SILVERNET
WIRELESS-NETWORK-SOLUTIONS

LAYER 3 RACK MOUNT MANAGED SWITCHES WITH 10G SFP+

SIL 54424MP

SIL 716E8C4M

SIL 516S8C4M & SIL 716S8C4M

Configuration Manual

TABLE OF CONTENTS

Introduction

The SilverNet Layer 3 Rack Mount Managed Switches are reliable, high performance, high specification and cost effective Managed switches suitable for all network operations. The SilverNet Layer 3 Rack Mount Managed Switches are fully compliant (PoE models only) with the IEEE802.3af/at standard, providing Power-over-Ethernet over twisted pair cables. The fibre optics ports feature a modular SFP+ slot for any kind of MSA-compliant pluggable 10Gbps SFP transceiver.

Support Products

This manual covers all 5 & 7 Series products listed below:

- 716E8C4M
- 716S8C4M
- 54424MP
- 516S8C4M

For more information, visit http://www.silvernet.com

System Requirements

• Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10, Linux, or Mac OS X

• Web Browser: Mozilla Firefox, Apple Safari, Google Chrome, or Microsoft Edge

Packing List

Please check the following items in the package before installing the device

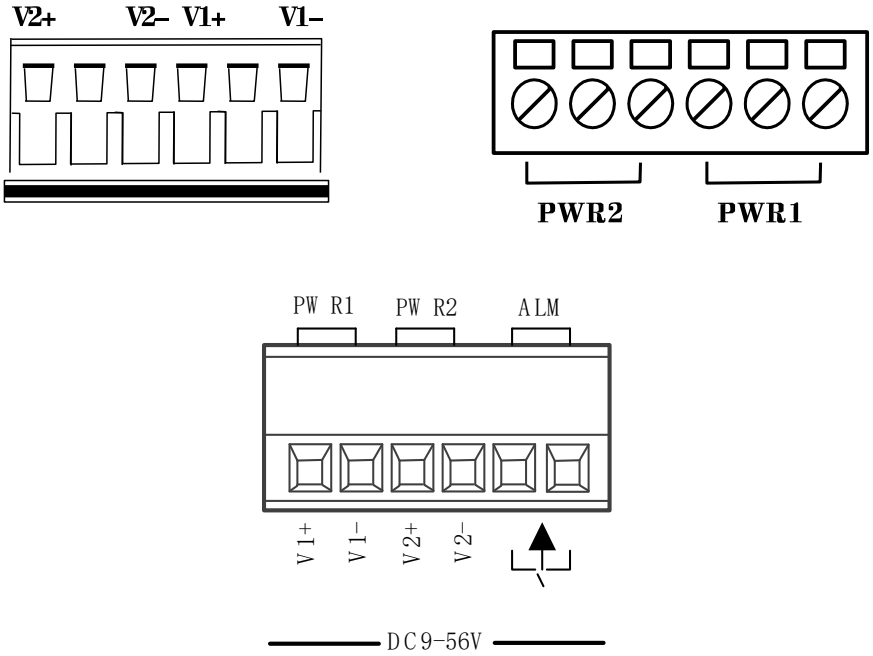
Network Switch	1 piece
Quick Start Guide	1 copy
Rack Mount Kit	1 copy
Serial Cable	1 piece

Please contact your distributor immediately for any missing or damaged items.

POWER

The input terminal of the switch is for 6 PIN plug type terminals, V1+ and V1- is for power supply 1 (PWR1), V2 + and V2- is for power supply 2 (PWR2) and GND for the earthing terminal, as shown in image below.

The input voltage range for power 1 and power 2 is 12VDC ~ 56VDC, V1+, and V2+ are positive, V1- and V2- are negative.



The switch can be powered by two power supplies simultaneously allowing the switch to continue functioning even if one of the power supplies fails.

Note*

For the **SIL 716E8C4M** please use power supply **SIL MDR 60-48**

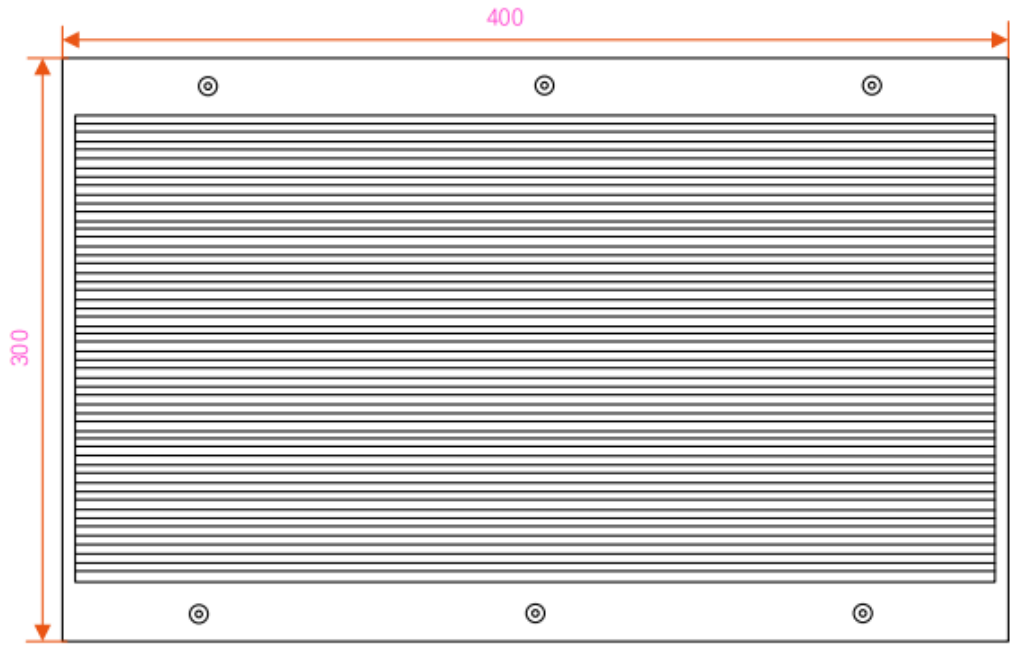
For the **SIL 716S8C4M** please use power supply **SIL MDR 60-48**

For the **SIL 54424MP** the power cable is included.

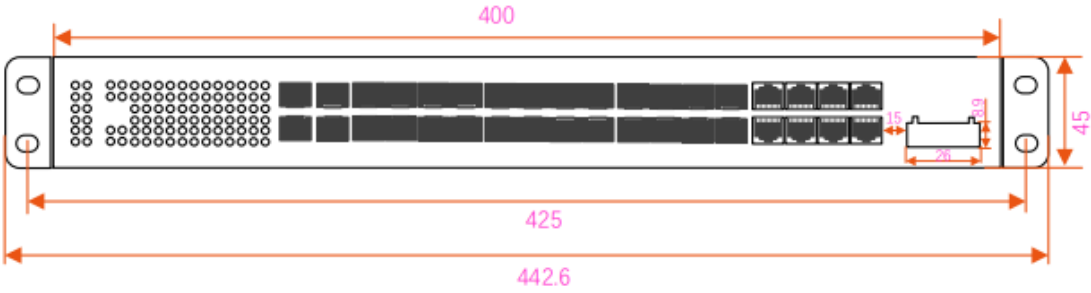
For the **SIL 516S8C4M** the power cable is included.

PRODUCT DIMENSION

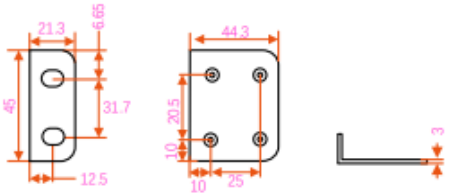
SIL 716E8C4M & SIL 716S8C4M



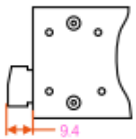
Top View



Front View



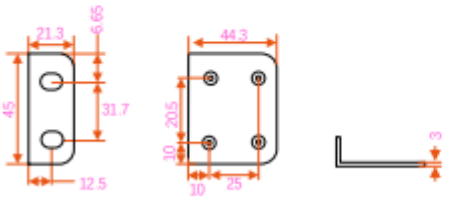
Rack Mount Kit



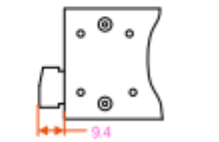
(Side View)
Height of projections

SIL 54424MP

Top View

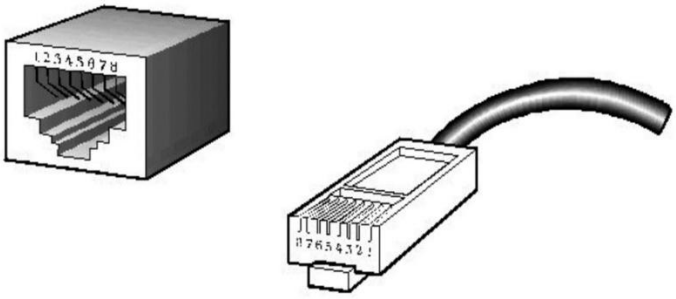


Rack Mount Kit



(Side View)
Height of projections

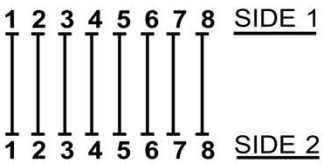
COPPER CABLE CONNECTION



STANDARD RJ45 CONNECTOR

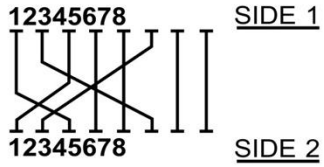
There are 8 wires on a standard UTP/STP cable, and each wire is colour coded. The following shows the pin allocation and colour of a straight through cable and crossover cable:

Straight Cable



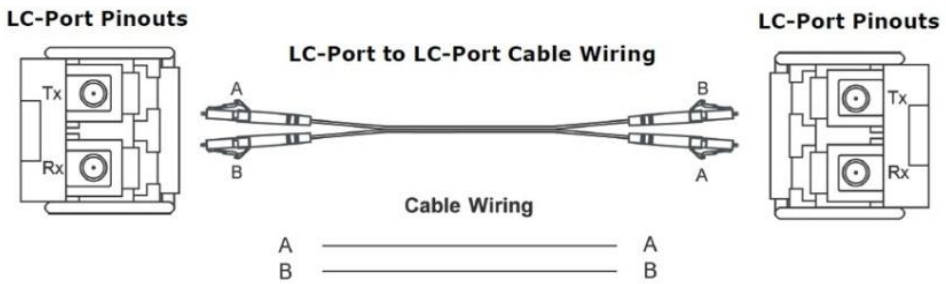
SIDE 1	SIDE 2
1 = White/Orange	1 = White/Orange
2 = Orange	2 = Orange
3 = White/Green	3 = White/Green
4 = Blue	4 = Blue
5 = White/Blue	5 = White/Blue
6 = Green	6 = Green
7 = White/Brown	7 = White/Brown
8 = Brown	8 = Brown

Cross Over Cable



SIDE 1	SIDE 2
1 = White/Orange	1 = White/Green
2 = Orange	2 = Green
3 = White/Green	3 = White/Orange
4 = Blue	4 = Blue
5 = White/Blue	5 = White/Blue
6 = Green	6 = Orange
7 = White/Brown	7 = White/Brown
8 = Brown	8 = Brown

FIBRE CABLE CONNECTION

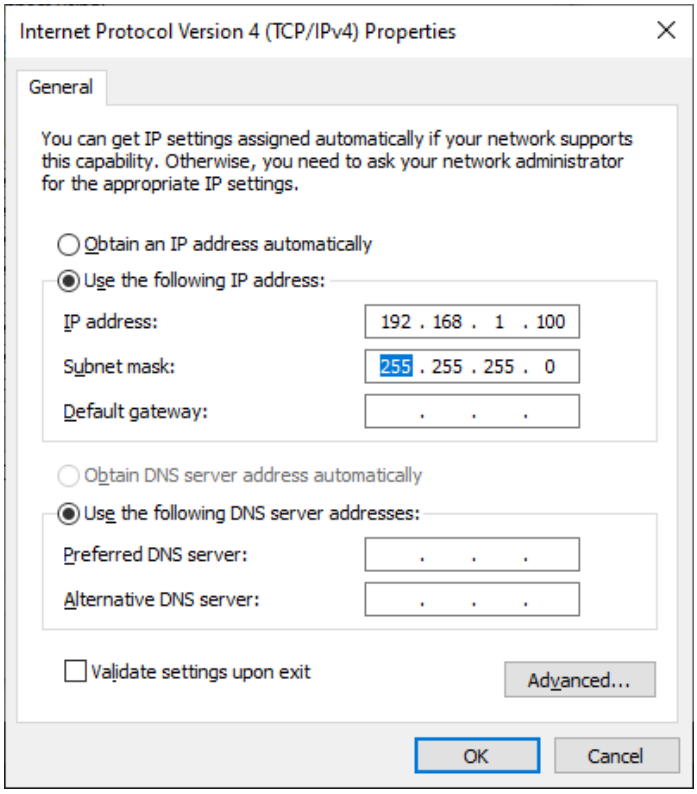


CONFIGURATION

GETTING STARTED

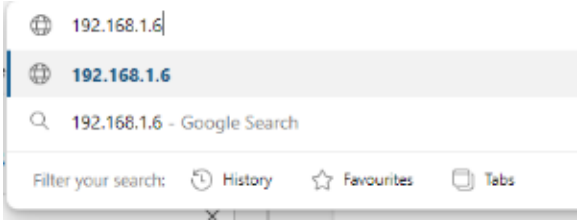
To access the equipment management interface, perform the following steps:

1. Configure the Ethernet adapter on your computer with a static IP address on the 192.168.1.x subnet (for example, IP address: 192.168.1.100 and subnet mask: 255.255.255.0



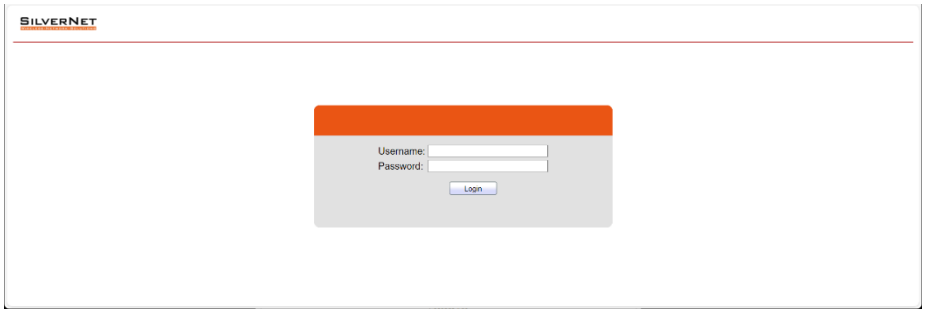
2. Launch your web browser and enter the default IP address of your device in the address field.

Series 5 and 7 Switches have an IP address of 192.168.1.6



If the unit has been reset, it will go to the default IP address of 192.168.1.6. You will need to change your Ethernet adapter IP address to 192.168.1.x subnet.

3. Enter **admin** in the Username field and **admin** in the Password field and click **Login**.

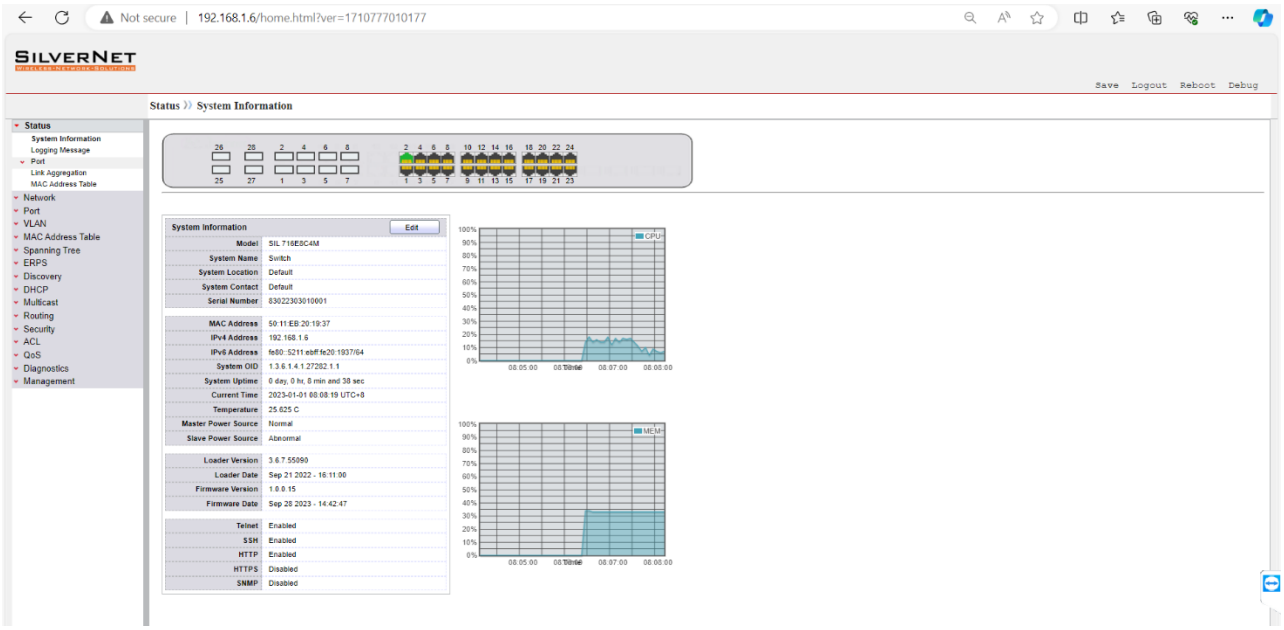


STATUS

Use the status page to view key system information.

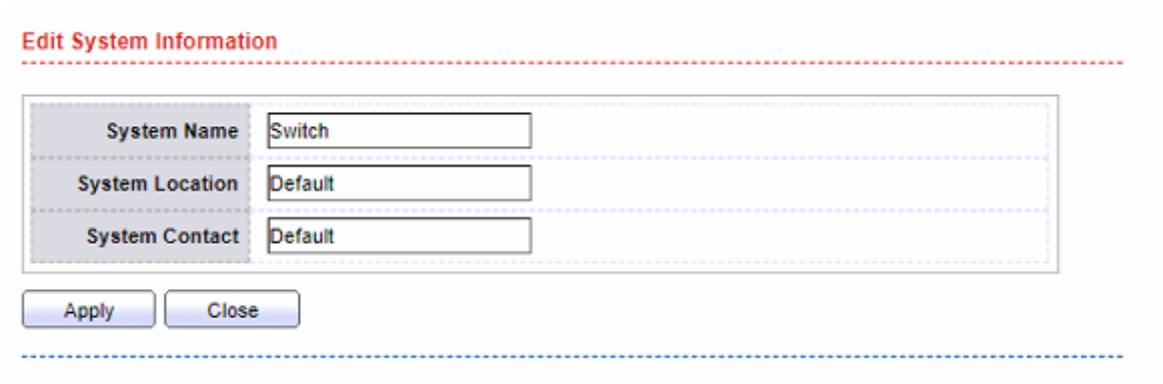
SYSTEM INFORMATION

This page shows key information such as the device model, IP address, Uptime, Temperature and Firmware version. It will also allow you to edit the System name, System location and System Contact details.



Field	Description
Model	Model name of the switch
System Name	System name of the switch.
System Location	Location information of the switch
System Contact	Contact information of the switch
MAC Address	Base MAC address of the switch
IPv4 Address	Current system IPv4 address
IPv6 Address	Current system IPv6 address
System OID	SNMP system object ID
System Uptime	Total elapsed time from booting
Current Time	Current system time
Loader Version	Boot loader image version
Loader Date	Boot loader image build date
Firmware Version	Current running firmware image version
Firmware Date	Current running firmware image build date
Telnet	Current Telnet service enable/disable state
SSH	Current SSH service enable/disable state
HTTP	Current HTTP service enable/disable state
HTTPS	Current HTTPS service enable/disable state
SNMP	Current SNMP service enable/disable state

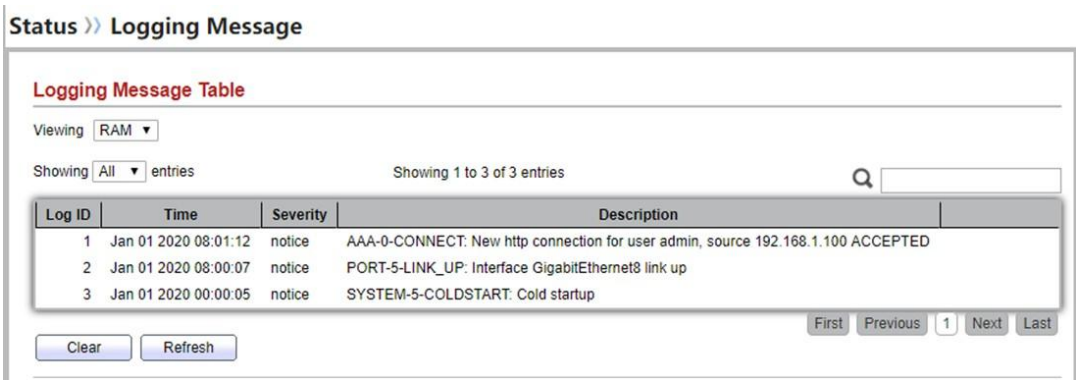
Click the “Edit” button on the table title to edit following system information.



Field	Description
System Name	System name of the switch.
System Location	Location information of the switch
System Contact	Contact information of the switch

LOGGING MESSAGE

Displays logging messages stored in RAM and Flash.



Field	Description
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.

Figure 2.2 Logging Message fields

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.

