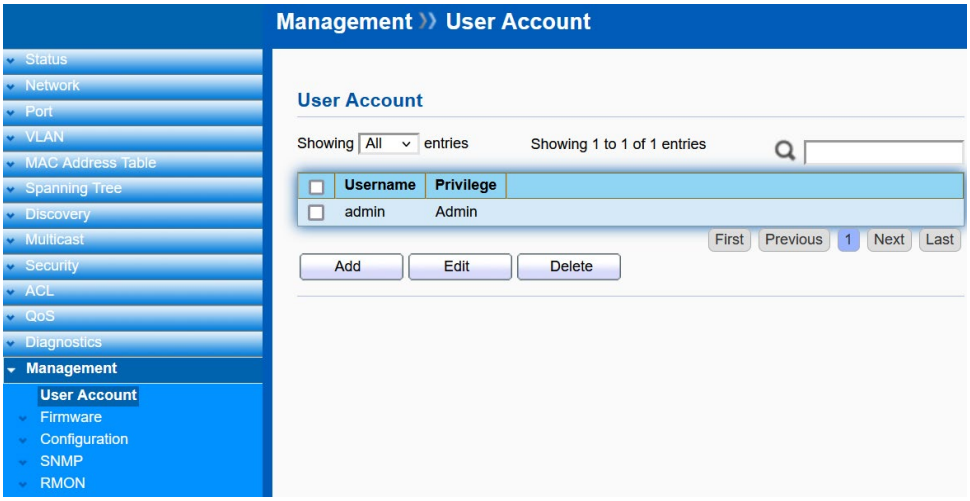
Chapter 15 Management

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

15.1 User Account

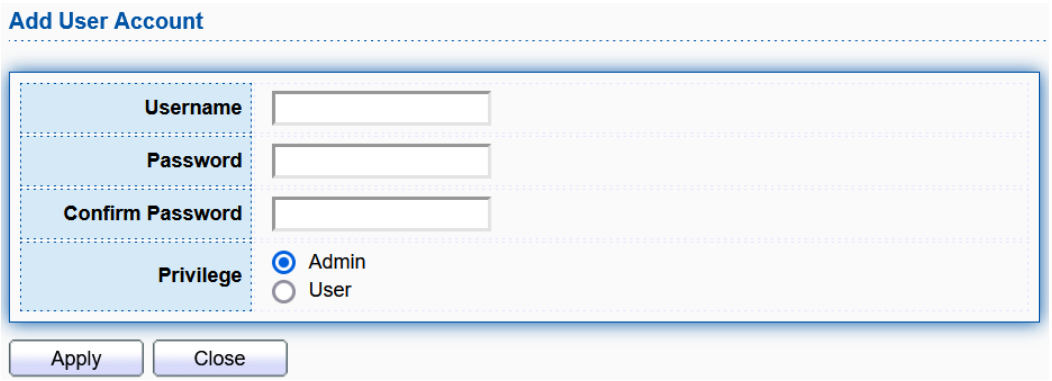
Click **Management** > **User Account**

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



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

Click "**Add**" or "**Edit**" to add/edit User Account.



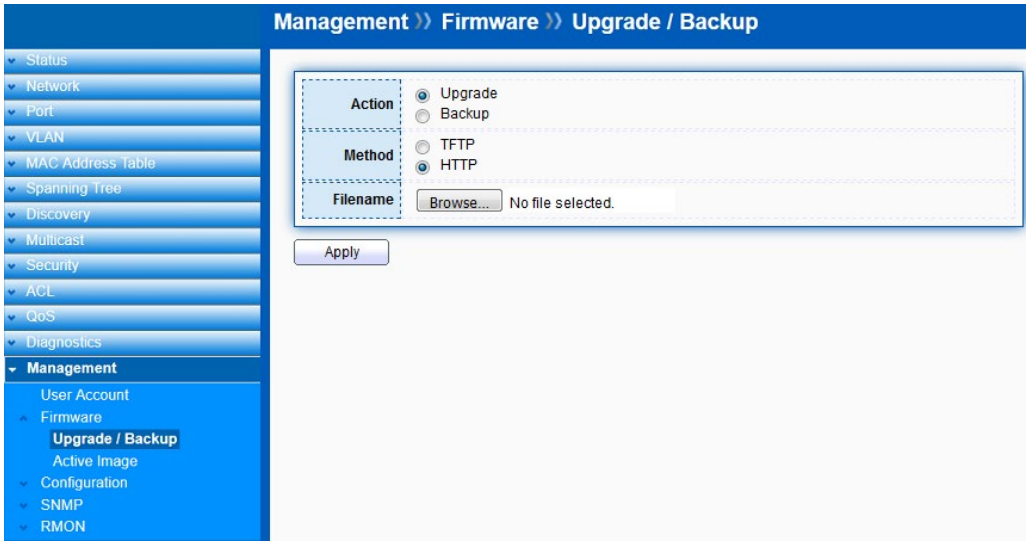
Field	Description
Username	User name of the account.
Password	Set password of the account.
Confirm Password	Set the same password of the account as in "Password" field
Privilege	Select privilege level for new account. **Admin**: Allow to change switch settings. Privilege value equals to 15. **User**: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

15.2 Firmware

15.2.1 Upgrade / Backup

Click **Management** > **Firmware** > **Upgrade/Backup**

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



Upgrade Firmware through HTTP

Field	Description
Action	Firmware operations **Upgrade**: Upgrade firmware from remote host to DUT. **Backup**: Backup firmware image from DUT to remote host.
Method	Firmware upgrade/backup method **TFTP**: Using TFTP to upgrade/backup firmware. **HTTP**: Using WEB browser to upgrade/backup firmware.
Filename	Use browser to upgrade firmware, you should select firmware image file on your host PC.

Upgrade Firmware through TFTP.

Field	Description
Action	Firmware operations **Upgrade**: Upgrade firmware from remote host to DUT. **Backup**: Backup firmware image from DUT to remote host.
Method	Firmware upgrade/backup method **TFTP**: Using TFTP to upgrade/backup firmware. **HTTP**: Using WEB browser to upgrade/backup firmware.
Address Type	Specify TFTP server address type **Hostname**: Use domain name as server address. **IPv4**: Use IPv4 as server address **IPv6**: Use IPv6 as server address
Server Address	Specify TFTP server address.
Filename	Firmware image file name on remote TFTP server

Backup Firmware through HTTP

Field	Description

Action	Firmware operations **Upgrade**: Upgrade firmware from remote host to DUT. **Backup**: Backup firmware image from DUT to remote host.
Method	Firmware upgrade/backup method **TFTP**: Using TFTP to upgrade/backup firmware. **HTTP**: Using WEB browser to upgrade/backup firmware.
Firmware	Select which image file to backup. **Image0**: backup image0. **Image1**: backup image1.