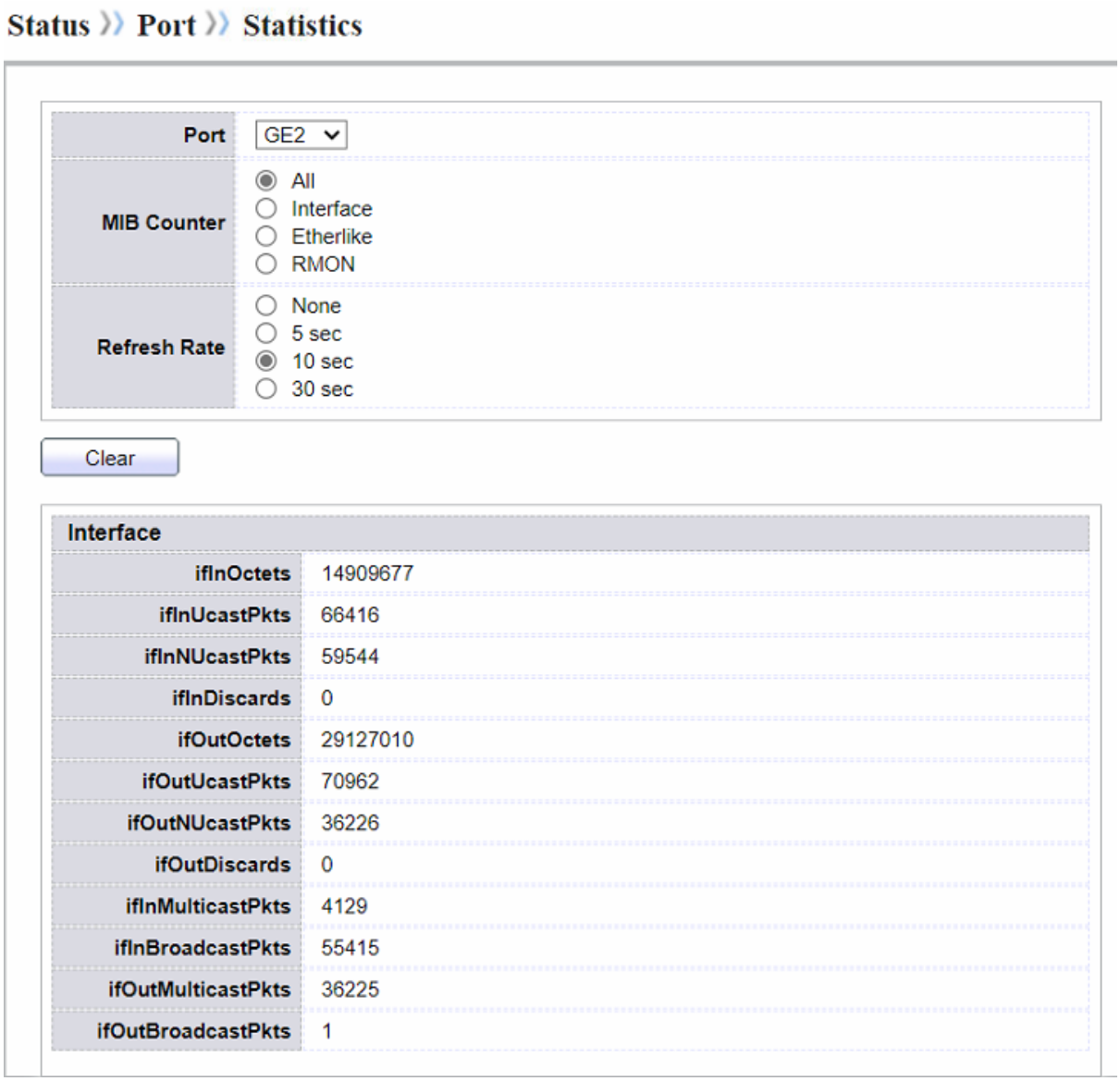
PORT

Displays the port summary and status information.

STATISTICS

This page displays standard counters on network traffic form the Interfaces.

The “Clear” button will clear MIB counter of current selected port.



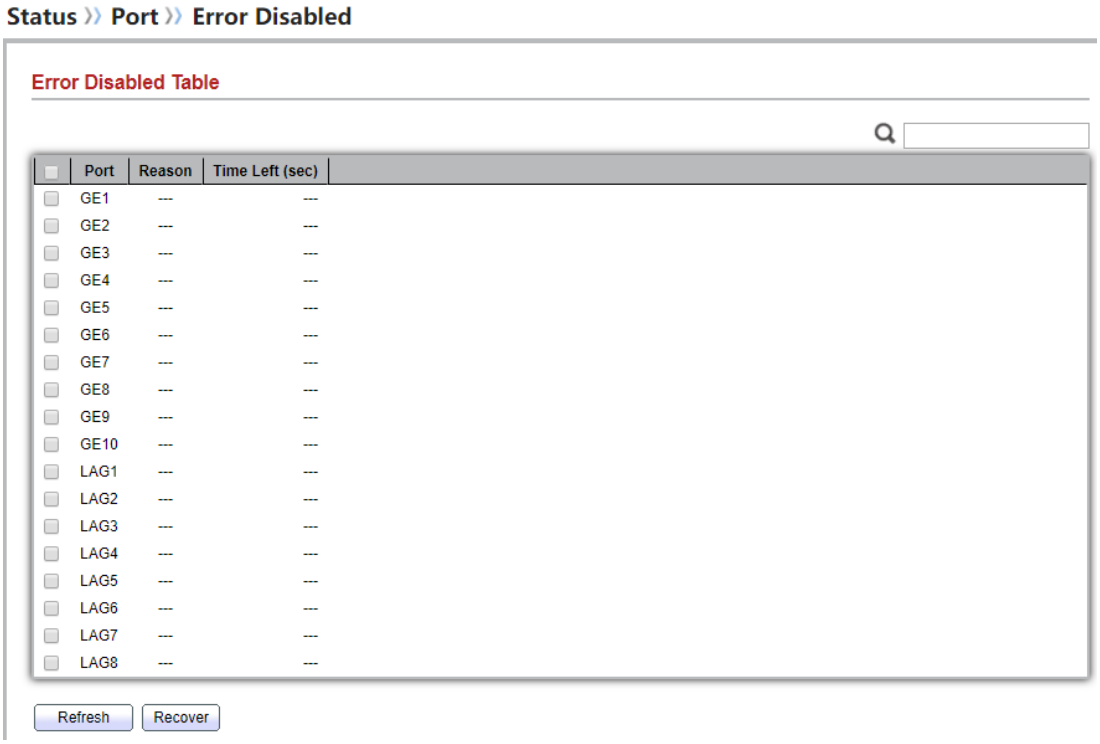
Etherlike	
dot3StatsAlignmentErrors	0
dot3StatsFCSErrors	0
dot3StatsSingleCollisionFrames	0
dot3StatsMultipleCollisionFrames	0
dot3StatsDeferredTransmissions	0
dot3StatsLateCollisions	0
dot3StatsExcessiveCollisions	0
dot3StatsFrameTooLongs	0
dot3StatsSymbolErrors	0
dot3ControlInUnknownOpcodes	0
dot3InPauseFrames	0
dot3OutPauseFrames	0

RMON	
etherStatsDropEvents	0
etherStatsOctets	14930559
etherStatsPkts	126137
etherStatsBroadcastPkts	55490
etherStatsMulticastPkts	4137
etherStatsCRCAlignErrors	0
etherStatsUnderSizePkts	0
etherStatsOverSizePkts	0
etherStatsFragments	0
etherStatsJabbers	0
etherStatsCollisions	0
etherStatsPkts64Octets	97003
etherStatsPkts65to127Octets	14260
etherStatsPkts128to255Octets	2283
etherStatsPkts256to511Octets	209
etherStatsPkts512to1023Octets	12382
etherStatsPkts1024to1518Octets	0

Field	Description
Port	Select one port to show counter statistics
MIB Counter	Select the MIB counter to show different counter type. • All: All counters. • Interface: Interface related 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 information of the specified port

ERROR DISABLED

Displays the status of the Errors on specified ports.

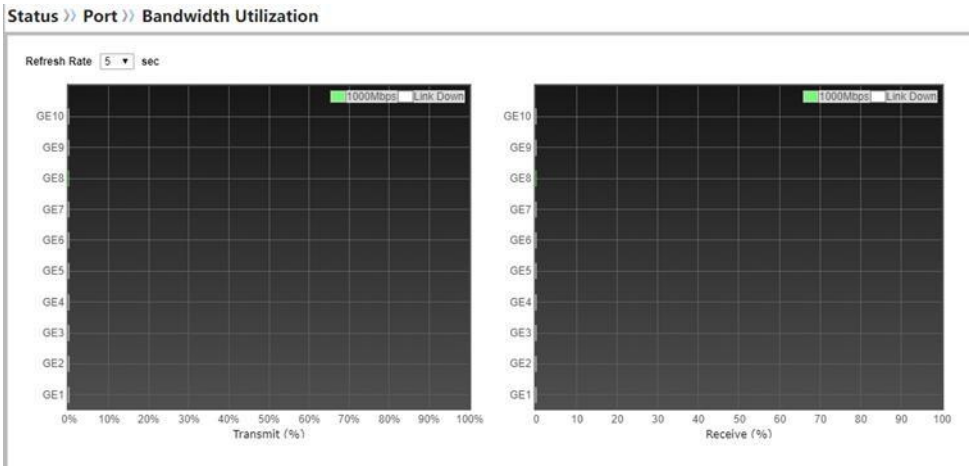


Field	Description
Port	Interface or port number.
Reason	Port will be disabled by one of the following error reason: • BPDU Guard • UDLD • Broadcast Flood • Unknown Multicast Flood • Unicast Flood • ACL

	• Port Security Violation • DHCP rate limit • ARP rate limit
Time Left (sec)	The time left in second for the error recovery.

BANDWIDTH UTILISATION

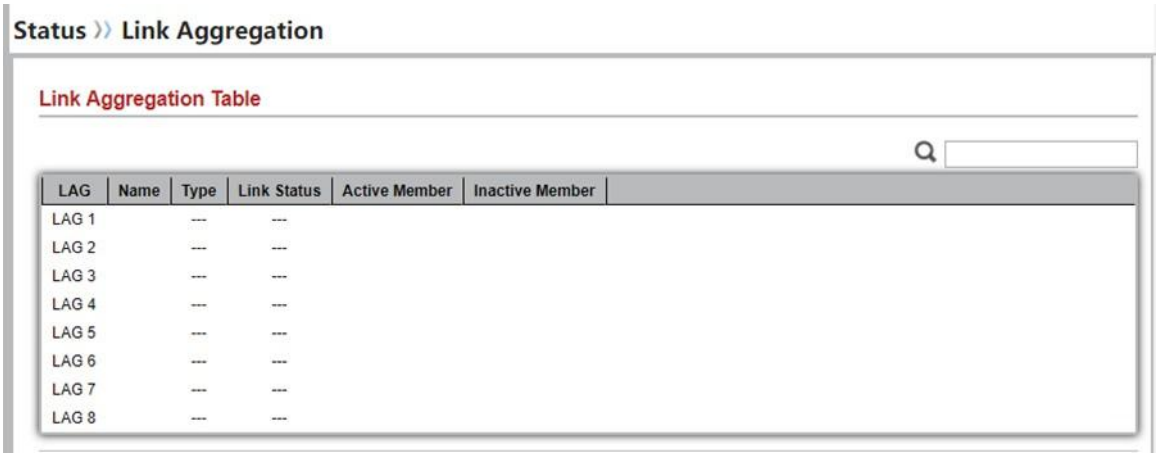
Displays the bandwidth utilisation in real-time. This page will refresh automatically every few seconds.



Field	Description
Refresh Rate	Refresh the web page every X amount of seconds to get new bandwidth utilisation data.

LINK AGGREGATION

Displays the link aggregation status page.

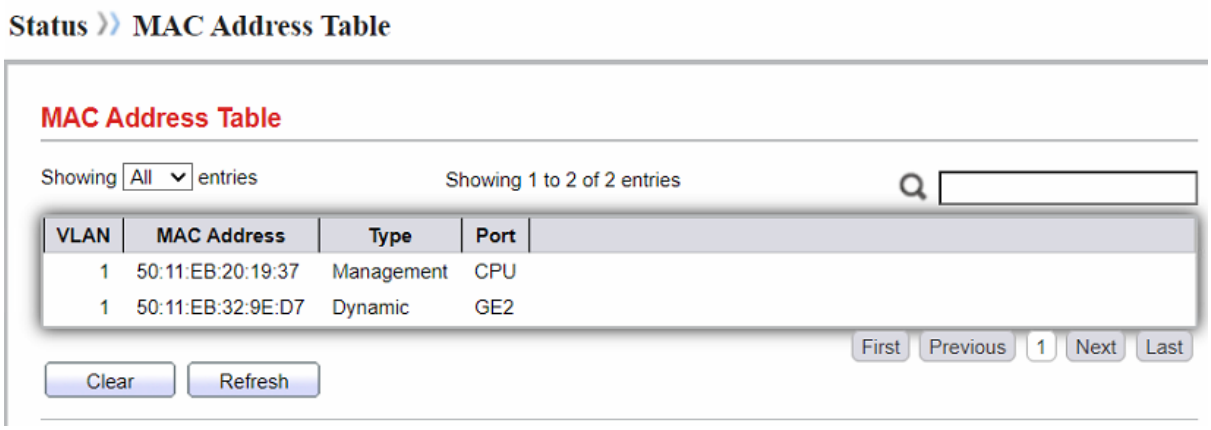


Field	Description
LAG	Interface or port number.
Name	LAG port description.
Type	The type of LAG • Static: The group of ports assigned to a static LAG are always active members. • LACP: The group of ports assigned to dynamic LAG are candidate ports. LACP determines which candidate ports are active member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

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 the “Refresh” button will retrieve latest MAC address entries and show them on page.

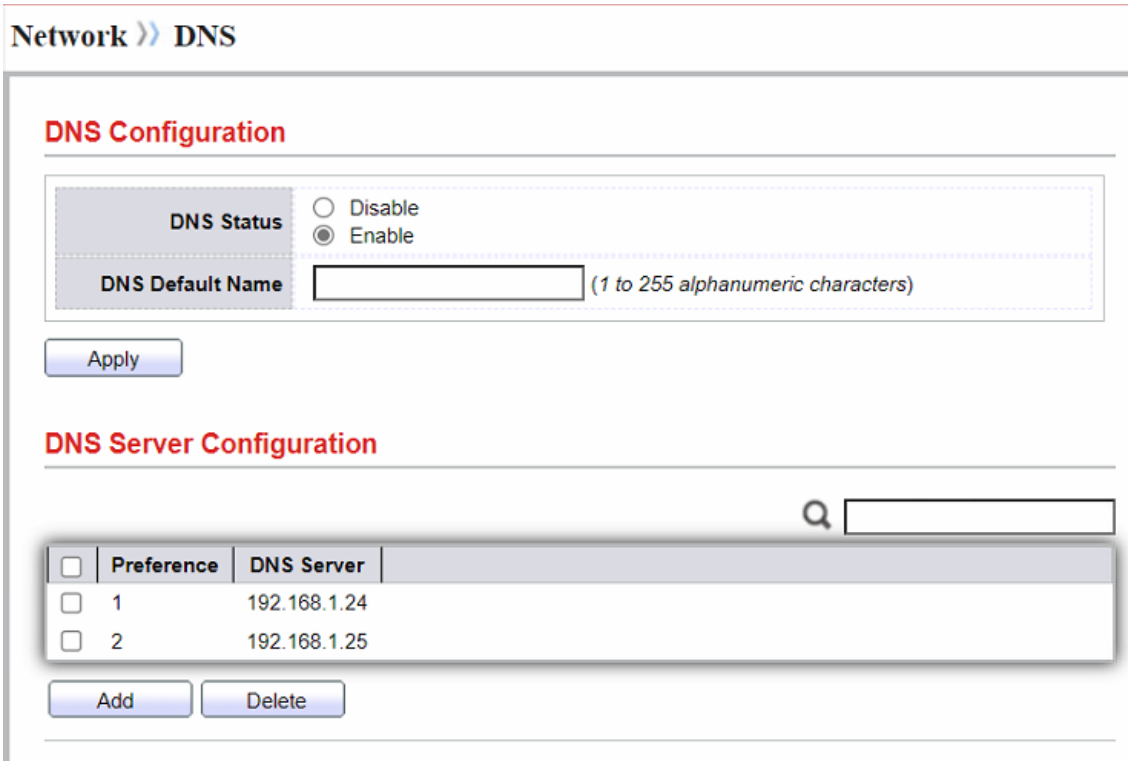


Field	Description
VLAN	VLAN ID of the mac address
MAC Address	MAC address
Type	The type of MAC address • **Management**: Base MAC address for management purpose. • **Static:** Manually configured by administrator. • **Dynamic**: Auto learned by hardware.
Port	LAG port link status

NETWORK

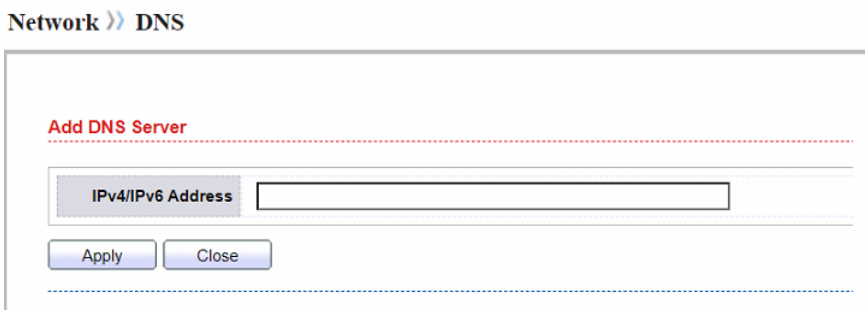
Use the Network pages to configure settings such as, DNS and System Time.

DNS

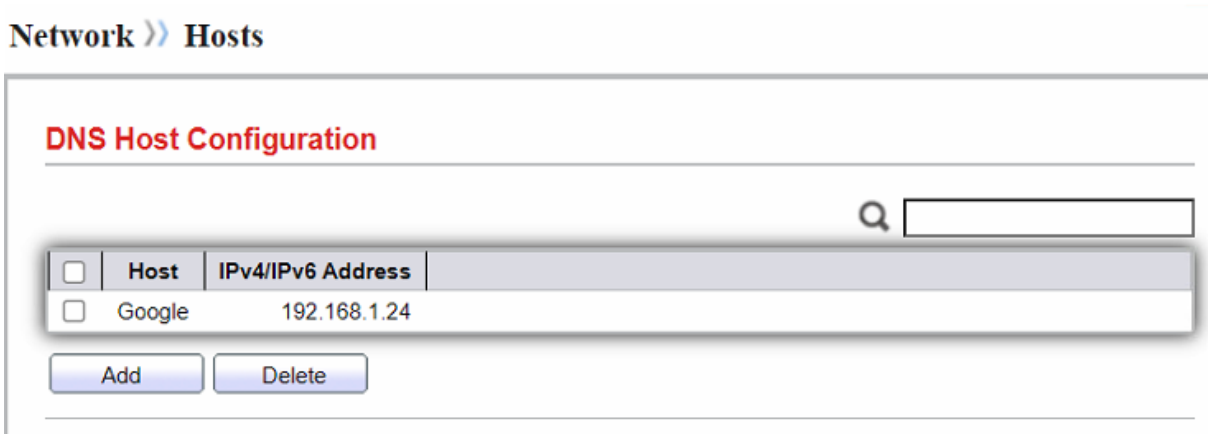


Field	Description
DNS Status	Disable or Enable DNS.
DNS Default Name	Enter DNS default name
Preference	Order of DNS Server.
DNS Server	IPv4/IPv6 Address of DNS Server.

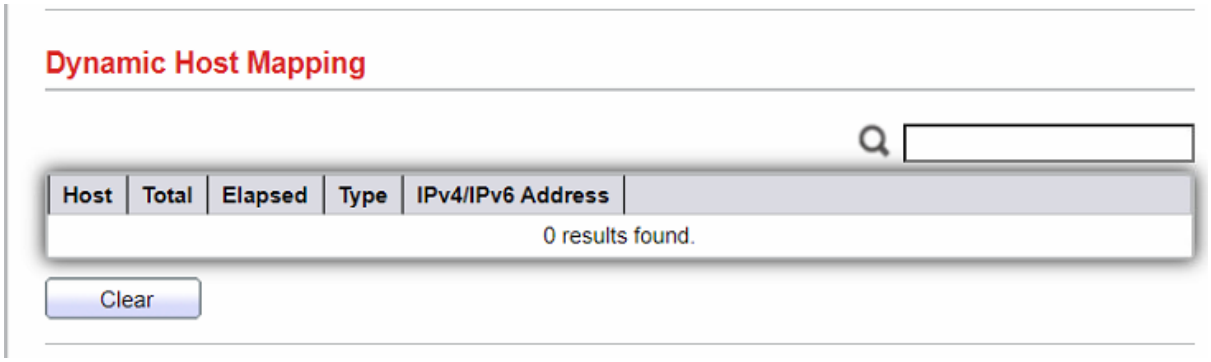
To Add a DNS Server “click” the add button.



Hosts



Field	Description
Host	Disable or Enable DNS.
IPv4/IPv6 Address	Enter DNS default name



Field	Description
Host	
Total	
Elapsed	
Type	
IPv4/IPv6 Address	

SYSTEM TIME

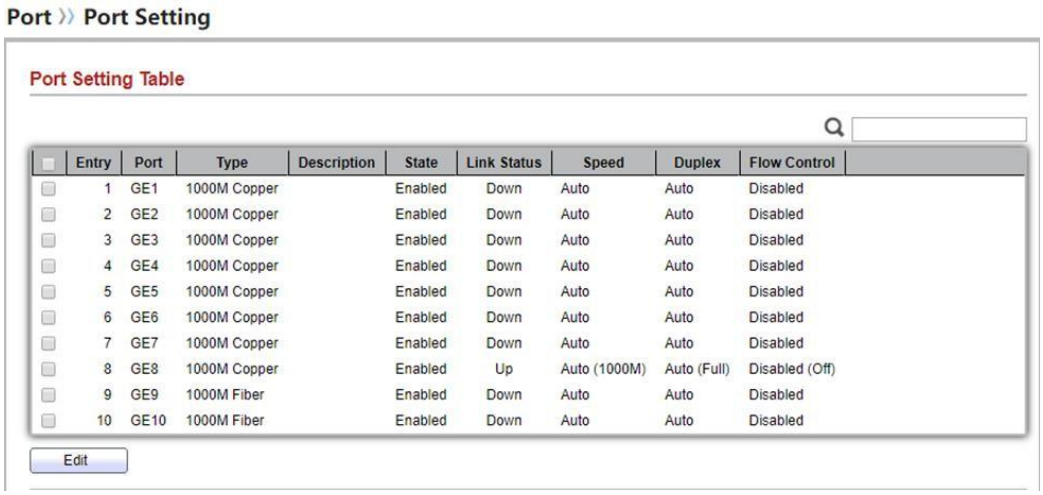
Use this page to configure the time and SNTP server.

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	Description
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	Description
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	Description
Type	Select the mode of daylight-saving time. • **Disable:** Disable daylight-saving time. • **Recurring:** Using recurring mode of daylight-saving time. • **Non-Recurring:** Using non-recurring mode of daylight-saving time. • **USA:** Using daylight saving time in the United States that starts on the second Sunday of March and ends on the first Sunday of November. • **European:** Using daylight saving time in the Europe that starts on the last Sunday in March and ending on the last Sunday in October.
Offset	Specify the adjust offset of daylight-saving time.
Recurring From	Specify the starting time of recurring daylight-saving time. This field available when selecting “Recurring” mode.
Recurring To	Specify the ending time of recurring daylight-saving time. This field available when selecting “Recurring” mode.
Non-recurring from	Specify the starting time of non-recurring daylight-saving time. This field available when selecting “non-recurring” mode.
Non-recurring to	Specify the ending time of recurring daylight-saving time. This field available when selecting “non-recurring” mode.