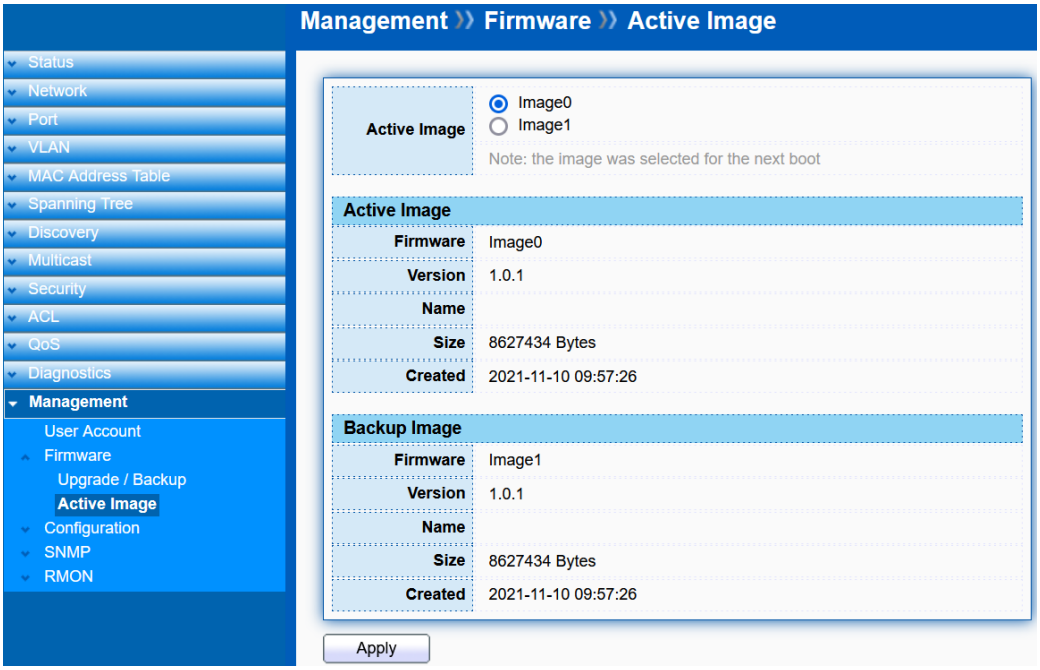
Backup Firmware through TFTP

Field	Description
Action	Firmware operations **Upgrade**: Upgrade firmware from remote host to DUT. **Backup**: Backup firmware image from DUT to remote host.
Method	Firmware upgrade/backup method **TFTP**: Using TFTP to upgrade/backup firmware. **HTTP**: Using WEB browser to upgrade/backup firmware.
Firmware	Select which image file to backup. **Image0**: backup image0. **Image1**: backup image1.
Address Type	Specify TFTP server address type **Hostname**: Use domain name as server address **IPv4**: Use IPv4 as server address **IPv6**: Use IPv6 as server address
Server Address	Specify TFPT server address
Filename	File name saved on remote TFTP server

15.2.2 Active Image

Click **Management** > **Firmware** > **Active Image**

This page allows user to select firmware image.



Field	Description
Active Image	Select the image to active.

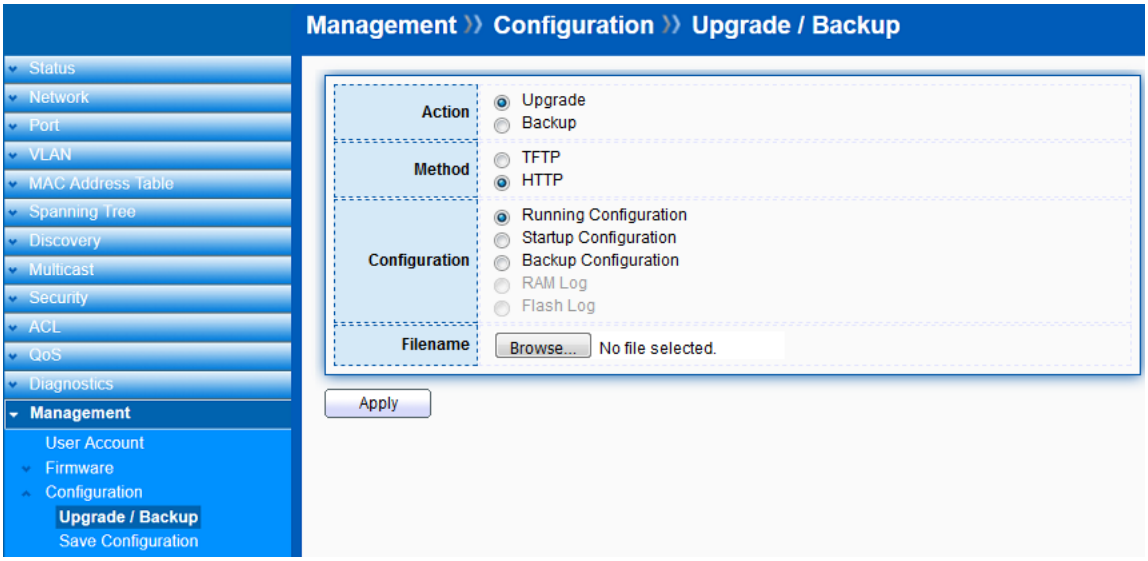
Active/Backup Image	**Firmware**: Image0 or Image1 **Version**: The firmware version of this image. **Name**: The filename of this image. **Size**: The file size of this image. **Created**: The date when this image created.

15.3 Configuration

15.3.1 Upgrade / Backup

Click **Management** > **Configuration** > **Upgrade/Backup**

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



Upgrade Configuration through HTTP

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

Upgrade Configuration through TFTP.

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

Configuration	Configuration types **Running Configuration**: Merge to current running configuration file. **Startup Configuration**: Replace the startup configuration file. **Backup Configuration**: Replace the backup configuration file.
Address Type	Specify TFTP server address type **Hostname**: Use domain name as server address. **IPv4**: Use IPv4 as server address **IPv6**: Use IPv6 as server address
Server Address	Specify TFTP server address.
Filename	Configuration image file name on remote TFTP server

Backup Configuration through HTTP

Field	Description
Action	Configuration operations **Upgrade**: Upgrade Configuration from remote host to DUT. **Backup**: Backup Configuration image from DUT to remote host.
Method	Configuration upgrade/backup method **TFTP**: Using TFTP to upgrade/backup Configuration. **HTTP**: Using WEB browser to upgrade/backup Configuration.
Configuration	Configuration types **Running Configuration**: Merge to current running configuration file. **Startup Configuration**: Backup the startup configuration file. **Backup Configuration**: Backup the backup configuration file. **RAM Log**: Backup log file stored in RAM **Flash Log**: Backup log files store in Flash.

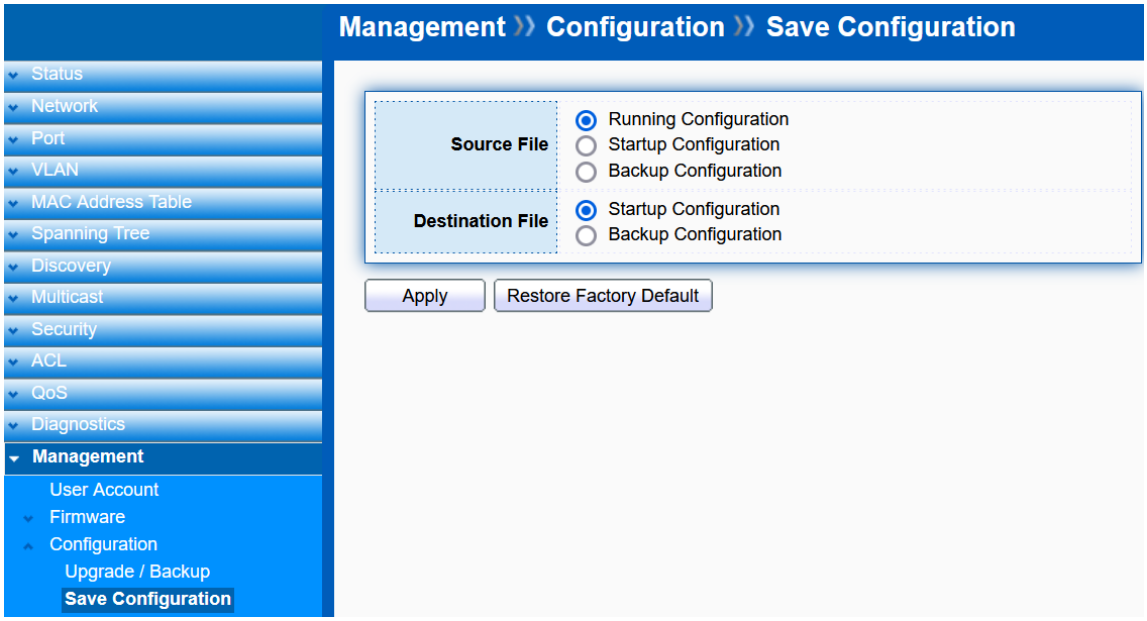
Backup Configuration through TFTP.

Field	Description
Action	Configuration operations **Upgrade**: Upgrade Configuration from remote host to DUT. **Backup**: Backup Configuration image from DUT to remote host.
Method	Configuration upgrade/backup method **TFTP**: Using TFTP to upgrade/backup Configuration. **HTTP**: Using WEB browser to upgrade/backup Configuration.
Configuration	Configuration types **Running Configuration**: Merge to current running configuration file. **Startup Configuration**: Backup the startup configuration file. **Backup Configuration**: Backup the backup configuration file. **RAM Log**: Backup log file stored in RAM **Flash Log**: Backup log files store in Flash.
Address Type	Specify TFTP server address type **Hostname**: Use domain name as server address. **IPv4**: Use IPv4 as server address **IPv6**: Use IPv6 as server address
Server Address	Specify TFTP server address.
Filename	Configuration image file name on remote TFTP server

15.3.2 Save Configuration

Click **Management** > **Configuration** > **Save Configuration**

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



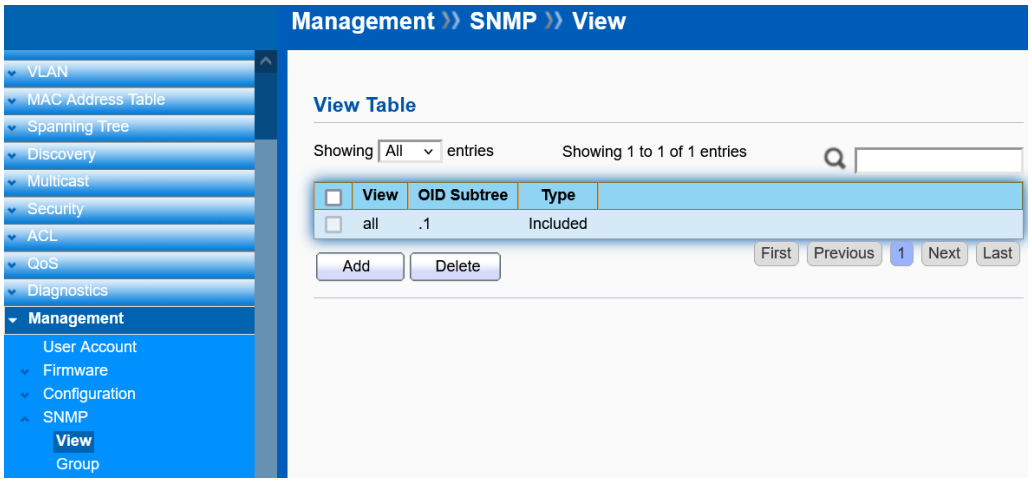
Field	Description
Source File	Source file types **Running Configuration**: Copy running configuration file to destination. **Startup Configuration**: Copy startup configuration file to destination. Backup Configuration: Copy backup configuration file to destination.
Destination File	Destination file **Startup Configuration**: Save file as startup configuration.

15.4 SNMP

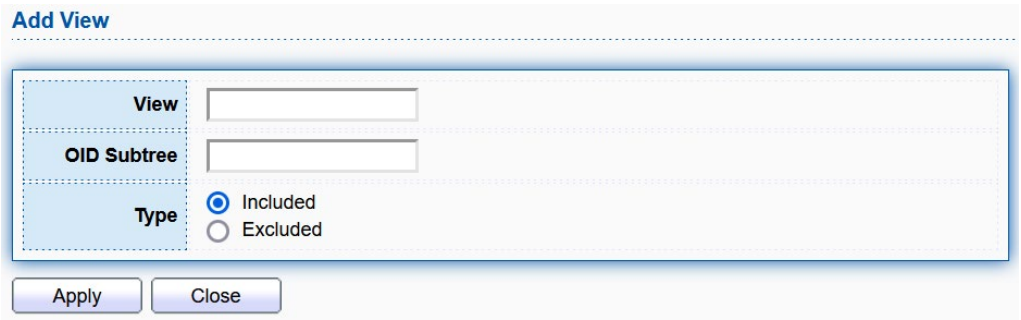
15.4.1 View

Click **Management** > **SNMP** > **View**

SNMP uses an extensible design, where the available information is defined by Management Information bases (MIBs). MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing Object Identifiers (OID) to organize themselves. Each OID identifies a variable that can be read or set via SNMP. The SNMP View List is created for the SNMP management station to manage MIB objects.



Click “**Add**” to add a new OID Subtree.

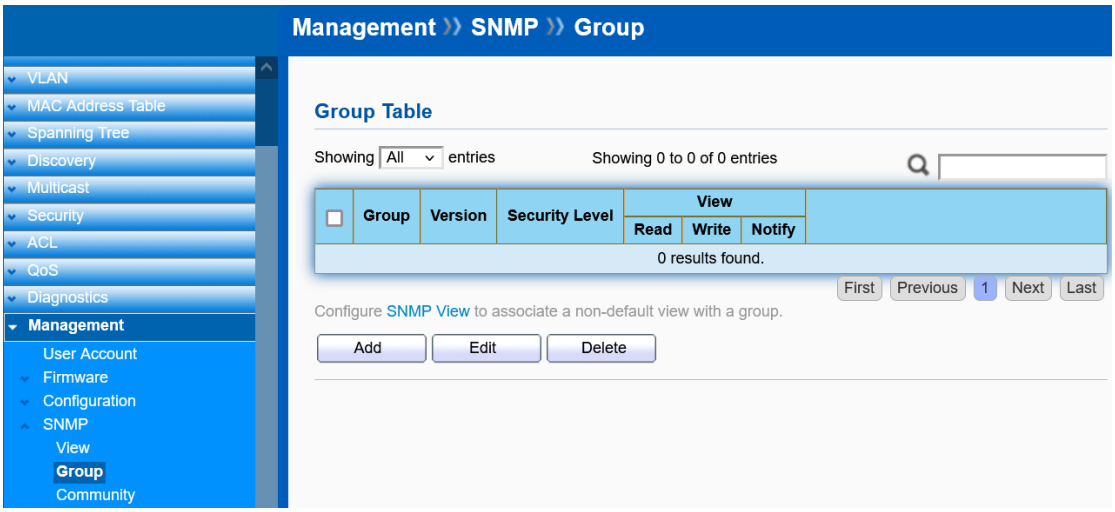


Field	Description
View	Enter the view name. The view name can contain up to 30 alphanumeric characters.
OID Subtree	Enter the Object Identifier (OID) Subtree. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager. Note that the first character must be a period (.). Wild cards can be used to mask a specific portion of the OID string using a period (.).
Type	Select whether the defined OID branch within MIB tree will be included or excluded from the selected SNMP view. Generally, if the view type of an entry is **Excluded**, another entry of view type **Included** should exist and its OID subtree should overlap the **Excluded** view entry.