PORT

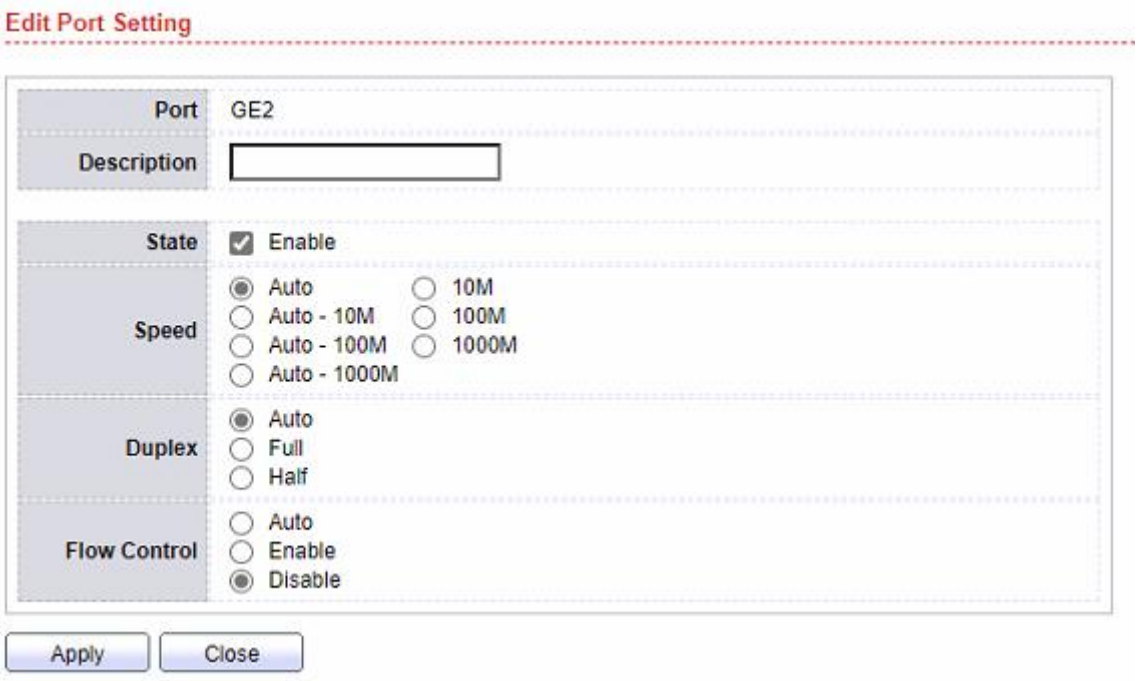
Use these pages to configure settings for port related features.

PORT SETTING



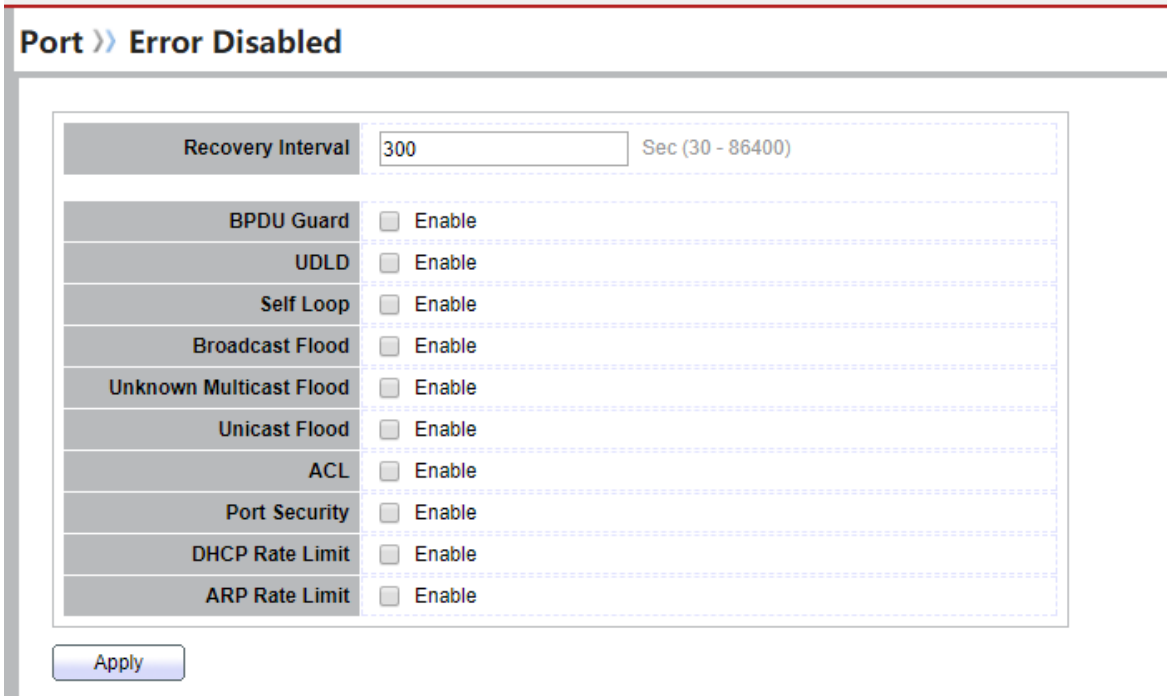
Field	Description
Port	Port Name
Type	Port media type
Description	Port description
State	Port admin state. • Enabled: Enable the port. • Disabled: Disable the port.
Link Status	Current port link status • Up: Port is link up • Down: Port is link down
Speed	Current port speed configuration and link speed status
Duplex	Current port duplex configuration and link duplex status
Flow Control	Current port flow control configuration and link flow control

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



Field	Description
Port	Shows the port currently selected
Description	Port description
State	Port admin state. • Enabled: Enable the port. • Disabled: Disable the port.
Speed	Port speed. • **Auto:** Auto negotiates the port speed. • **Auto-10M**: Auto negotiates the port speed up to 10M • **Auto-100M:** Auto negotiates the port speed up to 100M • **Auto-1000M:** Auto negotiates the port speed up to 1000M • **Auto-10M/100M:** Auto speed with 10M/100M abilities • **10M:** Force port speed to 10M • **100M:** Force port speed to 100M • **1000M:** Force port speed to 1000M
Duplex	Port duplex speed. • **Auto:** Auto duplex mode • **Half**: Sets the port to half duplex mode • **Full:** Sets the port to full duplex mode
Flow Control	Port flow control. • **Auto:** Auto negotiates flow control • **Enabled**: Enable flow control • **Disabled:** Disable flow control

ERROR DISABLED

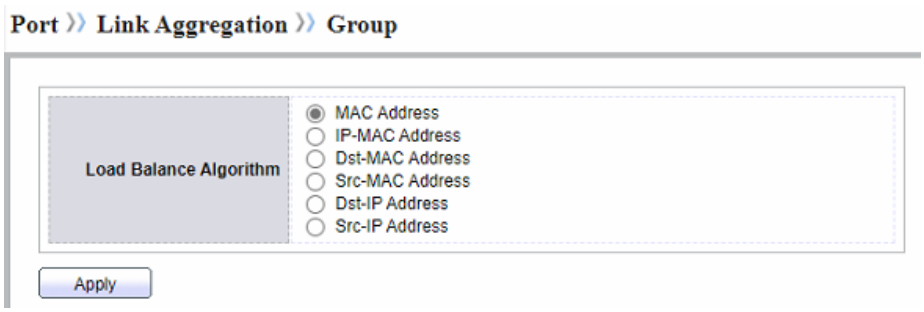


Field	Description
Recover Interval	Auto recovery after this interval for error disabled port.
BPDU Guard	Enable to auto shutdown the port when BPDU Guard error occurs.
UDLD	Enable to auto shutdown the port when UDLD violation occurs.
Self-Loop	Enable to auto shutdown the port when a Self-Loop error occurs.
Broadcast Flood	Enable to auto shutdown the port when a Broadcast Flood error occurs. This error is caused by the broadcast rate exceeding the broadcast storm control rate.
Unknown Multicast Flood	Enable to auto shutdown the port when an Unknown Multicast Flood error occurs. This error is caused by unknown multicast rate exceeding the unknown multicast storm control rate.
Unicast Flood	Enable to auto shutdown the port when a Unicast Flood error occurs. This error is caused by the unicast rate exceeding the unicast storm control rate.
ACL	Enable to auto shutdown the port when ACL shutdown port error occurs. This error is caused when a packet matches the ACL shutdown port action.
Port Security	Enable to auto shutdown the port when a Port Security Violation error occurs. This is caused by violation of the port security rules.
DHCP Rate Limit	Enable to auto shutdown the port when DHCP rate limit error occurs. This is caused by DHCP packet rate exceeding the DHCP rate limit.
ARP Rate Limit	Enable to auto shutdown the port when ARP rate limit reason occur. This reason caused by DHCP packet rate exceed ARP rate limit.

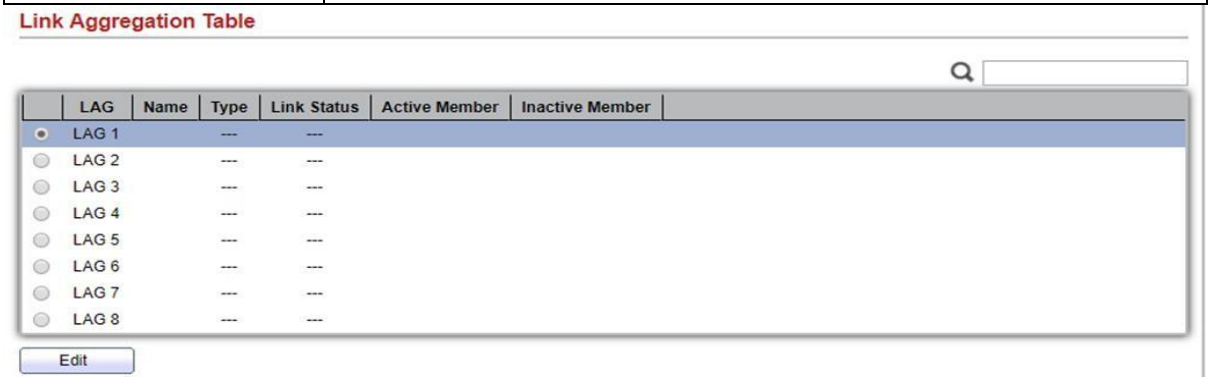
LINK AGGREGATION

GROUP

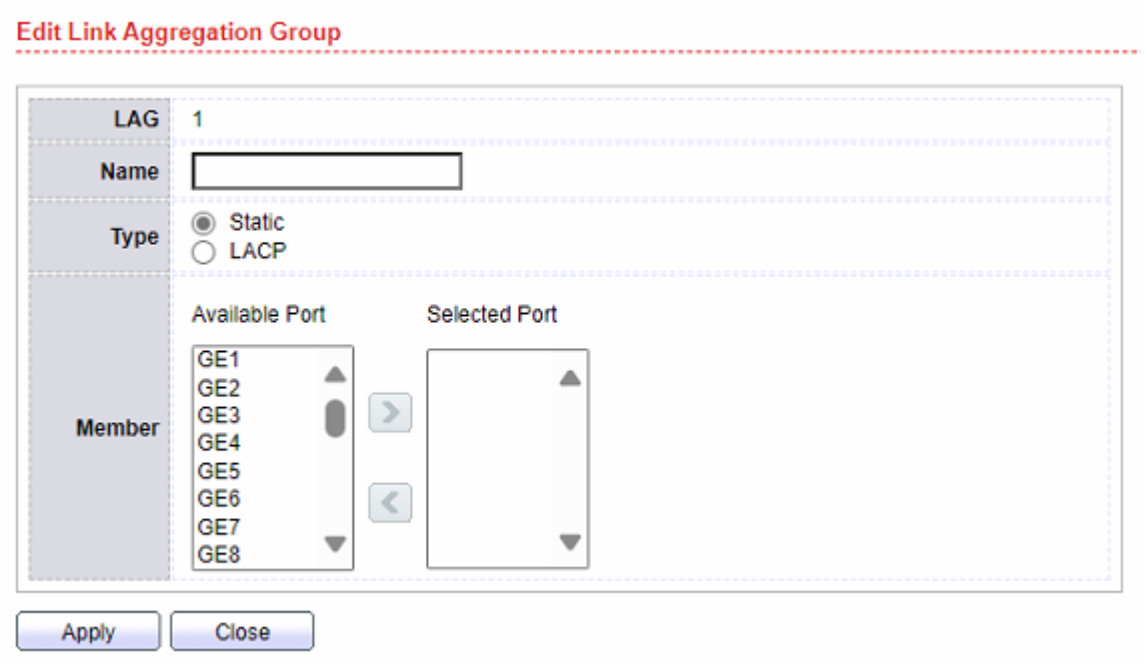
This page allows you to configure link aggregation groups, LAG and group members.



Field	Description
Load Balance Algorithm	• **MAC Address:** Based on MAC address. • **IP-MAC Address:** Based on IP address & MAC address. • **Dst-MAC Address:** Based on destination MAC address. • **Src-MAC Address:** Based on source MAC address. • **Dst-IP Address:** Based on destination IP address. • **Src-IP Address:** Based on source IP address.



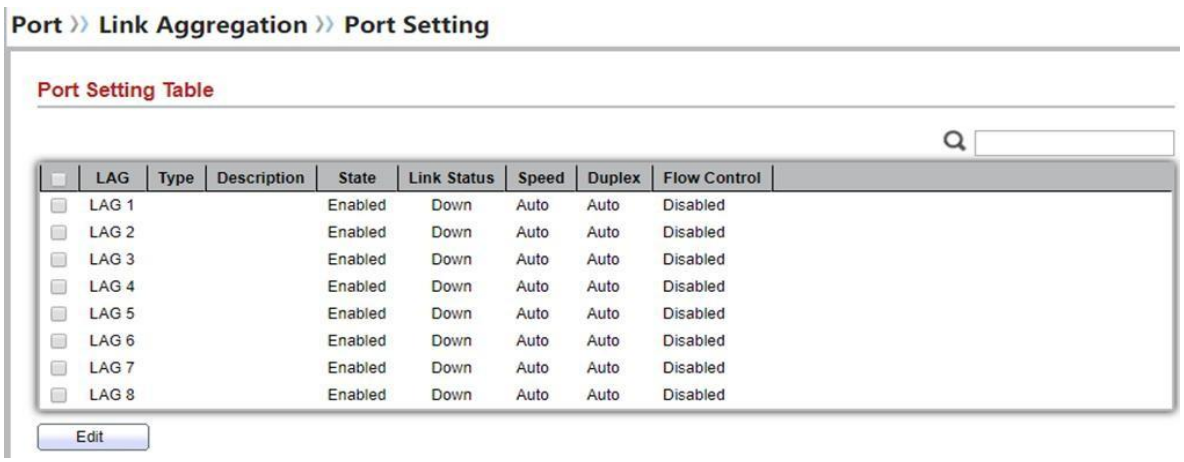
Field	Description
LAG	LAG Name
Name	LAG port description
Type	The type of the LAG • **Static:** The group of ports assigned to a static LAG are always active members. • **LACP:** The group of ports assigned to dynamic LAG are candidate ports. LACP determines which candidate ports are active member ports.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



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

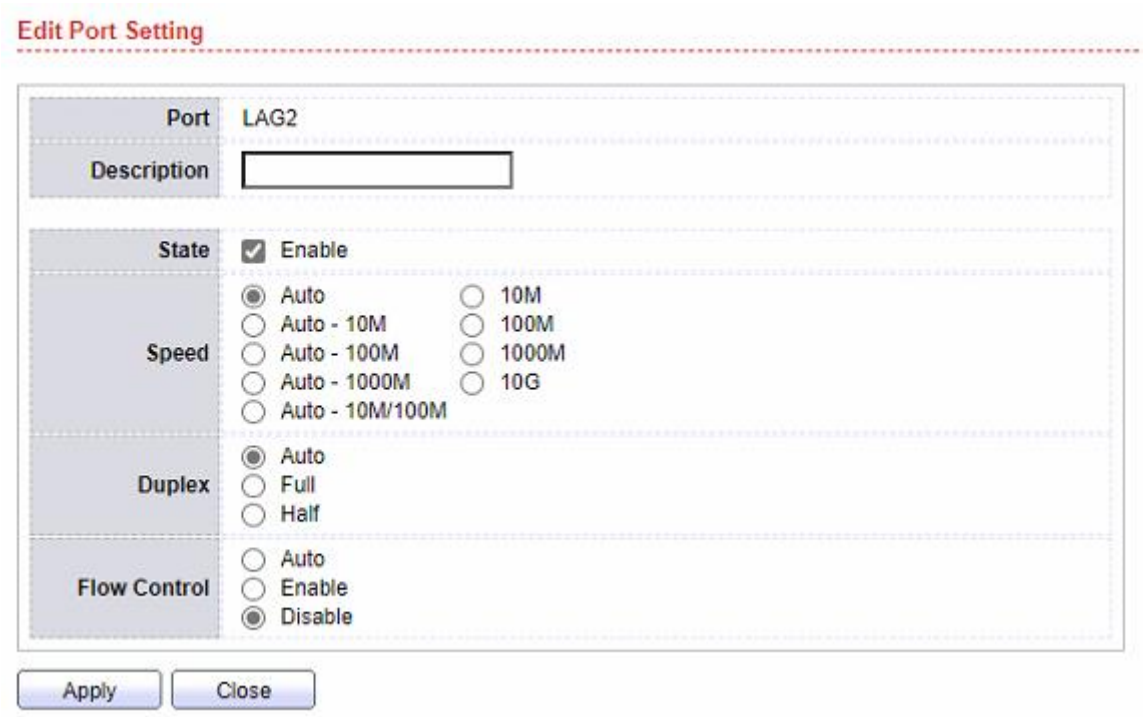
PORT SETTING

This page shows the current status of the LAG port and allows you to edit LAG port configurations. Select LAG entry and click the "Edit" button to edit the configuration.



Field	Description
LAG	LAG Name
Type	LAG port media type
Description	LAG Port description
State	LAG Port admin state. • **Enabled:** Enable the port. • **Disabled:** Disable the port.
Link Status	Curent 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 entry and click the “Edit” button to edit port configuration.



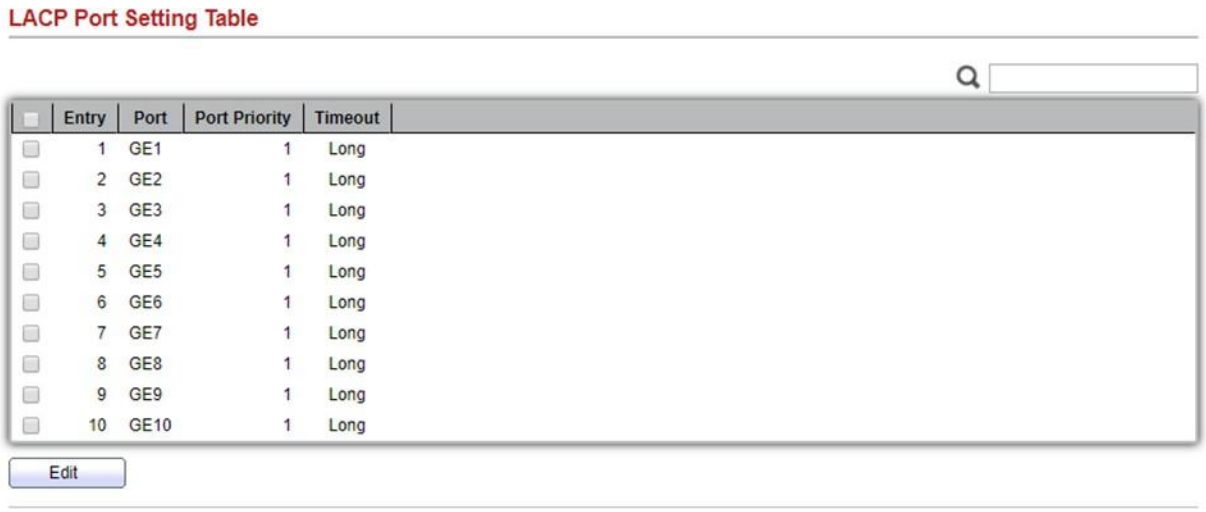
Field	Description
Port	Shows the port currently selected
Description	Port description
State	Port admin state. • Enabled: Enable the port. • Disabled: Disable the port.
Speed	Port speed. • **Auto:** Auto negotiates the port speed.

	• **Auto-10M**: Auto negotiates the port speed up to 10M • **Auto-100M:** Auto negotiates the port speed up to 100M • **Auto-1000M:** Auto negotiates the port speed up to 1000M • **Auto-10M/100M:** Auto speed with 10M/100M abilities • **10M:** Force port speed to 10M • **100M:** Force port speed to 100M • **1000M:** Force port speed to 1000M • **10G:** Force port speed to 10G
Duplex	Port duplex speed. • **Auto:** Auto duplex mode • **Half**: Sets the port to half duplex mode • **Full:** Sets the port to full duplex mode
Flow Control	Port flow control. • **Auto:** Auto negotiates flow control • **Enabled**: Enable flow control • **Disabled:** Disable flow control

LACP

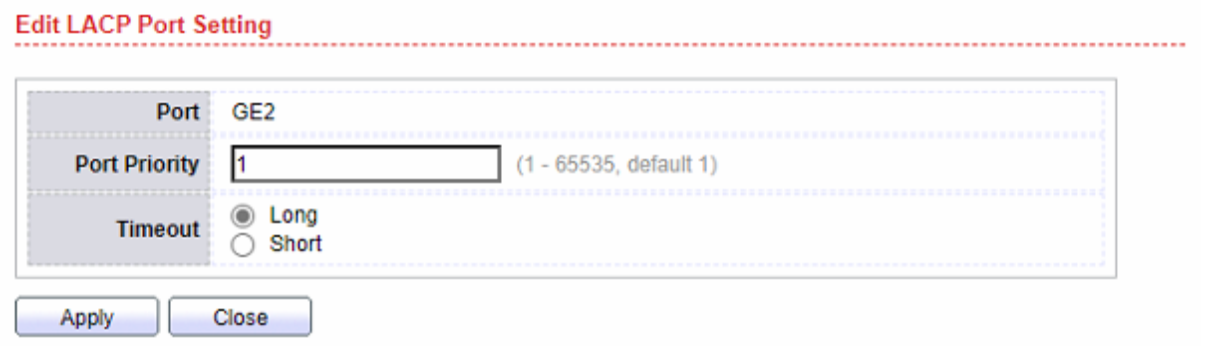
This page allows you to configure LACP global and port configurations.

Field	Description
System Priority	Configure the system priority of LACP.



Field	Description
Port	Port Name
Port Priority	LACP priority value of the port
Timeout	The periodic transmission type of LACP PDUs. • **Long:** Transmit LACP PDU with slow periodic (30s). • **Short:** Transmit LACPP DU with fast periodic (1s).

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



Field	Description
Port	Port Name
Port Priority	Enter the LACP priority value of the port
Timeout	Select the transmission type of LACP PDUs. • **Long:** Transmit LACP PDU with slow periodic (30s). • **Short:** Transmit LACPP DU with fast periodic (1s).