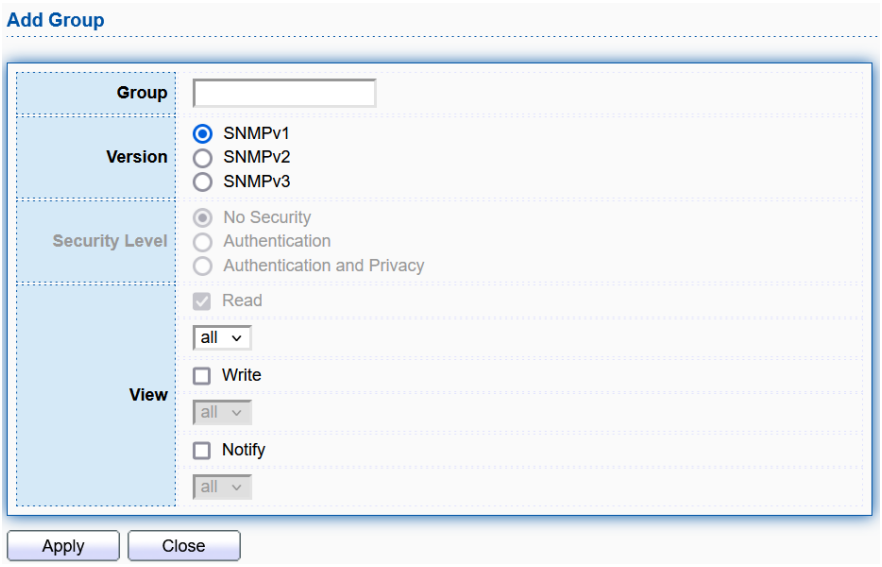
15.4.2 Group

Click **Management** > **SNMP** > **Group**

Configure SNMP Groups to control network access on the Switch by providing users in various groups with different management rights via the Read View, Write View, and Notify View options.



Click “**Add**” or “**Edit**” to add or edit a group.

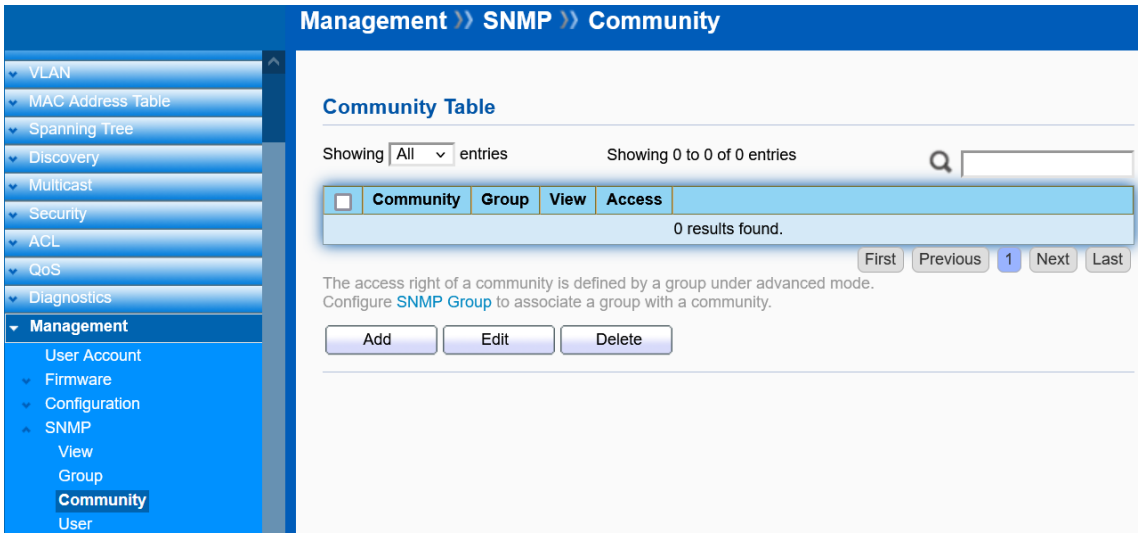


Field	Description
Group	Enter the group name that access control rules are applied to. The group name can contain up to 30 alphanumeric characters.
Version	Selects the SNMP version (v1, v2c, v3) associated with the group.
Security Level	Select the security level for the group. Security levels apply to SNMPv3 only. •**No Security** – Neither authentication nor the privacy security levels are assigned to the group. •**Authentication** – Authenticates SNMP messages. •**Authentication and Privacy** – Encrypts SNMP messages.
View	•**Read View**: Management access is restricted to read-only. •**Write View**: Select a SNMP to allow SNMP write privileges to the Switch’s SNMP agent. •**Notify View**: Select a SNMP group to receive SNMP trap messages generated by the Switch’s SNMP agent.

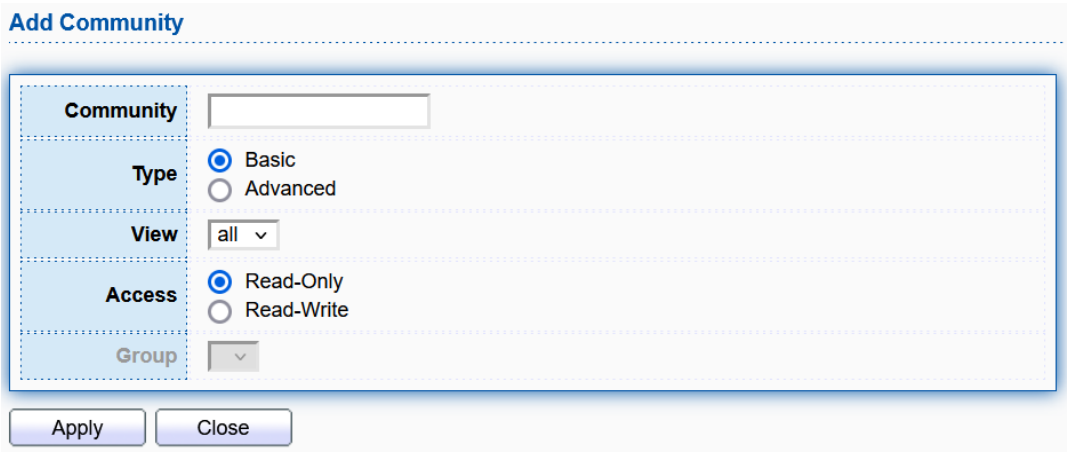
15.4.3 Community

Click **Management** > **SNMP** > **Community**

In SNMPv1 and SNMPv2c, user authentication is accomplished using types of passwords called Community Strings, which are transmitted in clear text and not supported by authentication. It is important to note that the community name can limit access to the SNMP agent from the SNMP network management station, functioning as a password.



Click "**Add**" or "**Edit**" to add or edit a community.