EEE

This page allows you to configure Energy Efficient Ethernet settings.

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

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

Field	Description
Port	Port Name
State	Port EEE admin state. • **Enabled:** Enable EEE • **Disabled:** Disable EEE

JUMBO FRAME

This page allows you to configure the size of the jumbo frames.

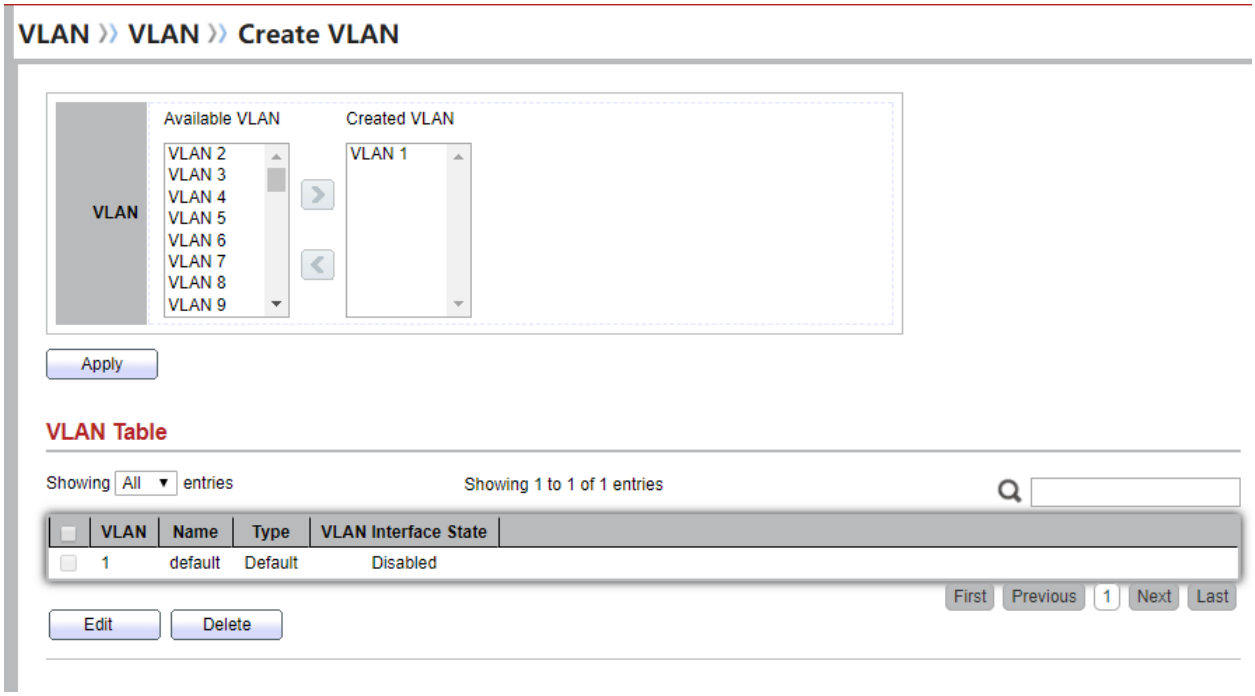
Field	Description
Jumbo Frame	Enable or disable jumbo frame. When jumbo frame is disabled, the default frame size of 1522 will be used.

VLAN

This chapter describes VLAN Configuration.

CREATE VLAN

This page allows you to add or delete VLAN ID entries and brows all VLAN entries that have been added. Each VLAN entry has a unique name, which can be edited.



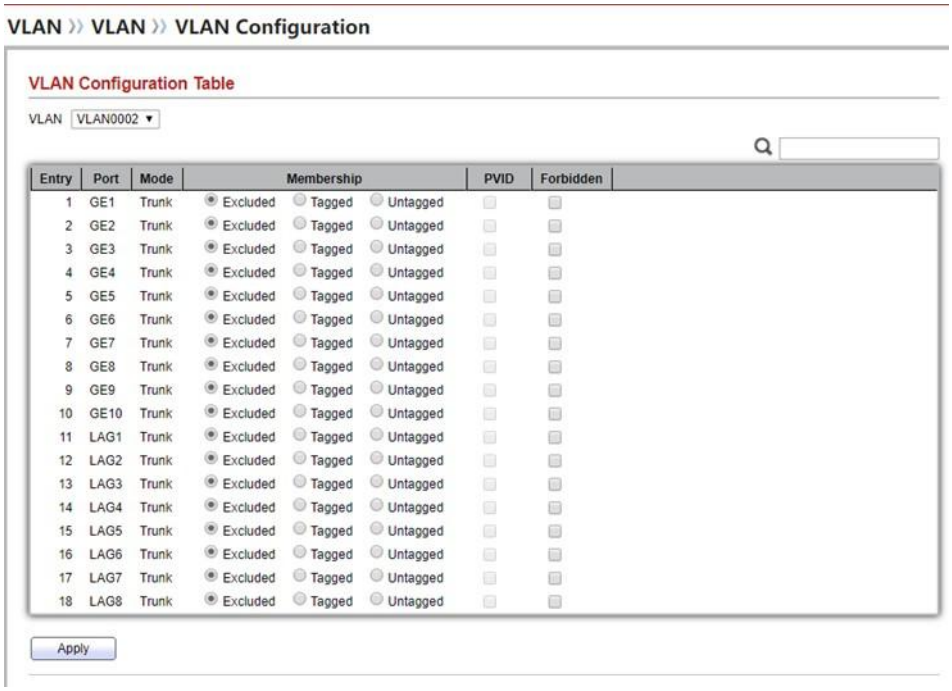
Field	Description
Available VLAN	VLAN has not been created yet. Move to right side to create that VLAN.
Created VLAN	VLAN has been created. Move to left side to remove that VLAN.

Select VLAN and click the “Edit” button to edit the VLAN name.

Field	Description
Name	Input the VLAN name.

VLAN CONFIGURATION

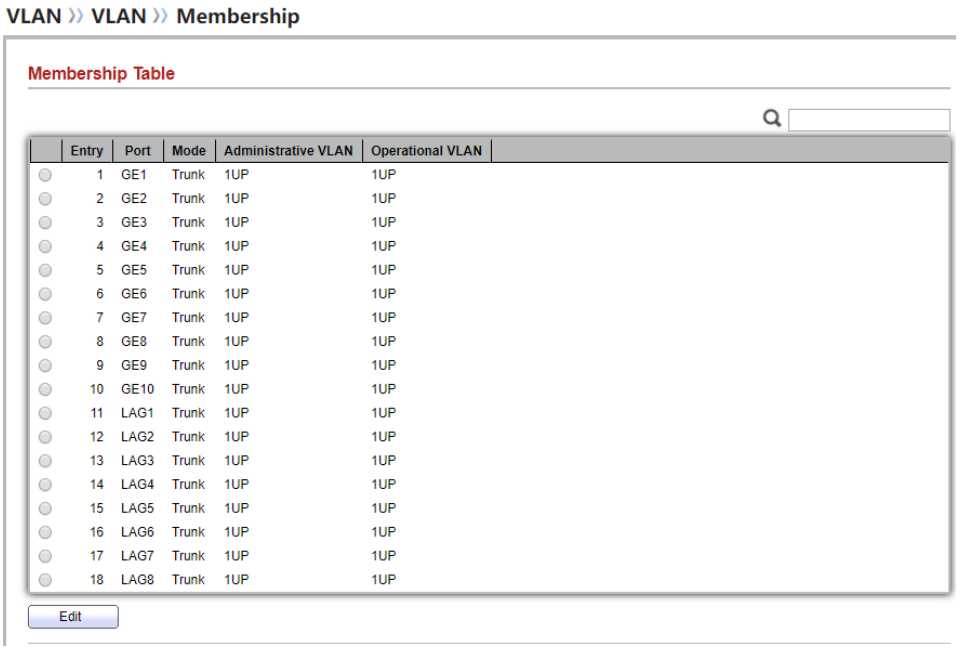
This page allows you to configure the VLAN membership of each port.



Field	Description
VLAN	Select specified VLAN ID to configure VLAN configuration.
Port	Port description
Mode	Displays the current VLAN mode of the port
Membership	Select the membership status of this port and specified VLAN ID. • **Excluded:** Excludes the port from the VLAN • **Tagged**: Makes the port a tagged member of that VLAN • **Untagged:** Makes the port an untagged member of that VLAN • **Forbidden:** Specifies that the port is forbidden on that VLAN
PVID	Shows if the Port VLAN ID is on the current interface

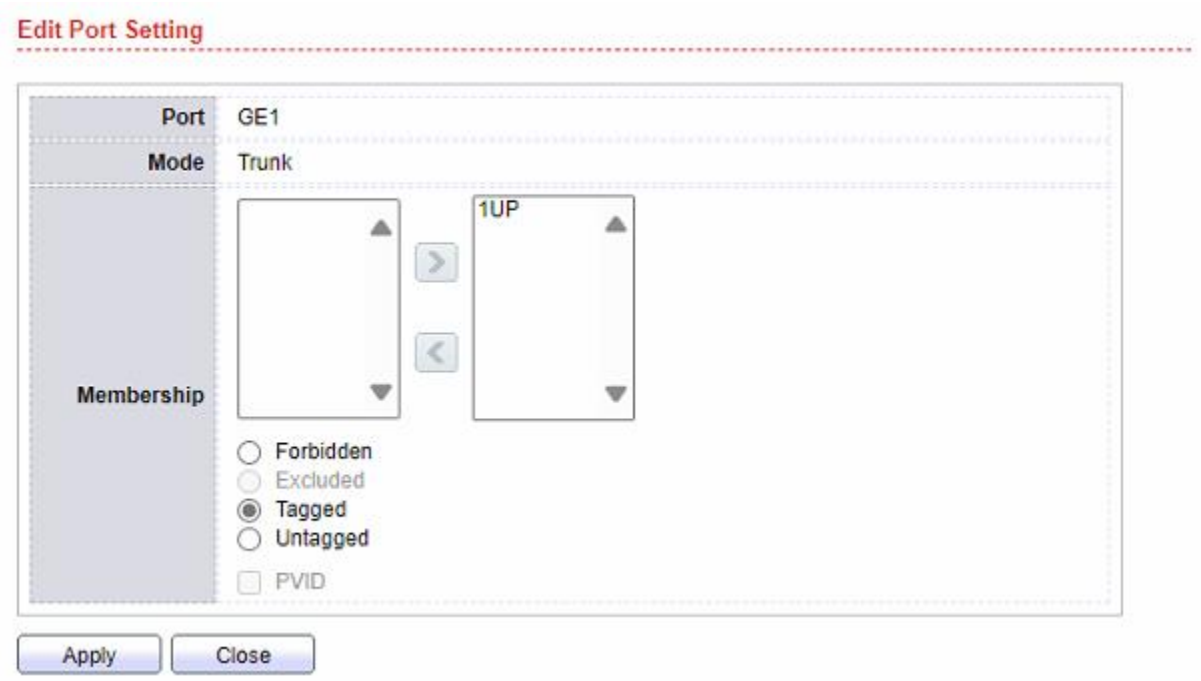
MEMBERSHIP

This page allows you to view membership information for each port and edit the membership information.



Field	Description
Mode	Shows the interface VLAN mode of port.
Administrative VLAN	Shows the administrative VLAN of this port.
Operational VLAN	Shows the operational VLAN of this port. This may be different to the administrative VLAN.

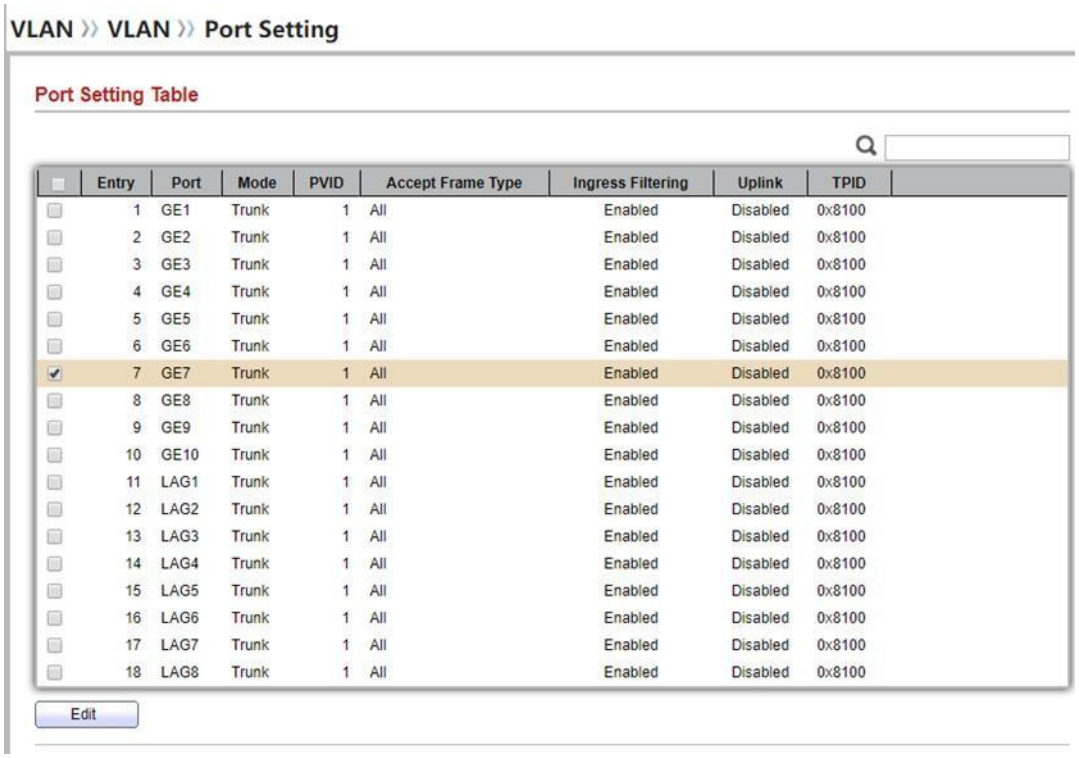
To edit the membership values click the “Edit” button.



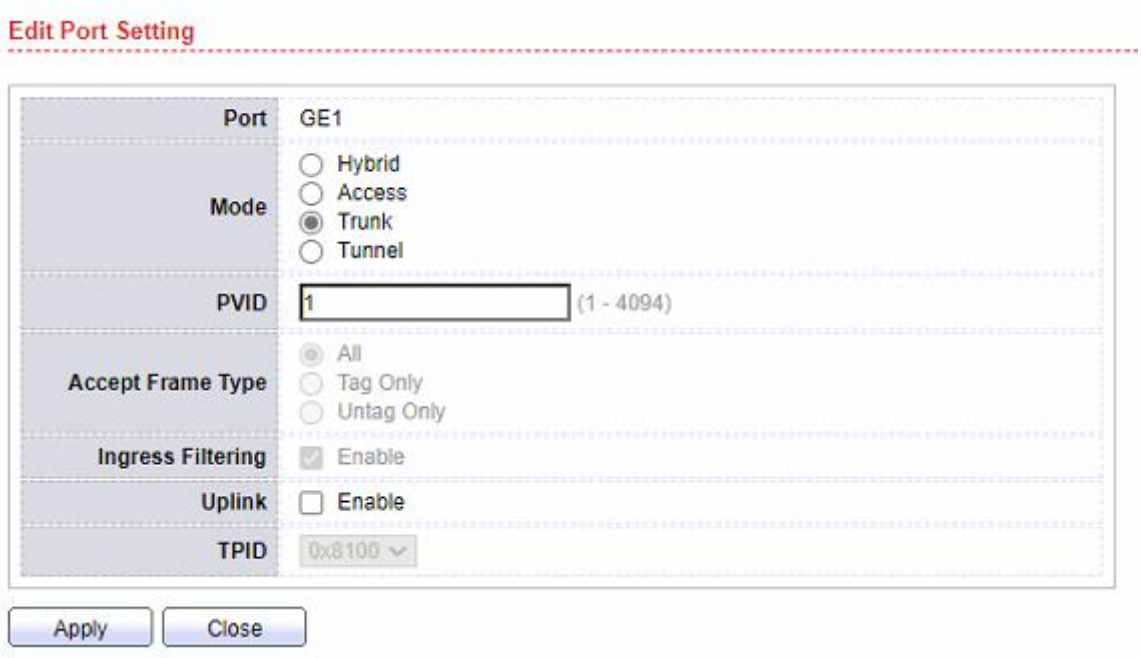
Field	Description
Port	Shows the currently selected port
Mode	Displays the current VLAN mode of the port.
Membership	Select the VLANs and move them to the right to add them. To remove them, simply move them to the left. • **Forbidden:** Specifies that the port is forbidden on that VLAN • **Excluded:** Excludes the port from the VLAN • **Tagged**: Makes the port a tagged member of that VLAN • **Untagged:** Makes the port an untagged member of that VLAN • **PVID:** Select this box to make this the PVID for this port

PORT SETTING

This page will allow you to configure port VLAN settings such as VLAN port mode, PVID etc.



Field	Description
Port	Port description
Mode	Displays the current VLAN mode of the port
PVID	Shows if the Port VLAN ID is on the current interface
Accept Frame Type	Displays the accept frame type
Ingress Filtering	Shows ingress filter status of the port
Uplink	Shows the Uplink status
TPID	Shows the TPID of the port

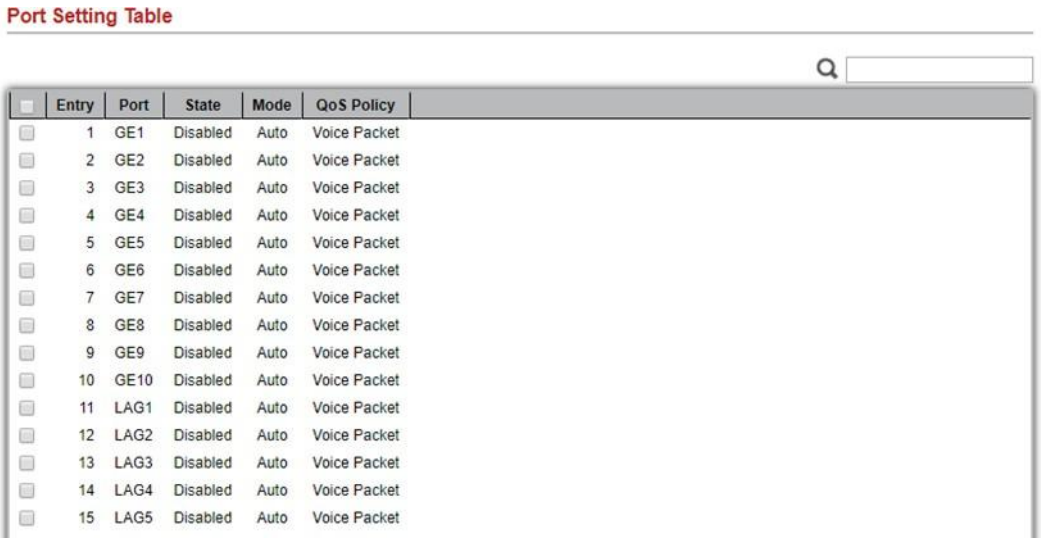


Field	Description
Port	Shows the selected port to be edited.
Mode	Select the VLAN mode. • **Hybrid:** As defined in IEEE 802.1Q, will allow multiple VLANs through. • **Access:** Only accepts untagged frames from a specific VLAN • **Trunk:** Used to send multiple Tagged VLANs
PVID	Specify the port based VLAN ID (1-4094). Only available with Hybrid and Trunk mode.
Accepted Type	Specify the acceptable-frame-type of the specified interface. only available with Hybrid mode.
Ingress Filtering	Enable/disable ingress filtering. Only available with Hybrid mode.
Uplink	Enable/disable Uplink mode. Only available with Trunk mode.
TPID	Select the TPID to be used. Only available with trunk mode.

VOICE VLAN

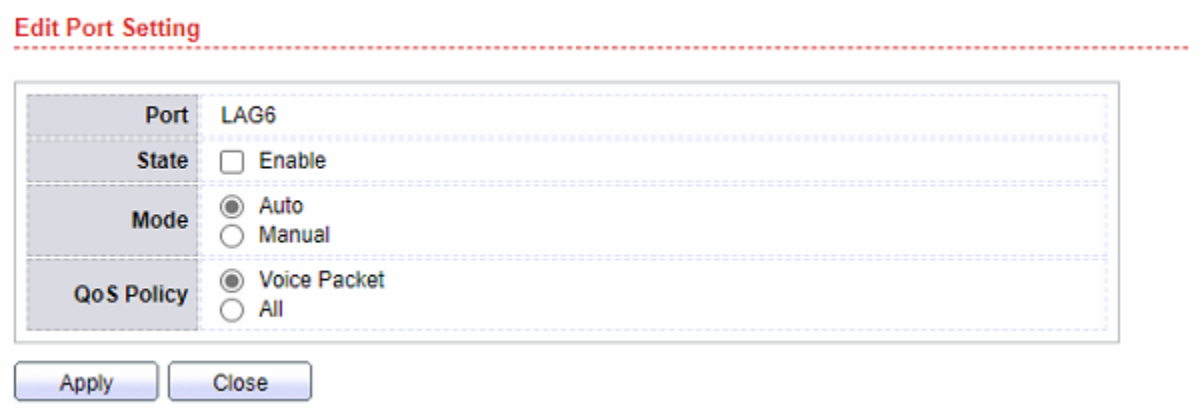
PROPERTY

Field	Description
State	Enable/Disable the Voice VLAN function
VLAN	Select the VLAN ID. It cannot be the default VLAN.
Cos/802.1p	Select a value for VPT. Qualified packets will use this VPT value as inner priority.
Remarking	Enable/Disable remarking.
Aging Time	Enter the value of Aging Time. Default is 1440 minutes. If no packets pass through within the set time, the Voice VLAN will age out.



Field	Description
Port	Port description
State	Displays the status of the interface
Mode	Displays the mode of the VLAN
QOS Policy	Displays the packet type

To edit the values, click the “Edit” button.



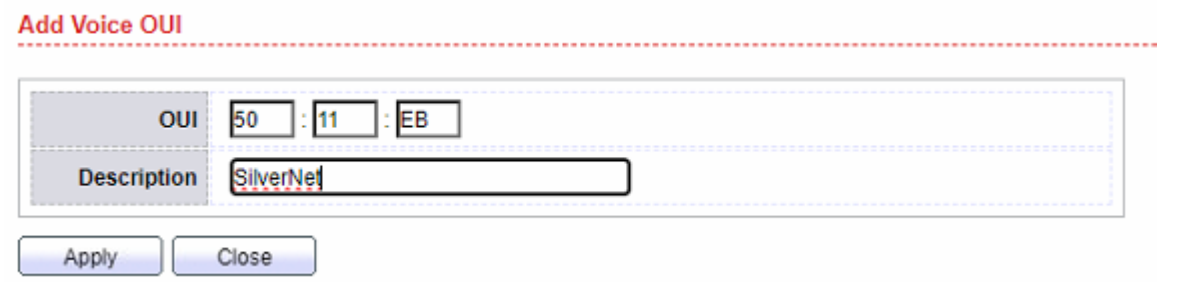
Field	Description
Port	Port description
State	Enable/Disable voice VLAN function on interface
Mode	Select mode. • **Auto:** Auto detect packets that match the OUI table and adds the receiving port into voice VLAN tagged member. • **Manual:** receiving ports will need to be added manually.
QOS Policy	Select 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.

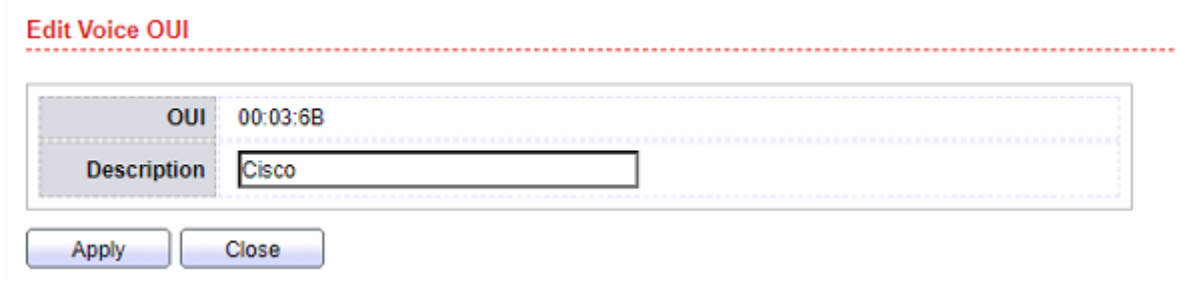
VOICE OUI

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

Field	Description
OUI	Shows the OUI MAC address
Description	Shows the description of the OUI entry

Add and edit OUI



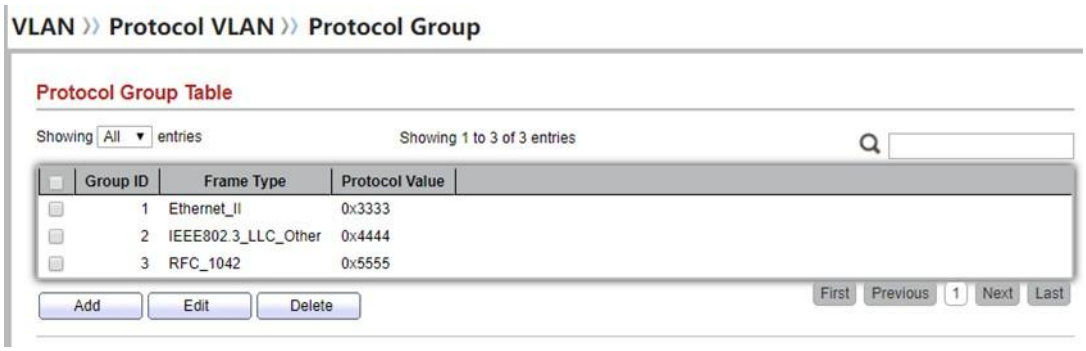


Field	Description
OUI	Enter OUI MAC address.
Description	Enter a description of the specified MAC address.

PROTOCOL VLAN

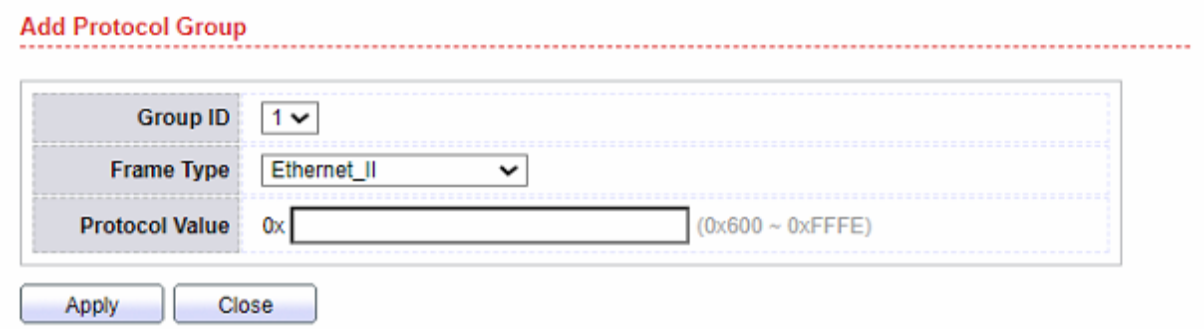
PROTOCOL GROUP

This page allows you to add or edit group settings of protocol VLAN.



Field	Description
Group ID	Displays the group ID
Frame Type	Displays the frame type
Protocol Value	Displays the protocol value

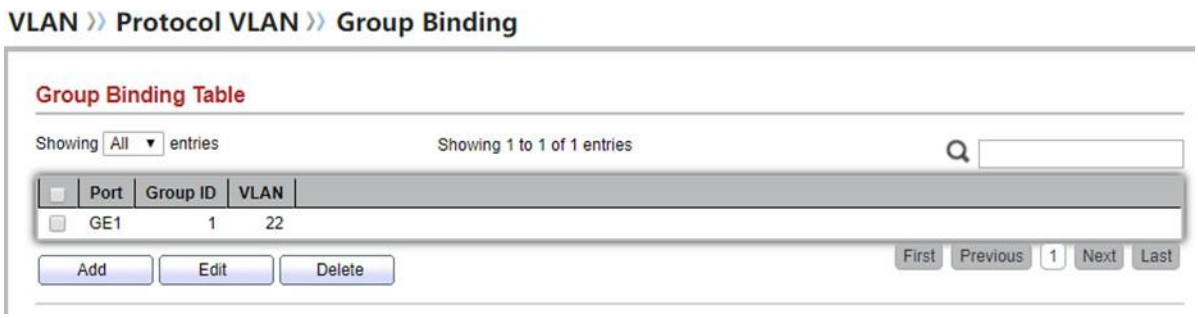
Add and edit Protocol Group.



Field	Description
Group ID	Select the group ID from the list.
Frame Type	Select the frame type. • **Ethernet_II:** packet type is Ethernet version 2 • **IEEE802.3_LLC_Other:** packet type is 802.3 packet with LLC • **RFC_1042:** packet type is rfc 1042 packet.
Protocol Value	Enter the protocol value. Packets that match this protocol value will be classified to the specified VLAN ID.

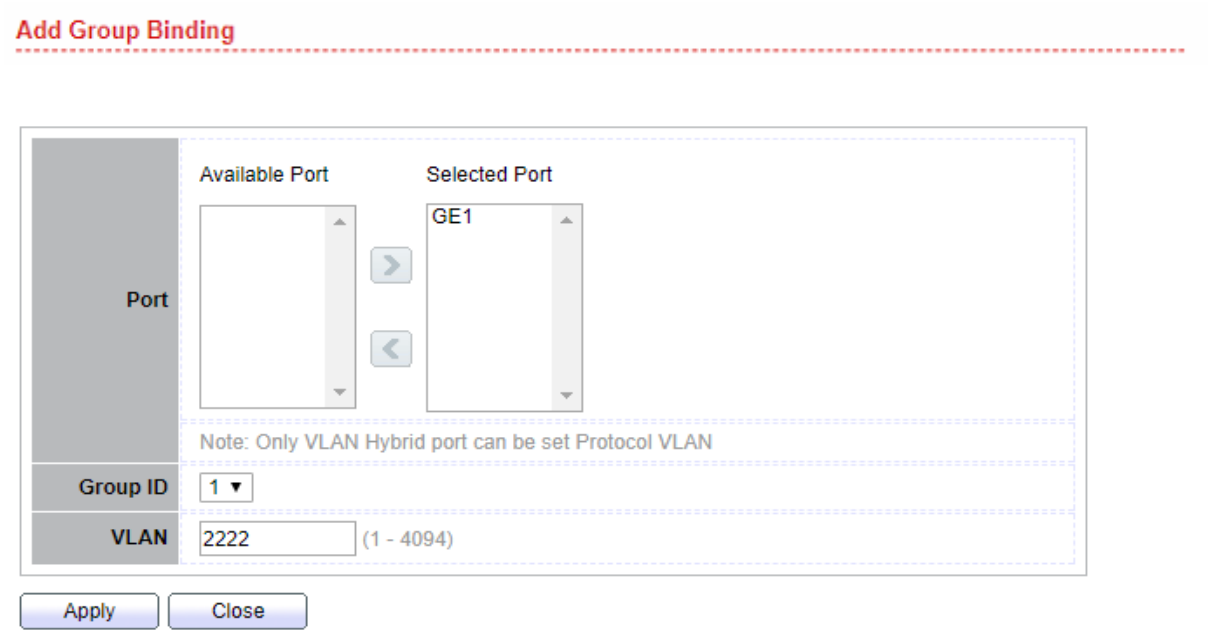
GROUP BINDING

This page allows you to bind a protocol VLAN group to each port with VLAN ID



Field	Description
Port	Displays the port ID.
Group ID	Displays the group ID.
VLAN	Displays the assigned VLAN.

Click the “Add” or “Edit” button.



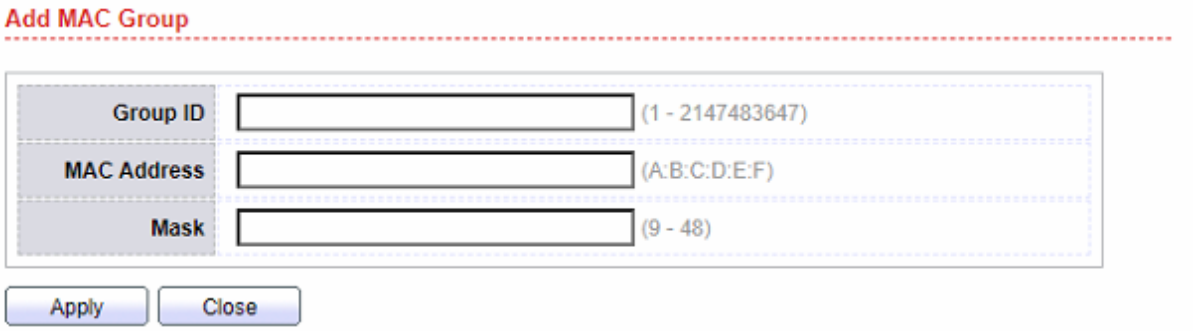
Field	Description
Port	Move ports to the right to select them.
Group ID	Select a Group ID to associate with the port.
VLAN	Enter the VLAN ID that will assign to packets which match the protocol group.

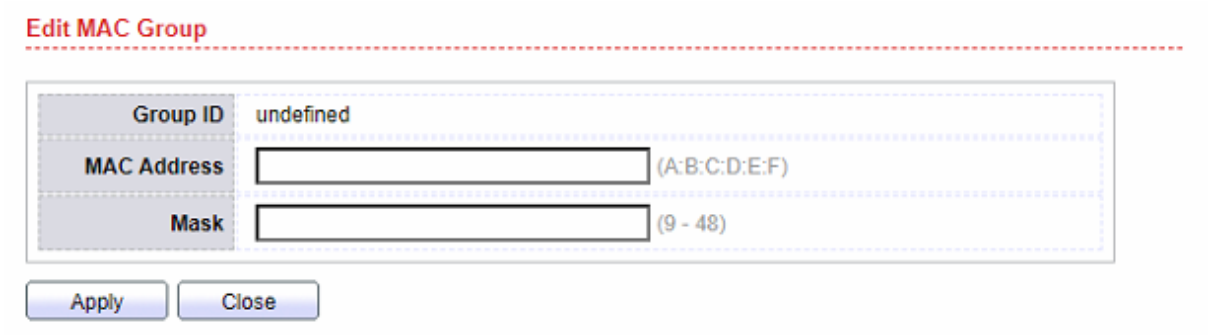
MAC LAN

MAC GROUP

This page allows you to add or edit group settings of MAC VLAN.

Field	Description
Group ID	Displays the Group ID.
MAC Address	Displays the MAC Address.
Mask	Displays the mask of the MAC Address for classified packet.

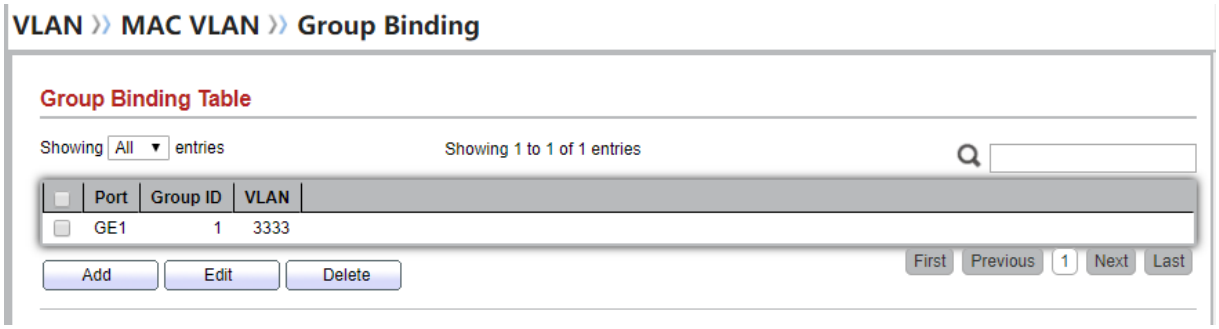




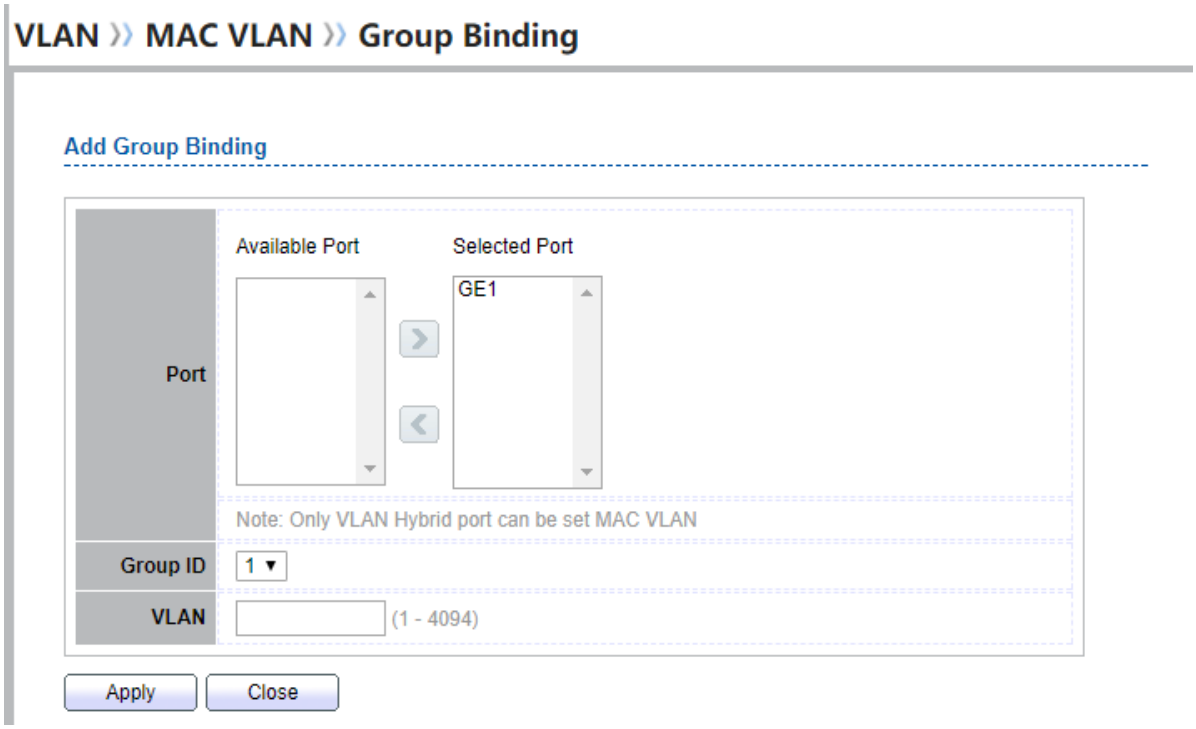
Field	Description
Group ID	Enter the group ID.
MAC Address	Enter the MAC address.
Mask	Enter the mask of the MAC address.

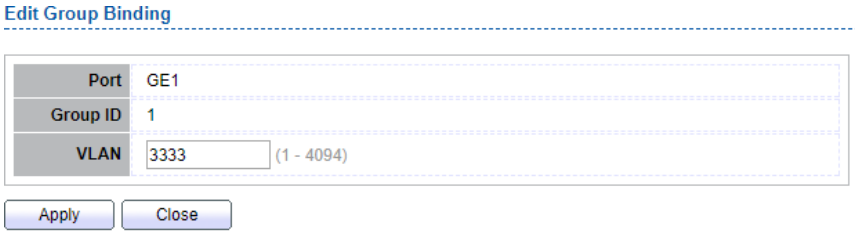
GROUP BINDING

This page allows you to bind a MAC VLAN group to each port with VLAN ID.



Field	Description
Port	Displays the port ID.
Group ID	Displays the group ID.
VLAN	Displays the assigned VLAN.



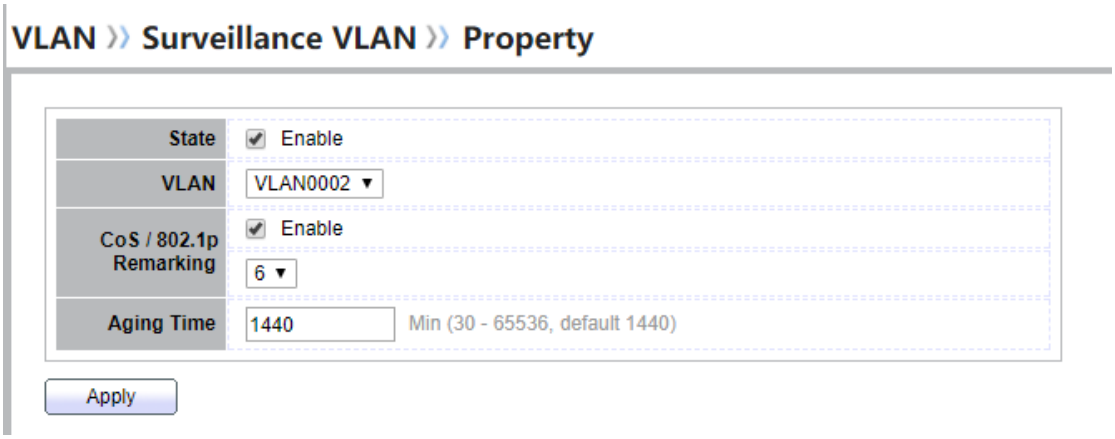


Field	Description
Port	Move ports to the right to select them.
Group ID	Select a Group ID to associate with the port.
VLAN	Enter the VLAN ID that will assign to packets which match the MAC group.

SURVEILLANCE VLAN

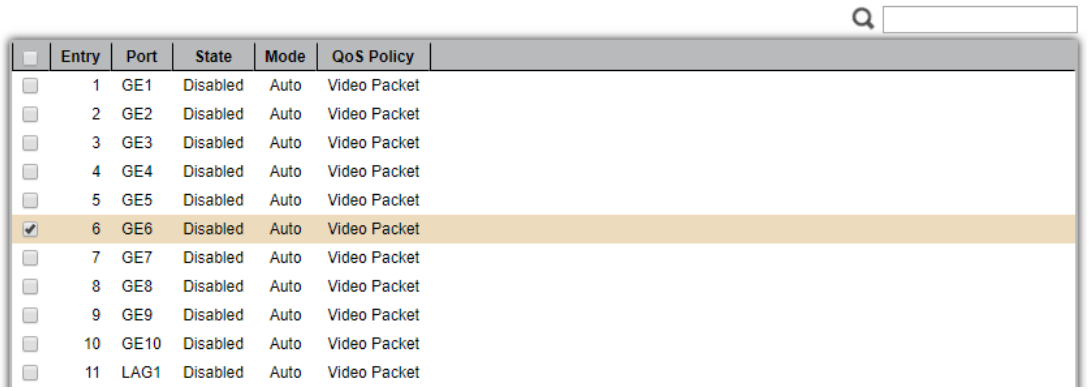
PROPERTY

This page shows how to configure global and per interface settings of Surveillance VLAN.



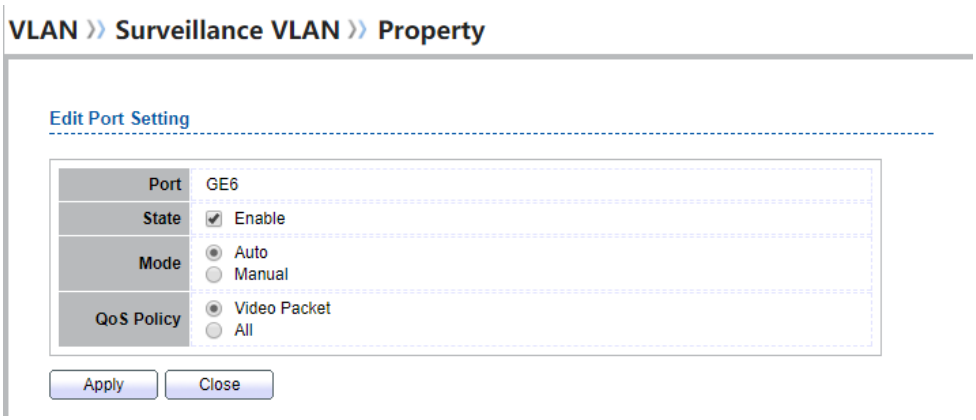
Field	Description
State	Enable/Disable the Voice VLAN function
VLAN	Select the VLAN ID. It cannot be the default VLAN.
Cos/802.1p	Select a value for VPT. Qualified packets will use this VPT value as inner priority.
Remarking	Enable/Disable remarking.
Aging Time	Enter the value of Aging Time. Default is 1440 minutes. If no packets pass through within the set time, the Voice VLAN will age out.