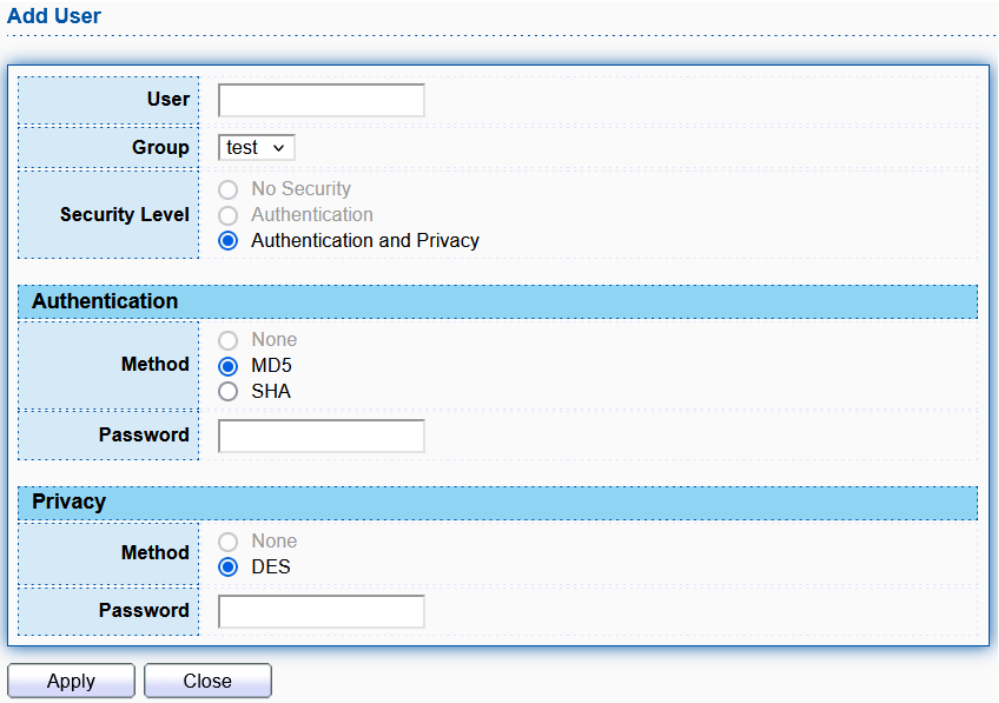
Field	Description
Community	The SNMP community name. Its maximum length is 20 characters.
Type	Select **Basic** or **Advance**. Select the **Advance** attached to the SNMP group.
View	Select the view name from a list.
Access Right	SNMP access mode **Read-Only**: Read only **Read-Write**: Read and Write.
Group	Select the SNMP group from a list.

15.4.4 User

Click **Management** > **SNMP** > **User**

Use the User page to create SNMP users for authentication with managers using SNMP v3 to associate them to SNMP groups. Click Add to add a new user.

Click “**Add**” or “**Edit**” to add or edit a user.



Field	Description
User	The SNMP user name. Its maximum length is 30 characters.
Group	Select the SNMP group from a list.
Security Level	Select the security level for the user. •**No Security** – Neither authentication nor the privacy security levels are assigned to the user. •**Authentication** – Authenticates SNMP messages. •**Authentication and Privacy** – Encrypts SNMP messages.
Authentication Field	
Method	Select the method used to authenticate users. •**MD5** – Using the HMACMD5 algorithm. •**SHA** – Using the HMACSHA-96 authentication level.

	Enter the SHA password and the HMAC-SHA-96 password to be used for authentication.
Password	Enter MD5 password and the HMAC-MD5-96 password to be used for authentication.
Privacy Field	
Method	Select the method used to authenticate users. •**None** – No user authentication is used. •**DES** – Using the Data Encryption Standard algorithm.
Password	Enter the Data Encryption Standard key.

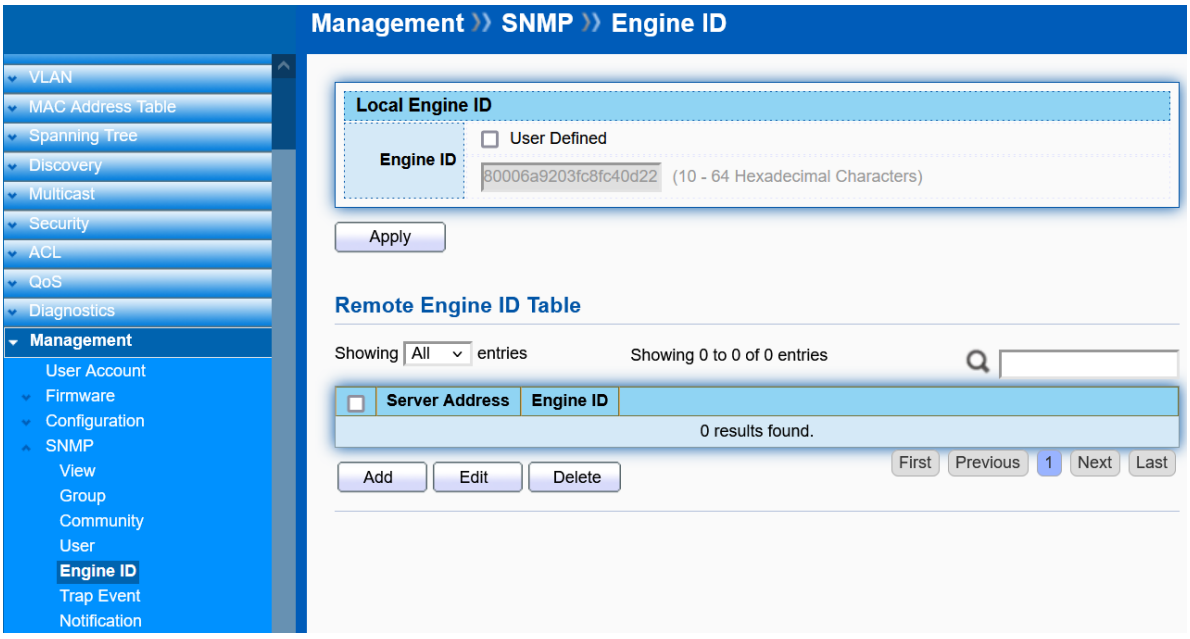
15.4.5 Engine ID

Click **Management** > **SNMP** > **Engine ID**

The Engine ID is only used by SNMPv3 entities to uniquely identify them. An SNMP agent is considered an authoritative SNMP engine. This means that the agent responds to incoming messages (Get, GetNext, GetBulk, Set), and sends trap messages to a manager.

Each SNMP agent maintains local information that is used in SNMPv3 message exchanges. The default SNMP Engine ID is comprised of the enterprise number and the default MAC address. The SNMP Engine ID must be unique for the administrative domain, so that no two devices in a network have the same Engine ID.

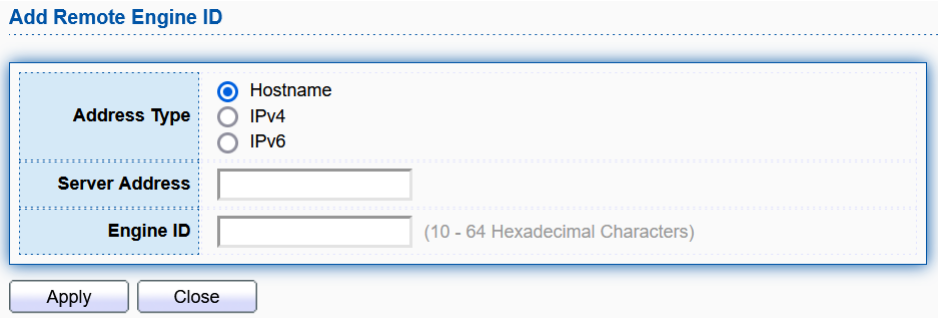
Local information is stored in four MIB variables that are read-only (snmpEngineId, snmpEngineBoots, snmpEngineTime, and snmpEngineMaxMessageSize).



Field	Description
Engine ID	**User Defined** – Enter the local device Engine ID. The field value is a hexadecimal string (range: 10 to 64). Each byte in the hexadecimal character strings is represented by two hexadecimal digits. The default Engine ID is based on the switch MAC address, and is defined per standard as: •First 4 octets – First bit = 1, the rest is the IANA enterprise number.

	•Fifth octet – Set to 3 to indicate the MAC address that follows. •Last 6 octets – MAC address of the switch.

Click “**Add**” or “**Edit**” to add or edit a remote Engine ID.



Field	Description
Server Address	Enter the IP address or domain name of the remote server that receives the traps
Engine ID	Enter the Engine ID.

15.4.6 Trap Event

Click **Management** > **SNMP** > **Trap Event**

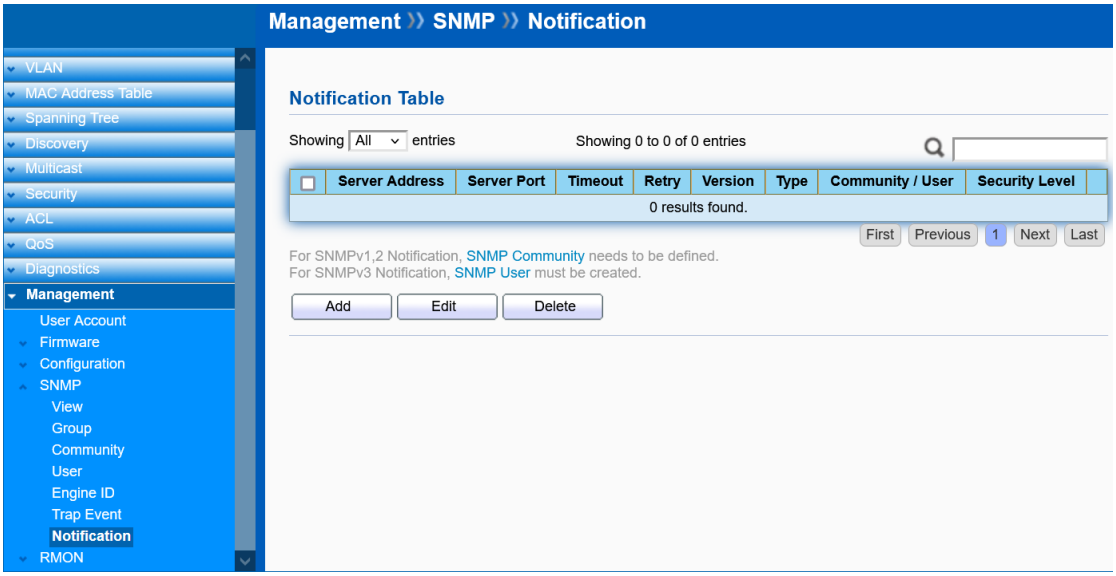
To display and configure the SNMP trap event.

Field	Description
Authentication Failure	SNMP authentication failure trap, when community not match or user authentication password not match.
Link Up/Down	Port link up or down trap.
Cold Start	Device reboot configure by user trap.
Warm Start	Device reboot by power down trap

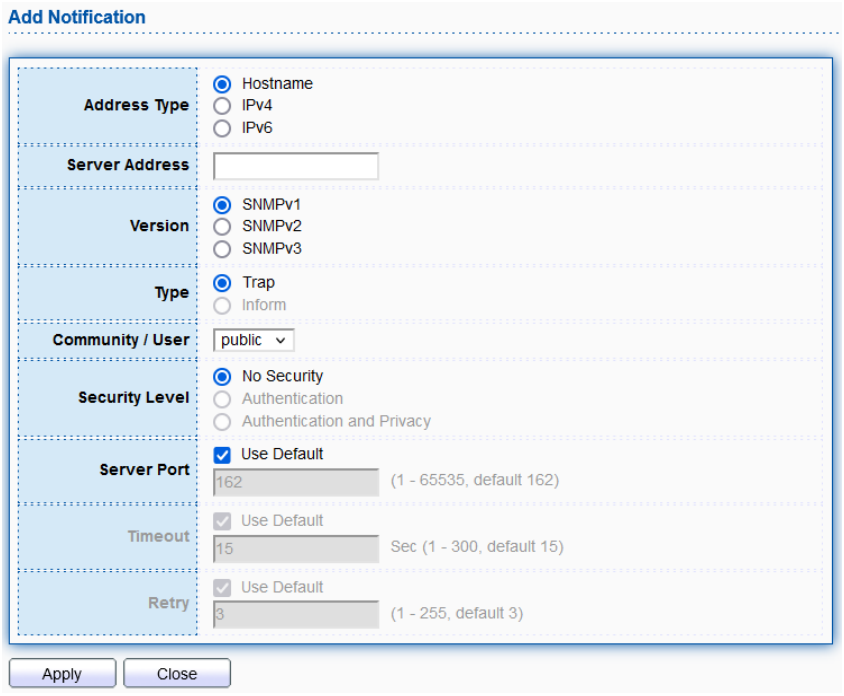
15.4.7 Notification

Click **Management** > **SNMP** > **Notification**

To configure the hosts to receive SNMP v1/v2/v3 notification.



Click “**Add**” or “**Edit**” to add or edit a host.



Field	Description
Server Address	IP address or the hostname of the SNMP trap recipients.
Version	Specify SNMP notification version.
Type	Notification Type **Trap**: Send SNMP traps to the host. **Inform**: Send SNMP informs to the host.
Community	SNMP community name for notification.
Security Level	Select the security level for the host. Security level apply to SNMPv3 only. •**No Security** – Neither authentication nor the privacy security levels are assigned to the group. •**Authentication** – Authenticates SNMP messages. •**Authentication and Privacy** – Encrypts SNMP messages.

Server Port	Enter the UDP port used to send notifications. The default is 162.
Timeout	Configurable only if the notify type is Informs. Enter the amount of time the device waits before re-sending. The default is 15 seconds.
Retry	Configurable only if the notify type is Informs. Enter the amount of time the device waits before re-sending an inform request. The default is 3 times.

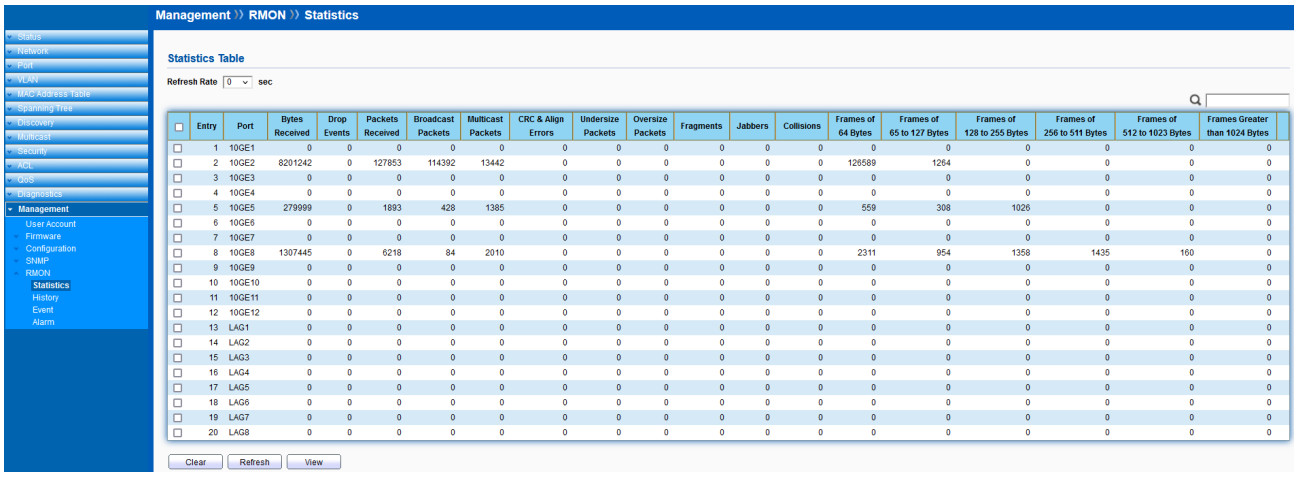
15.5 RMON

Remote Network Monitoring or RMON is used for support monitoring and protocol analysis of LANS by enabling various network monitors and console systems to exchange network-monitoring data through the Switch.