Port Setting Table



Entry	Port	State	Mode	QoS Policy
1	GE1	Disabled	Auto	Video Packet
2	GE2	Disabled	Auto	Video Packet
3	GE3	Disabled	Auto	Video Packet
4	GE4	Disabled	Auto	Video Packet
5	GE5	Disabled	Auto	Video Packet
6	GE6	Disabled	Auto	Video Packet
7	GE7	Disabled	Auto	Video Packet
8	GE8	Disabled	Auto	Video Packet
9	GE9	Disabled	Auto	Video Packet
10	GE10	Disabled	Auto	Video Packet
11	LAG1	Disabled	Auto	Video Packet

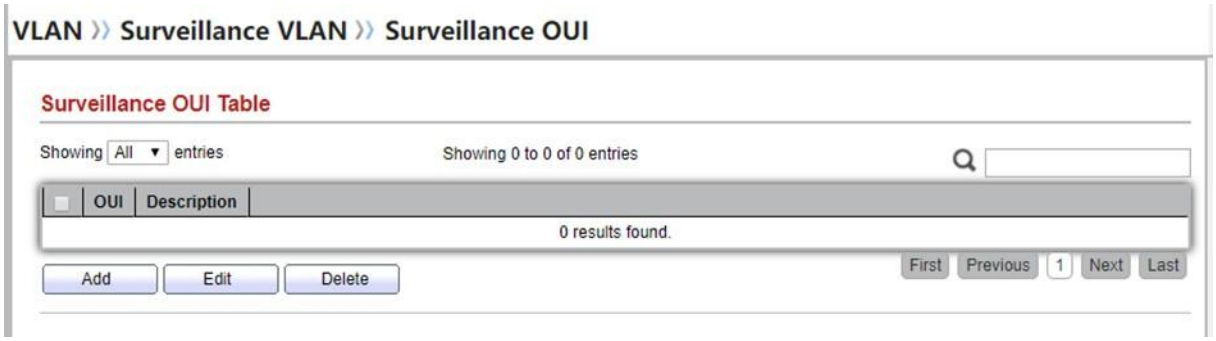
Field	Description
Port	Port description
State	Displays the status of the interface
Mode	Displays the mode of the VLAN
QOS Policy	Displays the packet type



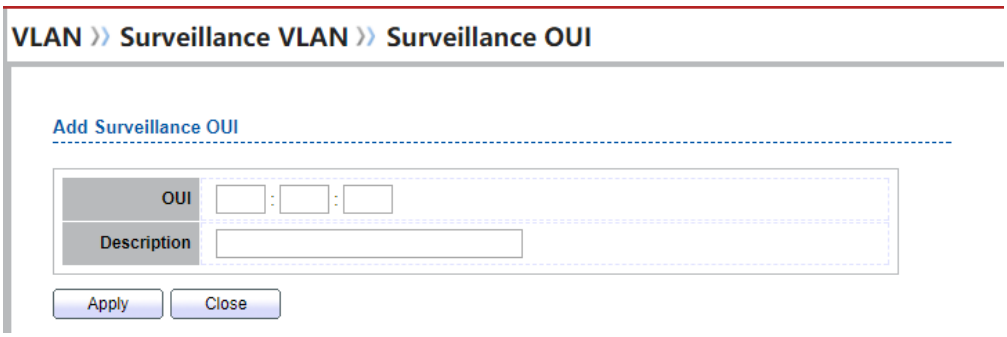
Field	Description
Port	Port description
State	Enable/Disable voice VLAN function on interface
Mode	Select mode. • **Auto:** Auto detect packets that match the OUI table and adds the receiving port into video VLAN tagged member. • **Manual:** receiving ports will need to be added manually.
QOS Policy	Select 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.

SURVEILLANCE OUI

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



Field	Description
OUI	Shows the OUI MAC address
Description	Shows the description of the OUI entry

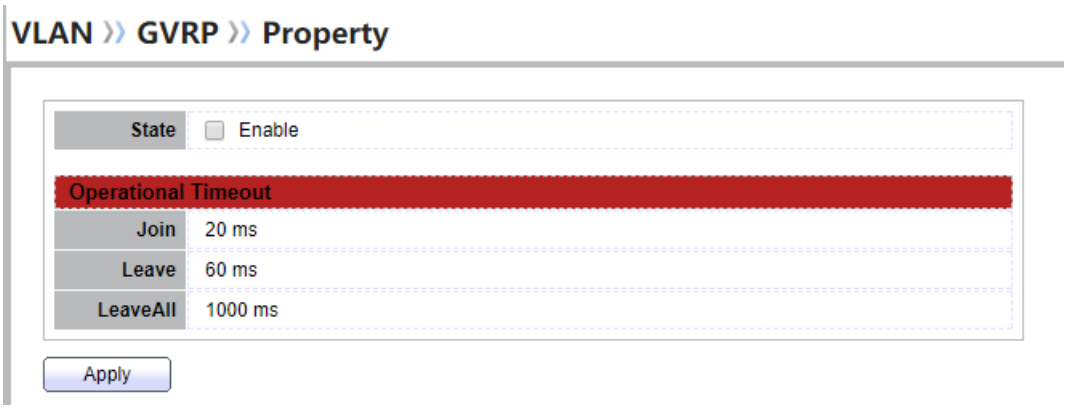


Field	Description
OUI	Enter OUI MAC address.
Description	Enter a description of the specified MAC address.

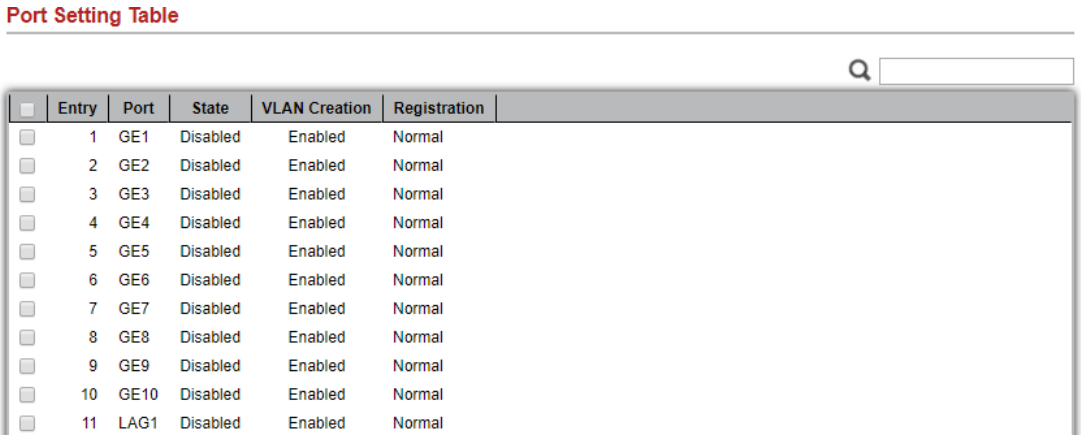
GVRP

PROPERTY

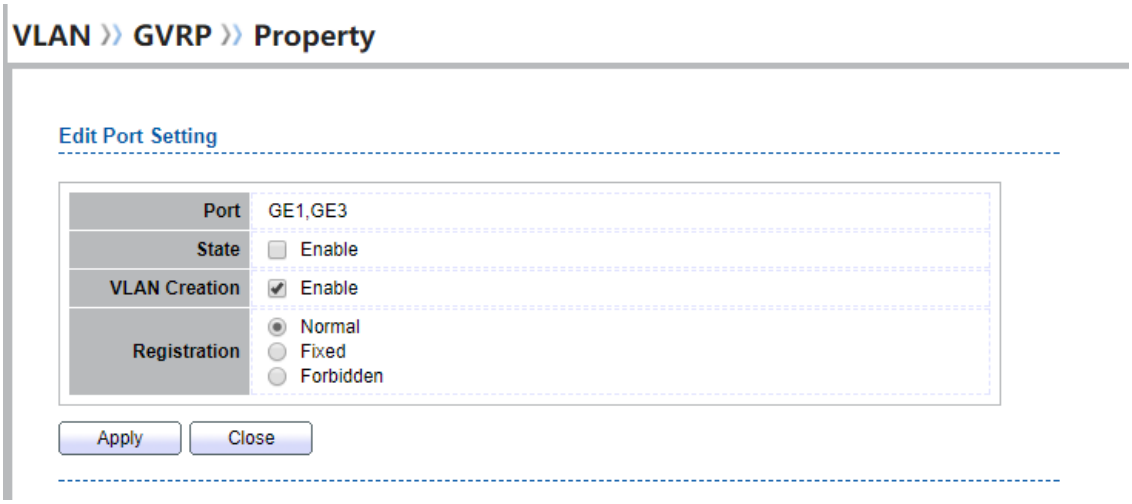
This page allows you to enable or disable GVRP function and GVRP port settings.



Field	Description
State	Enable/Disable GVRP functionality.
Operational Timeout	Description
Join	GVRP Join timeout.
Leave	GVRP leave timeout.
Leave All	GVRP leave all timeout.



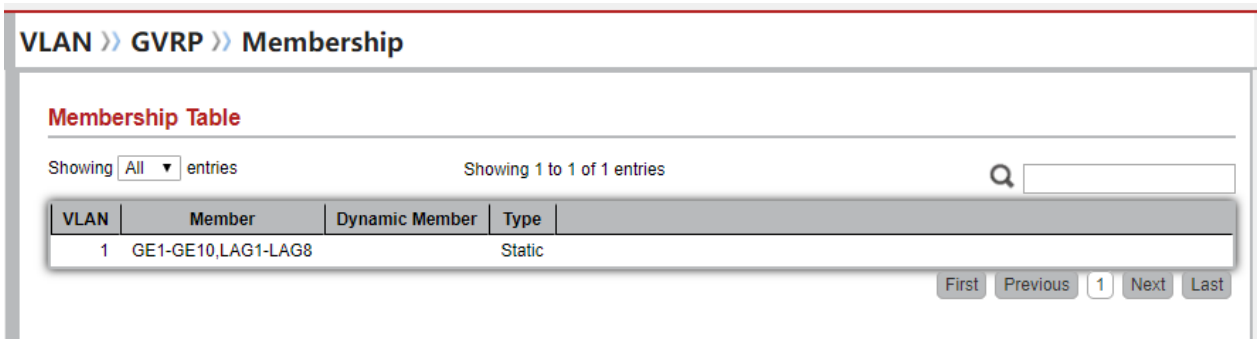
Field	Description
Port	Port description
State	Shows the state of GVRP is Enabled or Disabled.
VLAN Creation	Shows the state of VLAN creation.
QOS Policy	Shows the Registration Mode.



Field	Description
Port	Display the selected ports
State	Enable or Disable GVRP.
VLAN Creation	Enable or Disable dynamic VLAN creation.
Registration Mode	Set the registration mode of GVRP port. • **Normal:** Normal mode. • **Fixed:** The port will not learn any dynamic VLANs. It will only send static VLAN information to neighbours and allow static VLAN packets to pass. • **Forbidden:** The port will not learn any dynamic VLANs and only allow default VLAN packets to pass.

MEMBERSHIP

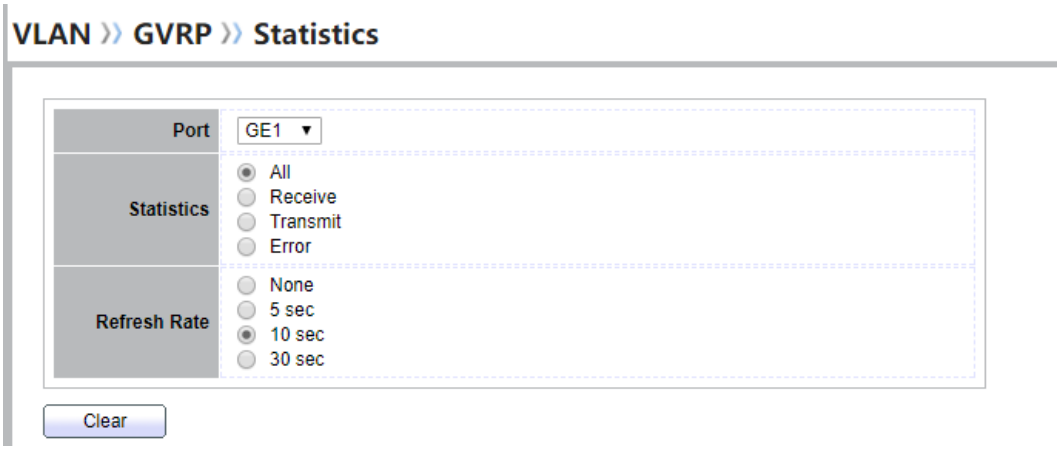
This page allows the user to browse all VLAN member settings that are learned by GVRP protocol or configured by the user.



Field	Description
VLAN	VLAN ID.
Member	VLAN port members including static and dynamic members.
Dynamic Ports	Dynamic members.
VLAN Type	The type of VLAN. Static or dynamic.

STATISTICS

This page allows the user to view GVRP port statistics by type and clear GVRP port statistics by port.



Field	Description
Port	Port ID
Statistics	Type of statistics • **All:** Display Receive, Transmit and Error port statistics • **Receive:** Display Receive port statistics • **Transmit:** Display Transmit port statistics • **Error:** Display Error port statistics
Refresh Rate	Web refresh rate • **None:** Will not refresh statistics • **5 sec:** Refresh display port statistics every 5 seconds • **10 sec:** Refresh display port statistics every 10 seconds • **30 sec:** Refresh display port statistics every 30 seconds

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

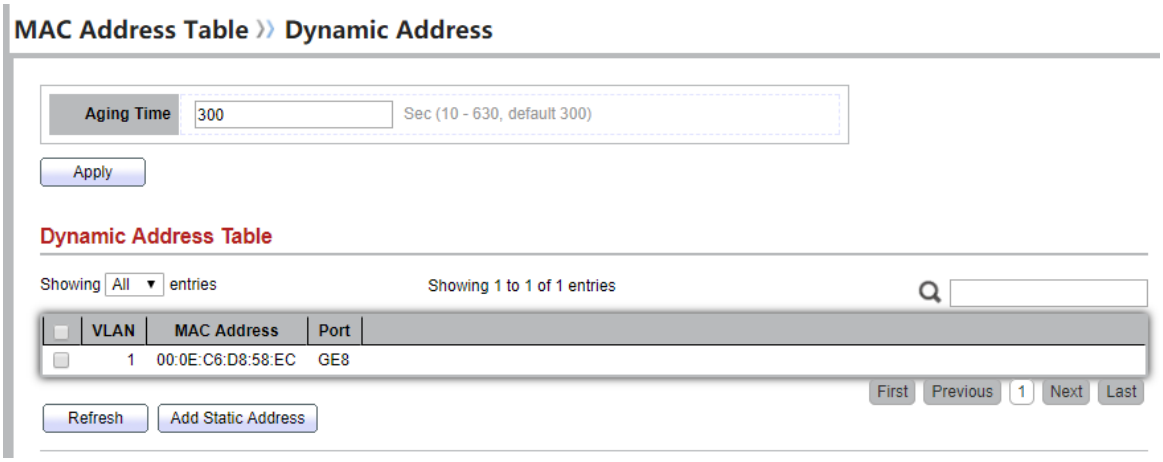
Transmit	
Join empty	0
Empty	0
Leave Empty	0
Join In	0
Leave In	0
Leave All	0

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

Field	Description
Join empty	The number of Receive or Transmit Join empty attribute value.
Empty	The number of Receive or Transmit Empty attribute value.
Leave Empty	The number of Receive or Transmit Leave Empty attribute value.
Join In	The number of Receive or Transmit Join In attribute value.
Leave In	The number of Receive or Transmit Leave In empty attribute
Leave All	The number of Receive or Transmit Leave All attribute value.
Invalid Protocol ID	The number of Receive Invalid Protocol ID
Invalid Attribute Type	The number of Receive Invalid Attribute Type
Invalid Attribute Value	The number of Receive Invalid Attribute value.
Invalid Attribute Length	The number of Receive Invalid Attribute Length.
Invalid Event	The number of Receive Invalid Event.

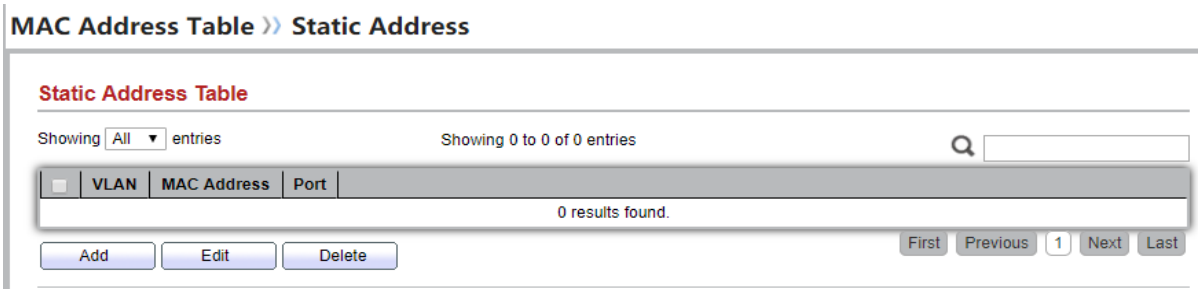
MAC ADDRESS TABLE

DYNAMIC ADDRESS



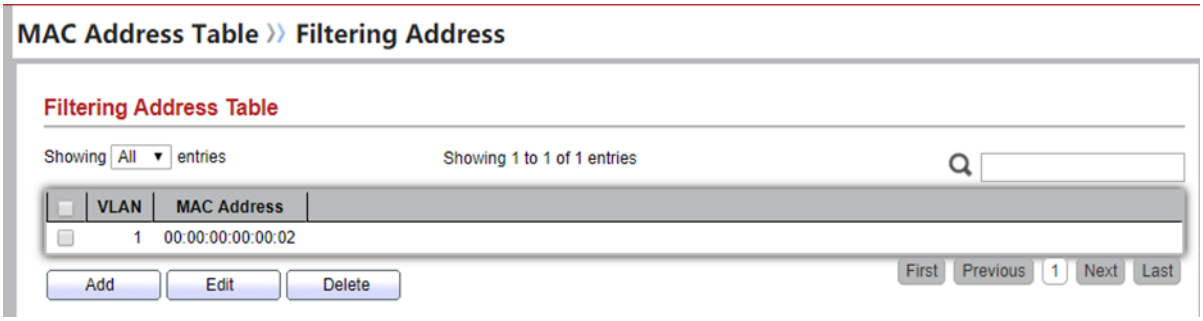
Field	Description
Aging Time	The time in seconds that an entry remains in the MAC address table.

STATIC ADDRESS



Field	Description
VLAN	Shows the VLAN
MAC Address	The MAC address to which packets will be forwarded.
Port	Interface or port number.

FILTERING ADDRESS

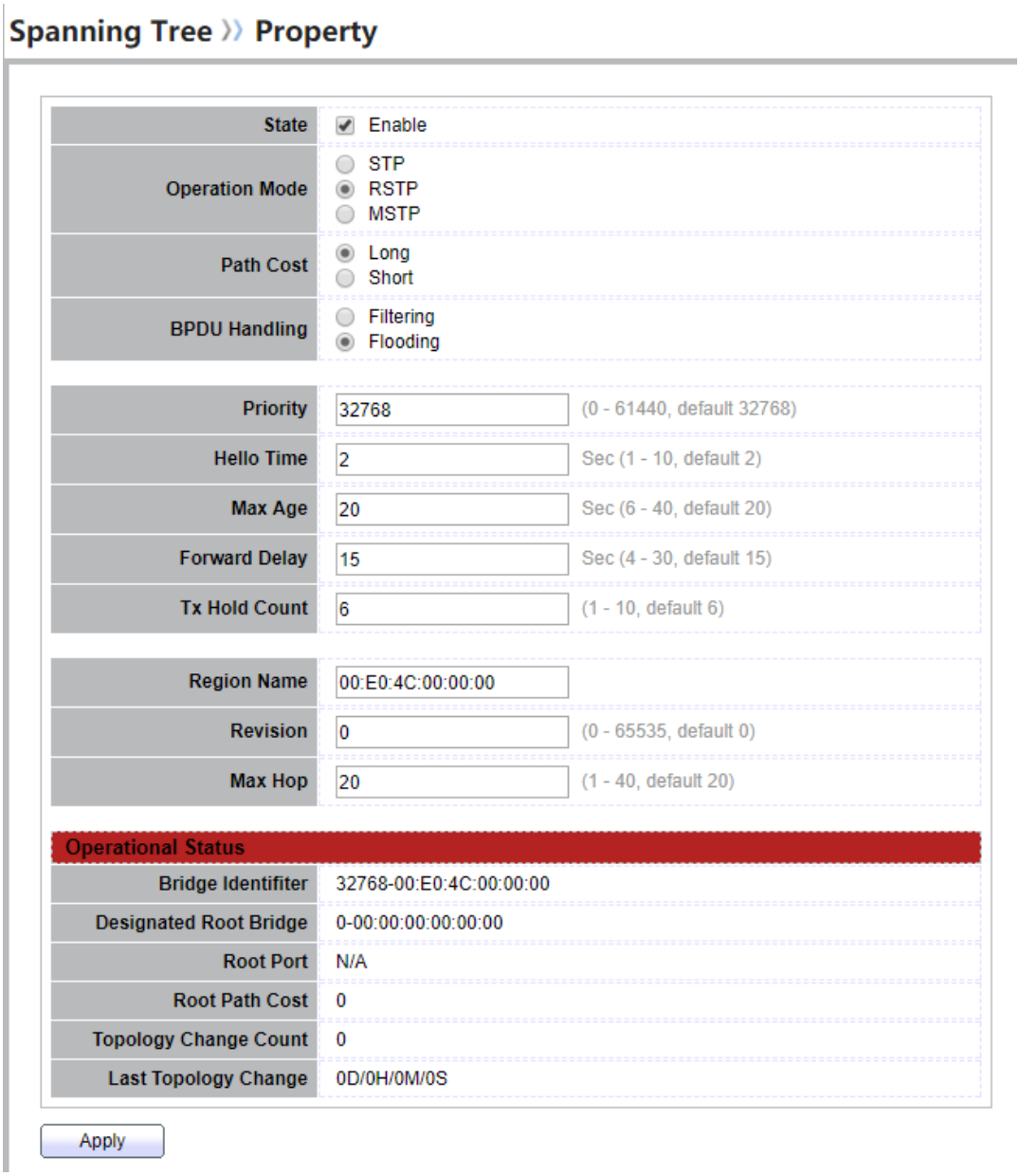


Field	Description
VLAN	Shows the VLAN
MAC Address	Block traffic from the specified MAC address

STP

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

PROPERTY



Field	Description
State	Enable/Disable Spanning Tree.
Operation Mode	Specify the Spanning Tree operation mode. **STP:** Enable Spanning Tree (STP) mode. **RSTP:** Enable Rapid Spanning Tree (RSTP) mode. **MSTP:** Enable Multiple Spanning Tree (MSTP) mode.

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. Default STP priority is 32768. The lower the priority the more likely the switch is to become the root bridge. The valid range is from 0 to 61440, and the value should be a multiple of 4096.
Hello Time	Specify the STP hello time in second to broadcast its hello message on other ports. Its valid range is from 1 to 10 seconds.
Max Age	Specify the maximum length of time that passes before a bridge port saves its configuration BPDU information.
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	Set the maximum number of BPDUs per second that the switch can send from an interface. The valid range is from 1 to 10.
Region Name	The MSTP region name. The maximum length is 32 characters. The default value is the MAC address of the switch.
Revision	The MSTP revision number. Its valid rage is from 0 to 65535.
Max Hops	Specify the number of hops in an MSTP region before the BPDU is discarded. The valid range is 1 to 40.

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	Number of topology changes.
Last Topology Change	The last time for the topology changed.