15.5.1 Statistics

Click **Management** > **RMON** > **Statistics**

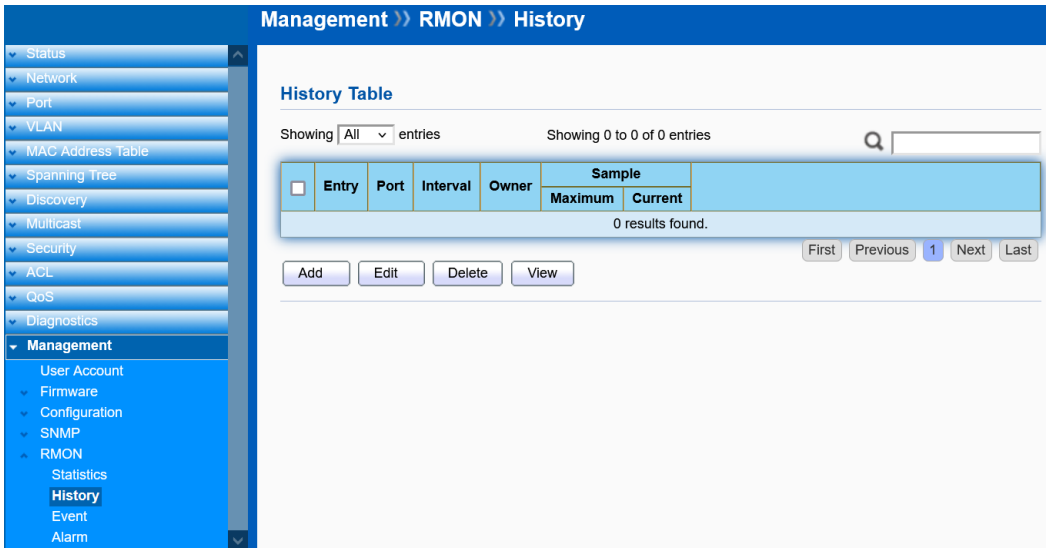
To display RMON statistics.



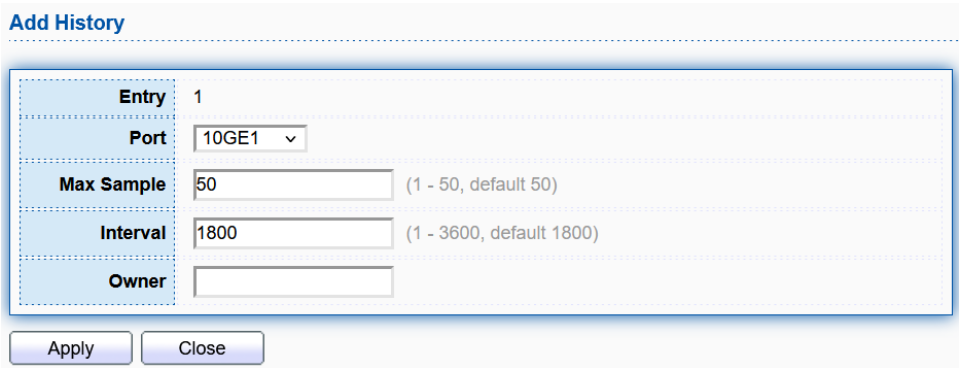
15.5.2 History

Click **Management** > **RMON** > **History**

The RMON History contains information about samples of data taken from the ports.



Click “**Add**” or “**Edit**” to add or edit a history.

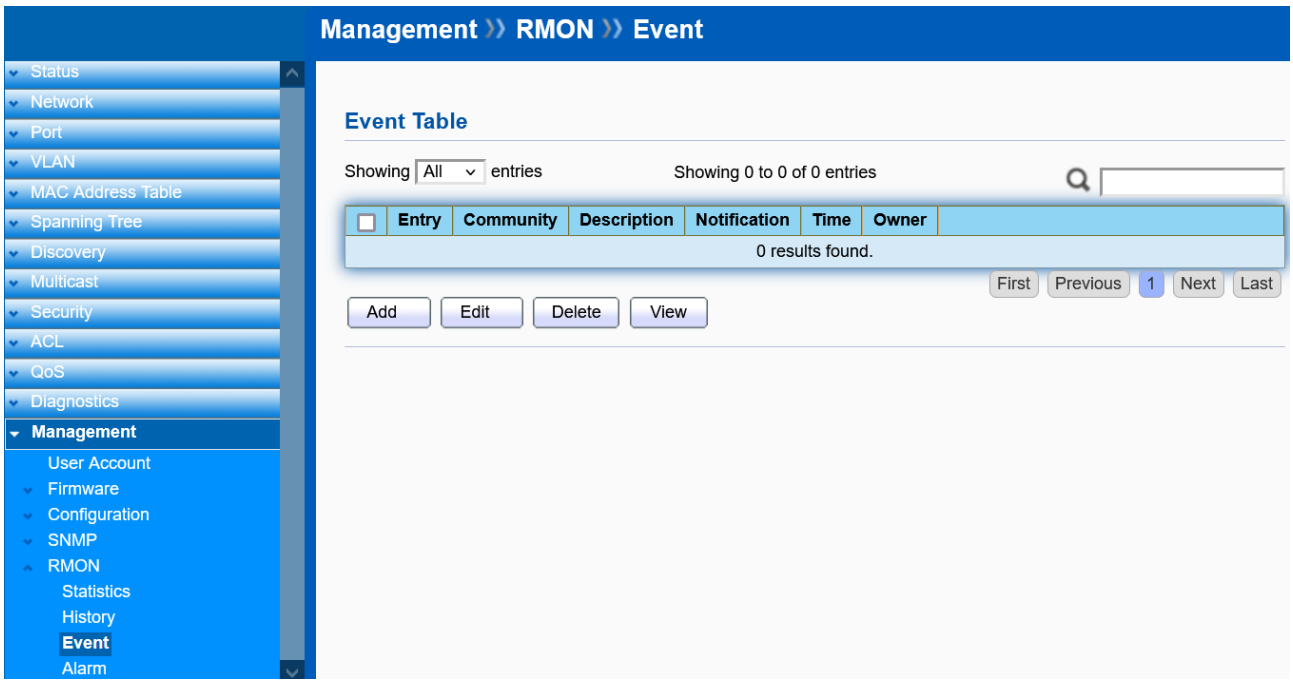


Field	Description
Entry	The entry number for History.
Port	Select the port from which the history samples were taken.
Max Sample	Enter the number of samples to be saved. The range is from 1- 50.
Interval	Enter the time that samples are taken from the ports. The field range is from 1-3600.
Owner	Enter the RMON user that requested the RMON information. The range is from 0-32 characters.