PORT SETTING

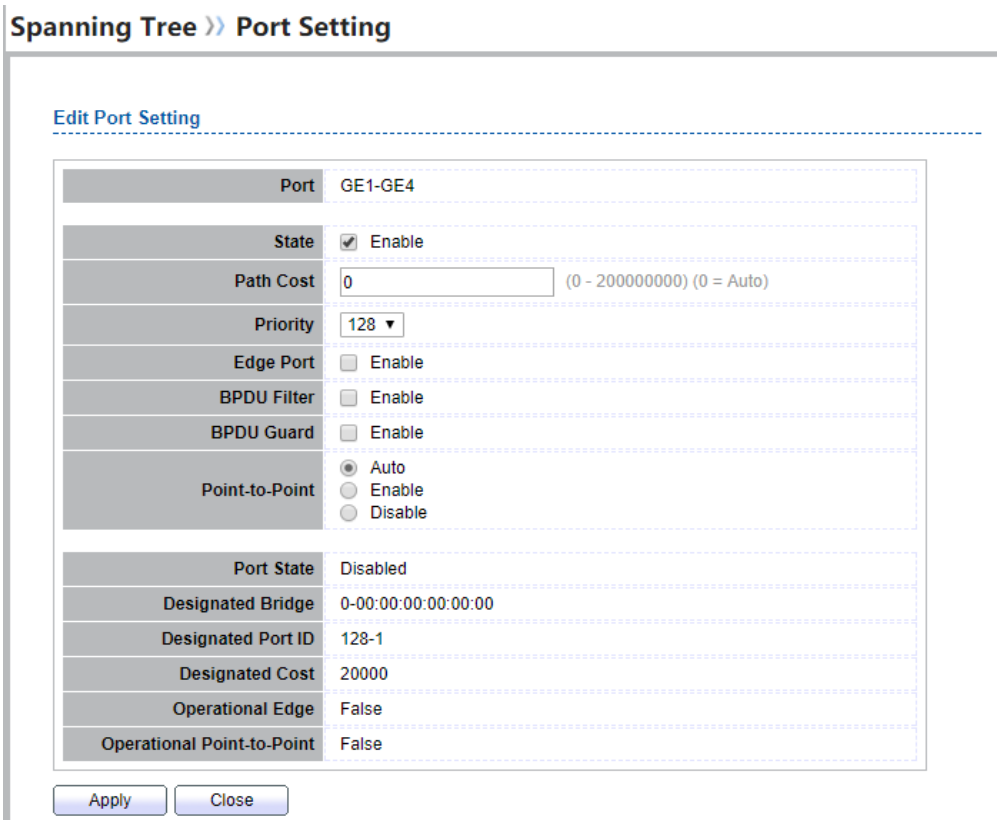
Spanning Tree ›› Port Setting

Port Setting Table

Entry	Port	State	Path Cost	Priority	BPDU Filter	BPDU Guard	Operational Edge	Operational Point-to-Point	Port Role	Port State	Designated Bridge	Designated Port ID	Designated Cost
1	GE1	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-1	20000
2	GE2	Enabled	20000	128	Disabled	Disabled	Enabled	Enabled	Designated	Forwarding	32768-50:11:EB:20:19:37	128-2	20000
3	GE3	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-3	20000
4	GE4	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-4	20000
5	GE5	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-5	20000
6	GE6	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-6	20000
7	GE7	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-7	20000
8	GE8	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-8	20000
9	GE9	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-9	20000
10	GE10	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-10	20000
11	GE11	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-11	20000
12	GE12	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-12	20000
13	GE13	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-13	20000
14	GE14	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-14	20000
15	GE15	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-15	20000
16	GE16	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-16	20000
17	GE17	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-17	20000
18	GE18	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-18	20000
19	GE19	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-19	20000
20	GE20	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-20	20000
21	GE21	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-21	20000
22	GE22	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-22	20000
23	GE23	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-23	20000
24	GE24	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-24	20000
25	TE1	Enabled	2000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-25	2000
26	TE2	Enabled	2000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-26	2000
27	TE3	Enabled	2000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-27	2000
28	TE4	Enabled	2000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-28	2000
29	LAG1	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-29	20000

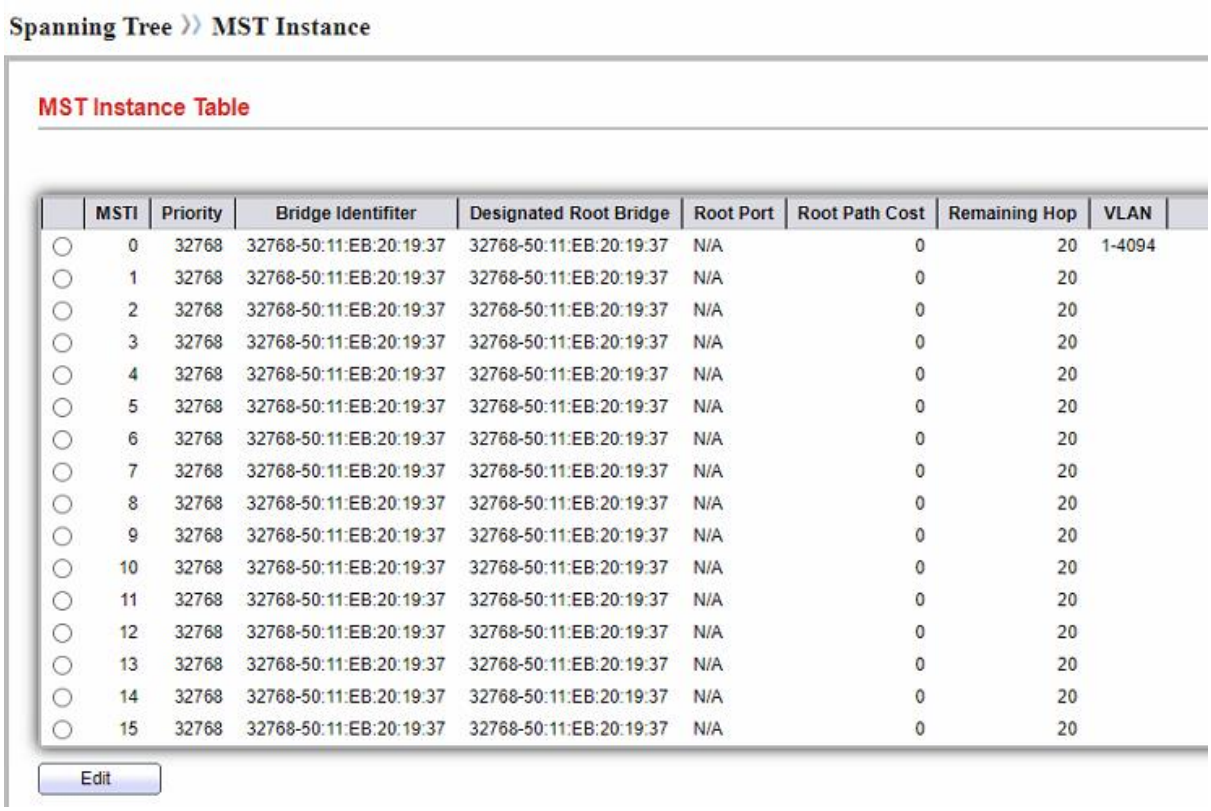
Field	Description
Port	Displays the port.
State	The operational state on the specified port.
Path Cost	STP path cost on the specified port.
Priority	STP priority on the specified port.
BPDU Filter	The state of the BPDU filter on the specified port.
BPDU Guard	The state of the BPDU guard on the specified port.
Operational Edge	The operational edge port status on the specified port.
Operational Point-to-Point	The operational point-to-point status on the specified port.
Port Role	The current port role on the specified port.
Port State	The current port state on the specified port.
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

Field	Description
Protocol Migration Check	Restart the Spanning Tree Protocol (STP) migration process on the specific interface.

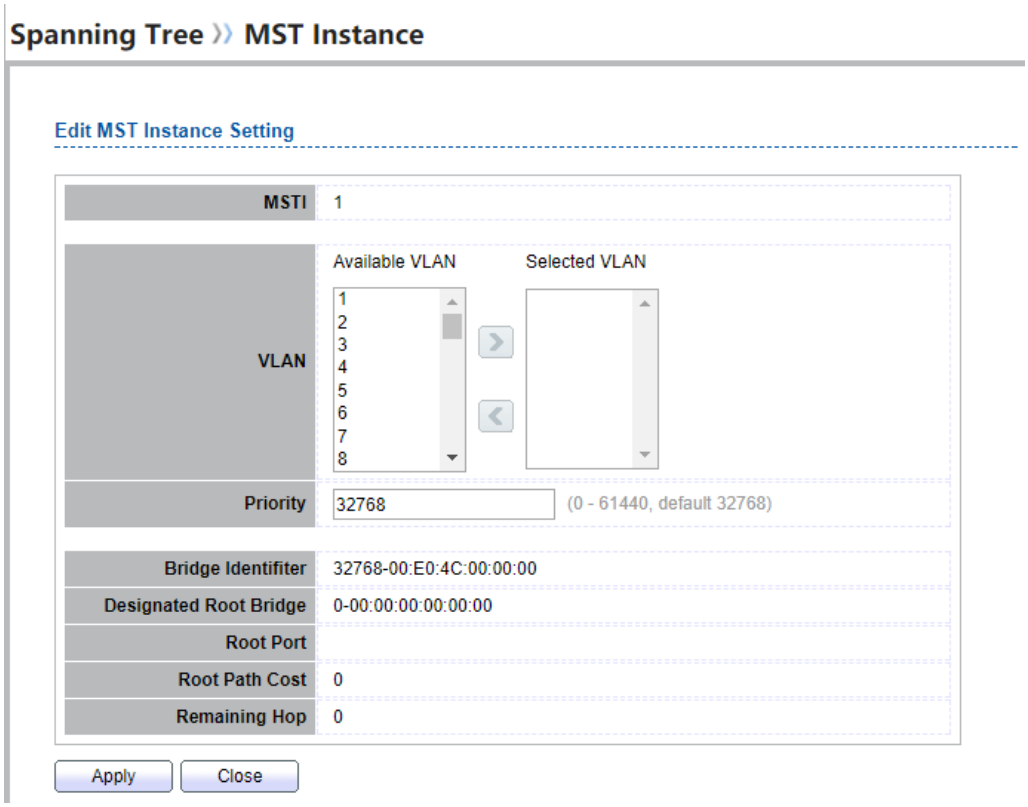


Field	Description
State	Enable/Disable the STP on the specified port.
Path Cost	Specify the STP path cost on the specified port.
Priority	Specify the STP path cost on the specified port.
Edge Port	Specify the edge mode. • **Enable:** Force to true state (as link to a host). • **Disable:** Force to false state (as link to a bridge). With edge mode, the interface will be put into Forwarding state immediately upon link up. If edge mode is enabled for the interface and there are BPDUs received on the interface, a loop might occur in the short time before the STP state changes.
BPDU Filter	The BPDU Filter configuration avoids receiving/transmitting BPDU from the specified ports. • **Enable:** Enable BPDU filter function. • **Disable:** Disable BPDU filter function.
BPDU Guard	The BPDU Guard configuration to drop the received BPDU directly. **Enable:** Enable BPDU guard function. **Disable:** Disable BPDU guard function.
Point-to-Point	Specify the Point-to-Point port configuration: **Auto:** Dependent on the duplex setting of the port. **Enable:** Force to true state. **Disable:** Force to false state.

MST INSTANCE

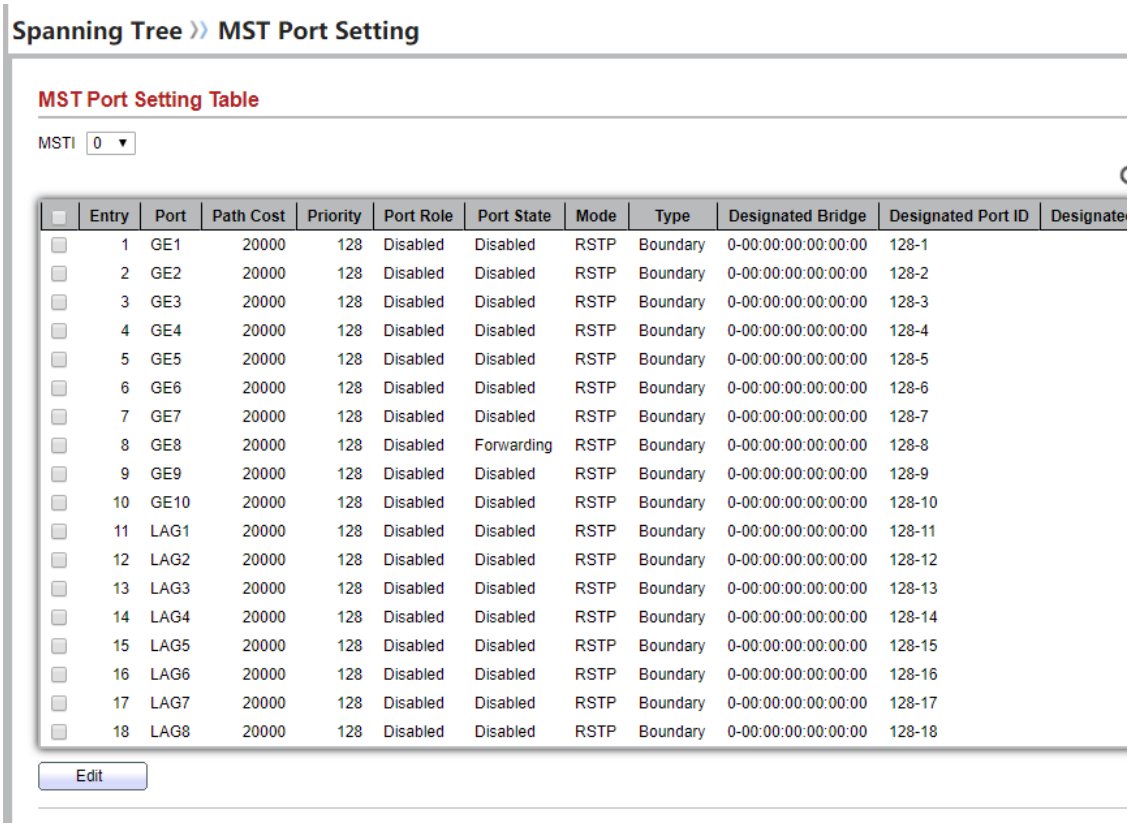


Field	Description
MSTI	MST instance ID.
Priority	The bridge priority on the specified MSTI.
Bridge Identifier	The bridge identifier on the specified MSTI.
Designated Root Bridge	The designated root bridge identifier on the specified MSTI.
Root Port	The designated root port on the specified MSTI.
Root Path Cost	The designated root path cost on the specified MSTI.
Remaining Hop	The remaining hop on the specified MSTI.
VLAN	The VLAN configuration on the specified MSTI.

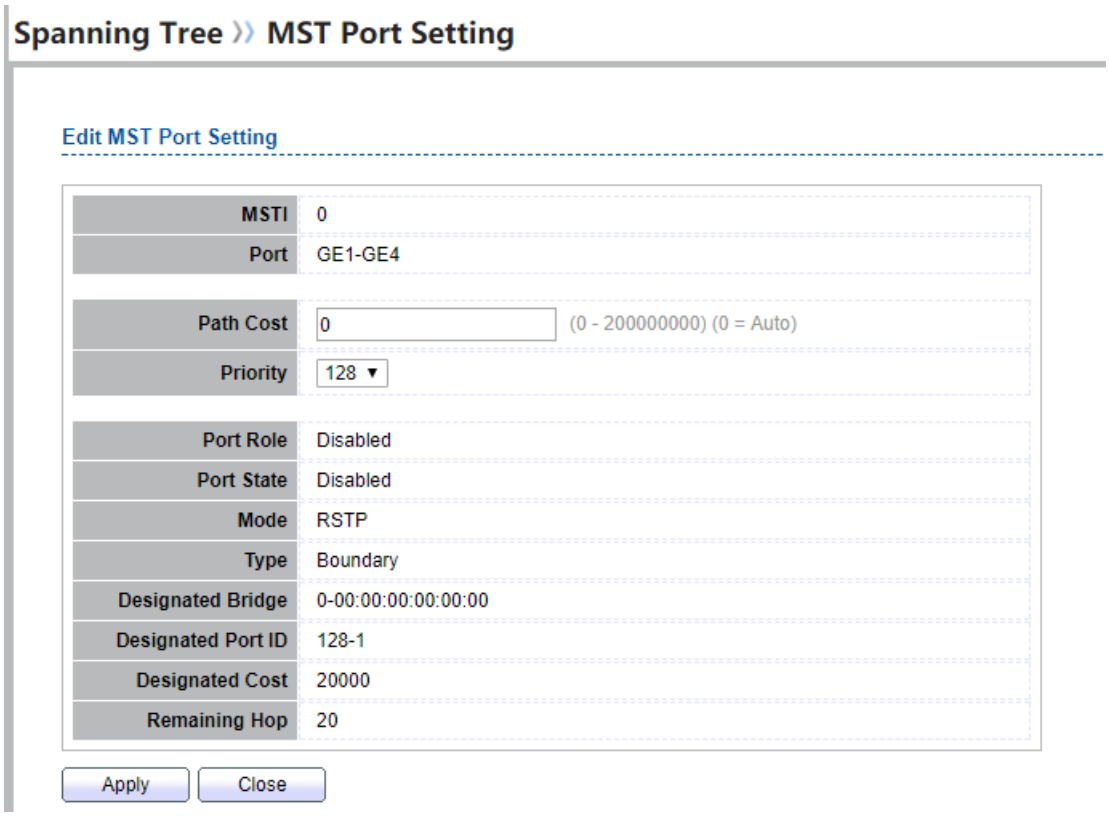


Field	Description
VLAN	Select the VLAN for the MSTI
Priority	Specify the bridge priority. Default STP priority is 32768. The lower the priority the more likely the switch is to become the root bridge. The valid range is from 0 to 61440, and the value should be a multiple of 4096.

MST PORT SETTING

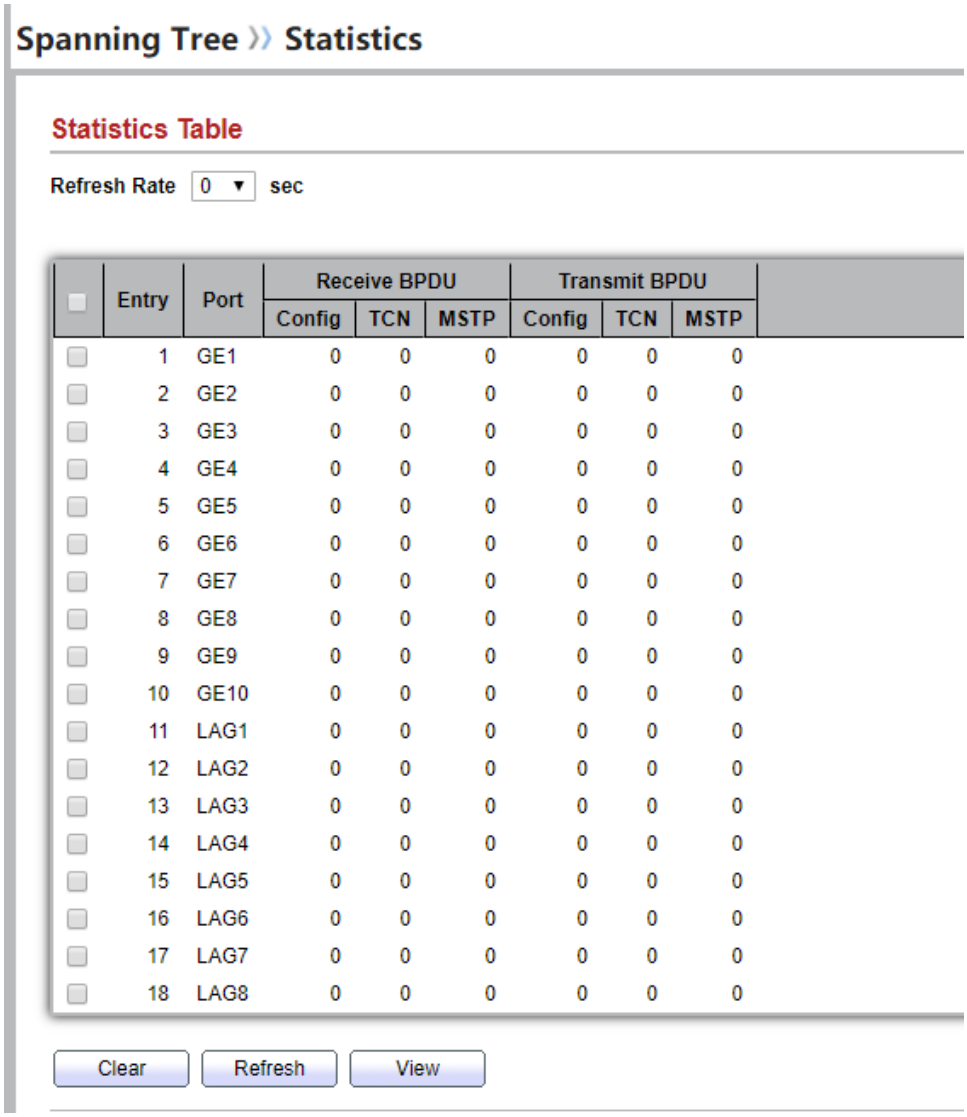


Field	Description
MSTI	MST instance ID.
Port	The port ID.
Path Cost	The port path cost on the specified MSTI.
Priority	The port priority on the specified MSTI.
Port Role	The current port role on the specified port.
Port State	The current port state on the specified port.
Mode	The operational STP mode on the specified port.
Type	The possible values for the port type are: • **Boundary:** The port is attaching an MST Bridge to a LAN that is not in the same region. • **Internal:** The port attaching an MST Bridge to a LAN that is not in the same region.
Designated Bridge	The ID of the designated bridge.
Designated Port ID	The designated port ID on the switch.
Designated Cost	The path cost of the designated port on the switch
Remaining Hop	The remaining hop count on the specified port.