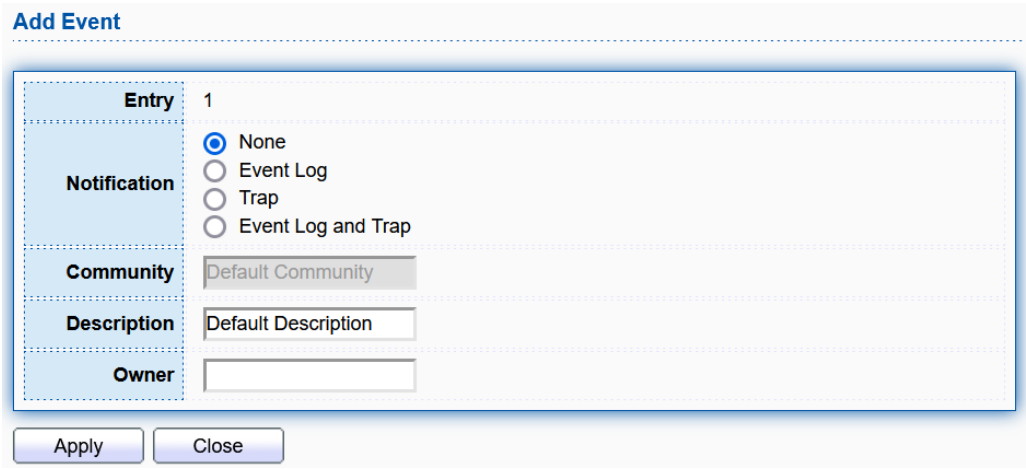
15.5.3 Event

Click **Management** > **RMON** > **Event**

The Event page defines RMON events on the Switch.



Click "**Add**" or "**Edit**" to add or edit an event.

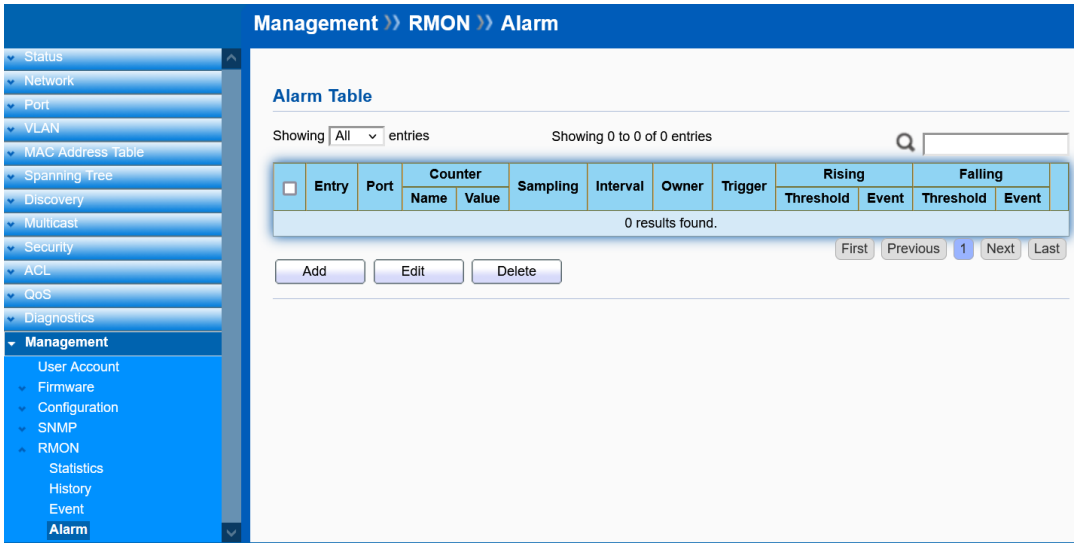


Field	Description
Entry	The entry number for Event.
Notification	Select the event type. •**Event Log** – The event is a log entry. •**Trap** – The event is a trap. •**Event Log and Trap** – The event is both a log entry and a trap.
Community	Enter the community to which the event belongs.
Description	Displays the number of good broadcast packets received on the interface.
Owner	Enter the switch that defined the event.

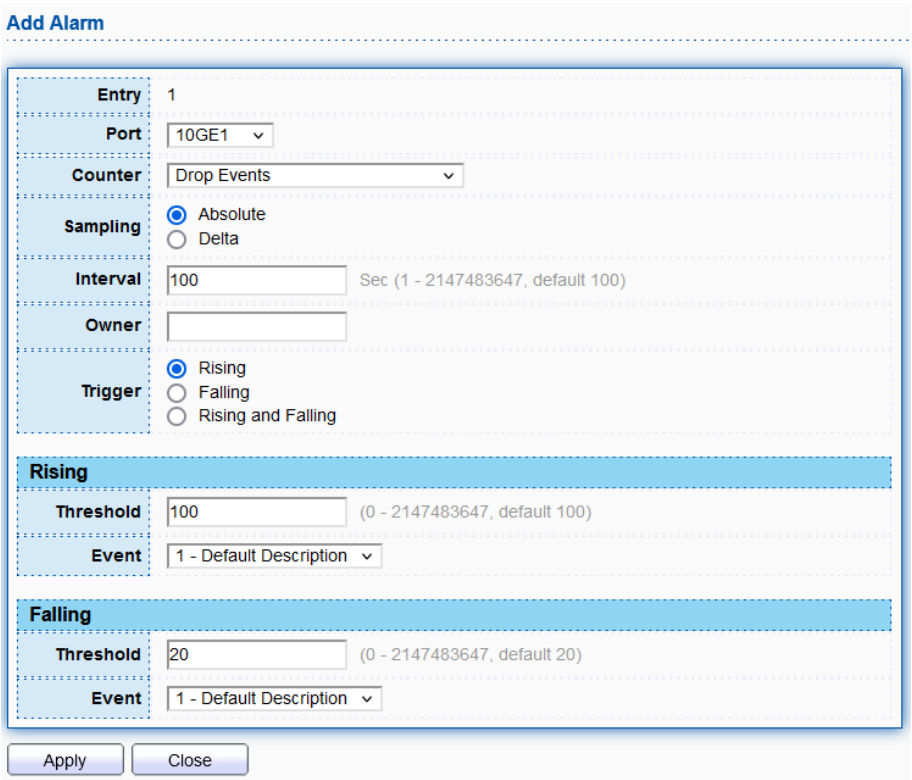
15.5.4 Alarm

Click **Management** > **RMON** > **Alarm**

You can configure Network alarms to occur when a network problem is detected. Choose your preferences for the alarm from the drop-down boxes.



Click "**Add**" or "**Edit**" to add or edit an alarm.



Field	Description
Entry	The entry number for Alarm.
Port	Select the port from which the alarm samples were taken.
Counter	Select the variable of samples for the specified alarm sample.
Sampling	Select the sampling method for the selected variable and comparing the value against the thresholds. •**Absolute** – Compares the values with the thresholds at the end of the sampling interval. •**Delta** – Subtracts the last sampled value from the current value.
Interval	Enter the alarm interval time.
Owner	Enter the Switch that defined the alarm.

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 Field	
Threshold	Enter the rising number that triggers the rising threshold alarm.
Event	Select the event number by the rising alarm is reported.
Falling Field	
Threshold	Enter the rising number that triggers the falling threshold alarm.
Event	Select the event number by the falling alarm is reported.