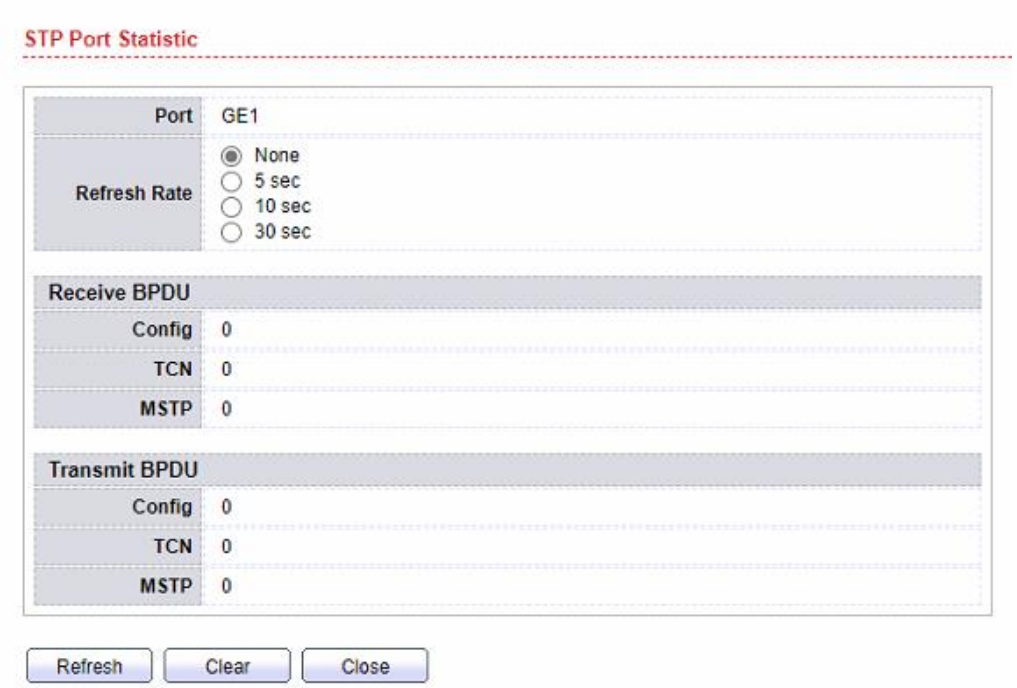


Field	Description
Path Cost	Select the STP port path coast for the MSTI
Priority	Specify the STP port priority on the MSTI.

STATISTICS



Field	Description
Refresh Rate	Select the refresh rate.
Receive BPDU (Config)	Shows the received CONFIG BPDU counts.
Receive BPDU (TCN)	Shows the received TCN BPDU counts.
Receive BPDU (MSTP)	Shows the received MSTP BPDU counts.
Transmit BPDU (Config)	Shows the transmitted CONFIG BPDU counts.
Transmit BPDU (TCN)	Shows the transmitted TCN BPDU counts.
Transmit BPDU (MSTP)	Shows the transmitted MSTP BPDU counts.
Clear	Clear the statistics for the selected interfaces
View	View the statistics for the interface.



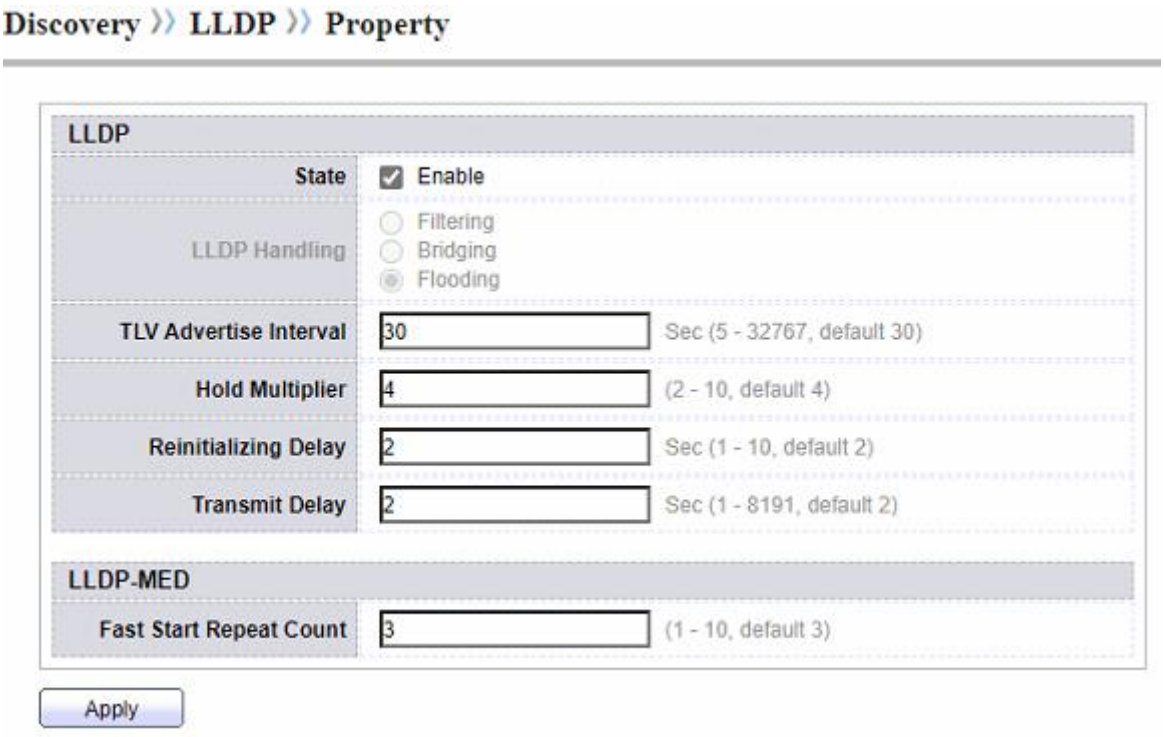
Field	Description
Refresh Rate	Select the refresh rate.
Receive BPDU (Config)	Shows the received CONFIG BPDU counts.
Receive BPDU (TCN)	Shows the received TCN BPDU counts.
Receive BPDU (MSTP)	Shows the received MSTP BPDU counts.
Transmit BPDU (Config)	Shows the transmitted CONFIG BPDU counts.
Transmit BPDU (TCN)	Shows the transmitted TCN BPDU counts.
Transmit BPDU (MSTP)	Shows the transmitted MSTP BPDU counts.
Clear	Clear the statistics for the selected interfaces
View	View the statistics for the interface.

DISCOVERY

LLDP

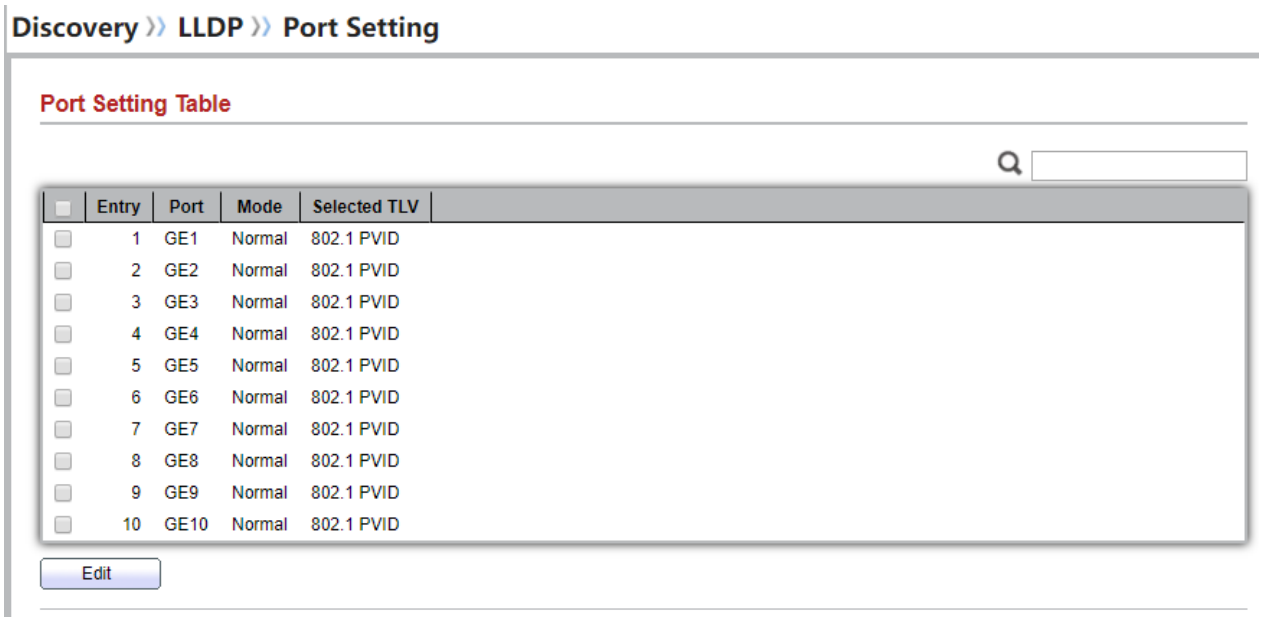
LLDP is a one-way protocol; there are no request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function.

PROPERTY

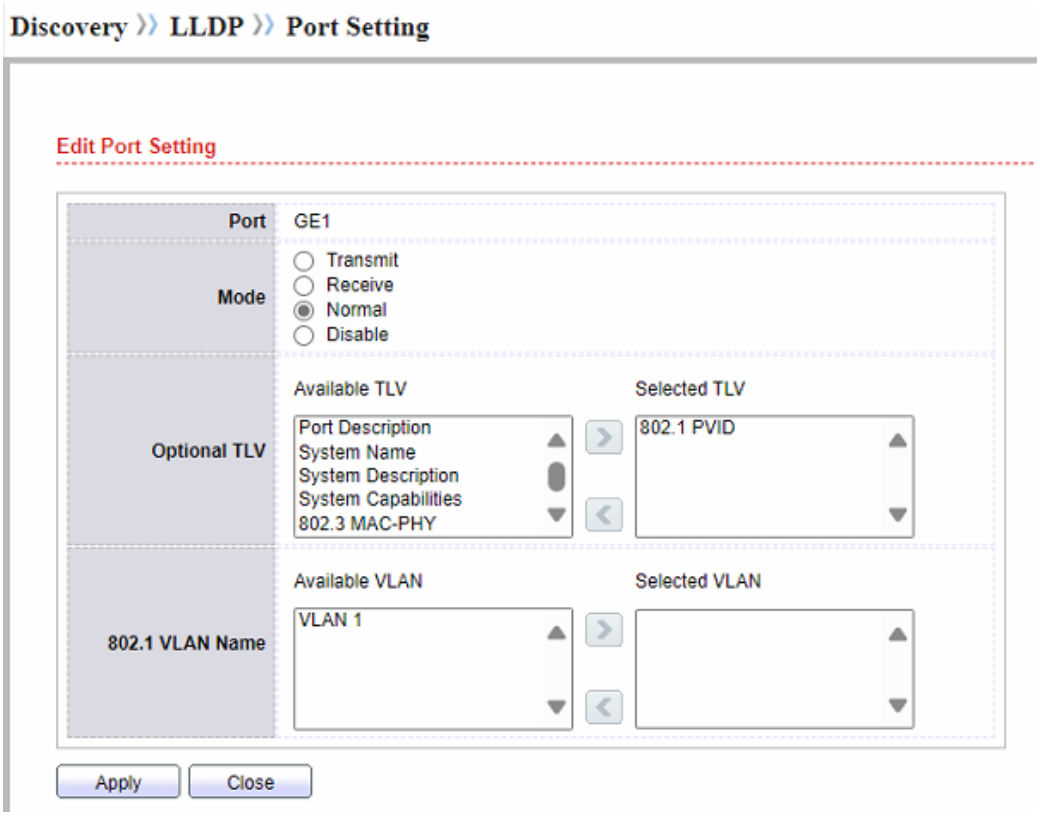


Field	Description
State	Enable or Disable LLDP
LLDP Handling	Select the LLDP PDU handling action. • **Filtering:** Deletes the packet • **Bridging:** (VLAN-aware flooding) Forwards the packet to all VLAN members. • **Flooding:** Forwards the packet to all ports
TLV Advertise Interval	Select the interval at which frames are transmitted.
Hold Multiplier	Select the multiplier on the transmit interval to assign to TTL.
Reinitialization Delay	Select the delay before a re-initialization.
Transmit Delay	Select the delay after an LLDP frame is sent.
Fast Start Repeat Count	Select the number of LLDP packets that are sent during the LLDP-MED fast-start period.

PORT SETTING

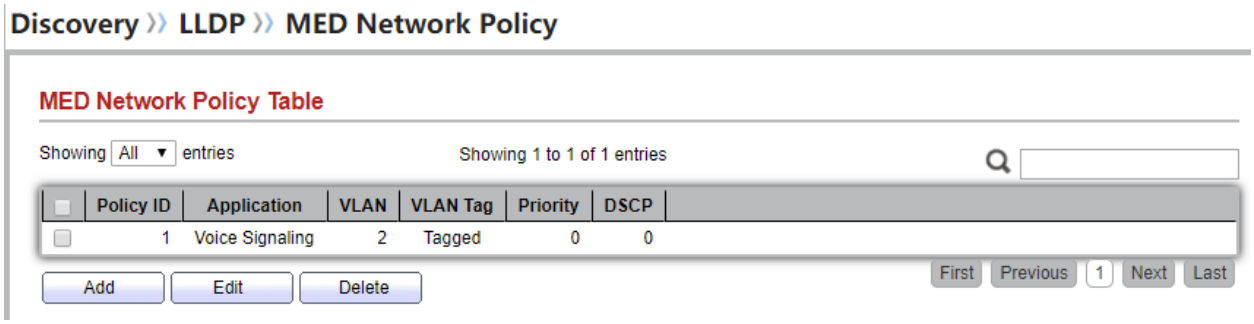


To edit a port page, select a port and click the “edit” button.



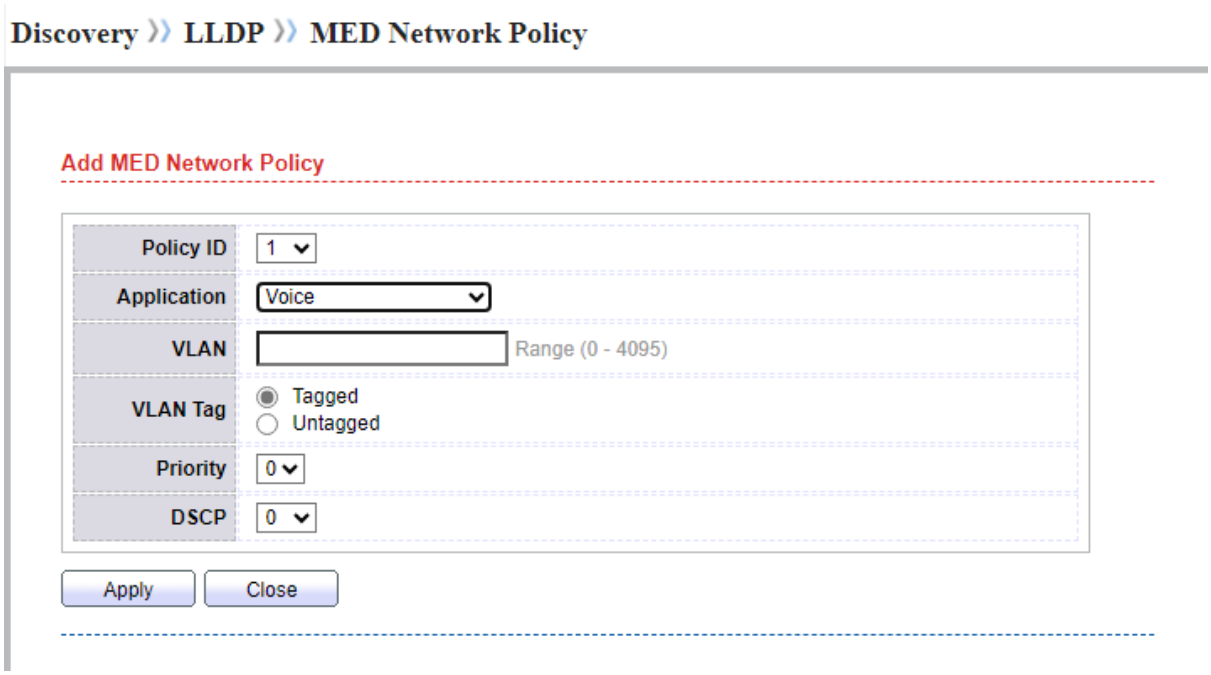
Field	Description
Port	Shows the currently selected port.
Mode	Select the transmission state of LLDP port interface. • **Transmit:** Only transmit LLDP PDU • **Receive:** Only receive LLDP PDU • **Normal:** Transmit and receive LLDP PDUs. • **Disable:** Disable the transmission of LLDP PDUs.
Optional TLV	Select the optional TLVs to be carried. • System Name • Port Description • System Description • System Capability • 802.3 MAC-PHY • 802.3 Link Aggregation • 802.3 Maximum Frame Size • Management Address 802.1 PVID
802.1 VLAN Name	Select the VLAN name ID (Multiple VLANS can be selected)

MED NETWORK POLICY



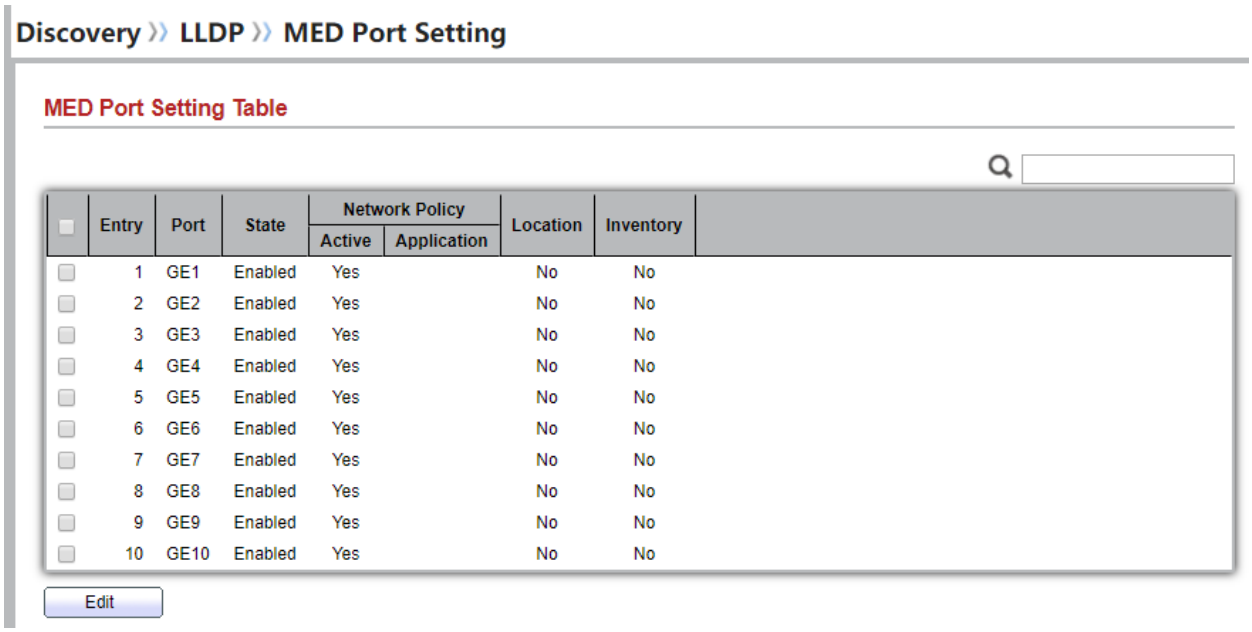
To add a MED Network Policy, select a port and click the “add” button.

To edit a port page, select a port and click the “edit” button.

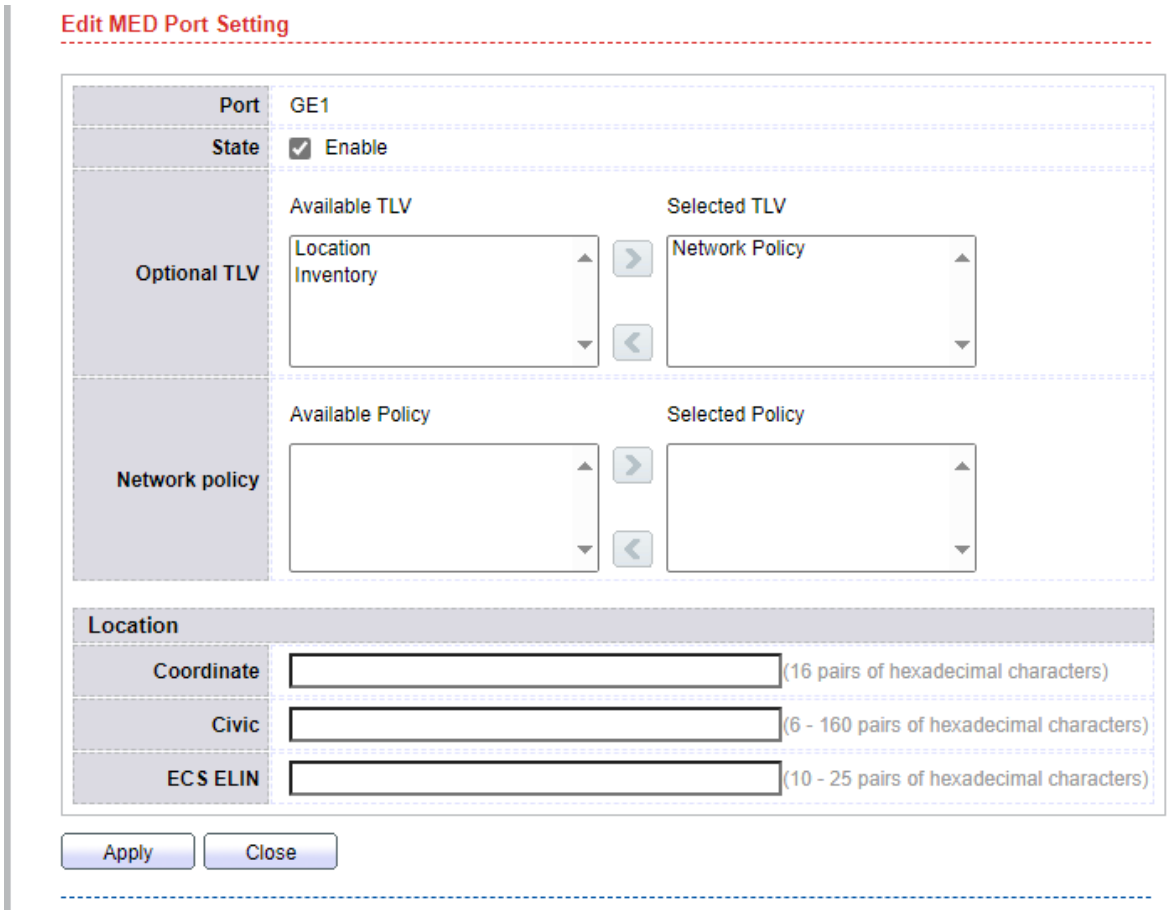


Field	Description
Policy ID	Select a network policy you wish to use.
Application	Select the network policy application type. • **Voice** • **Voice signalling** • **Guest Voice** • **Guest Voice Signalling** • **Softphone Voice** • **Video Conferencing** • **Streaming Video** • **Video Signalling**
VLAN	Set the VLAN ID you wish to use. Range is from 1 to 4094.
VLAN Tag	Select the VLAN status. • **Tagged:** Traffic is tagged • **Untagged:** Traffic is untagged
Priority	Set the L2 priority. Range is from 0 to 7.
DSCP - Differentiated Services Code Point	Set the DSCP value. Range is from 0 to 63. DSCP 0 is generally used for default traffic without a specific prioritization requirement.

MED PORT SETTING



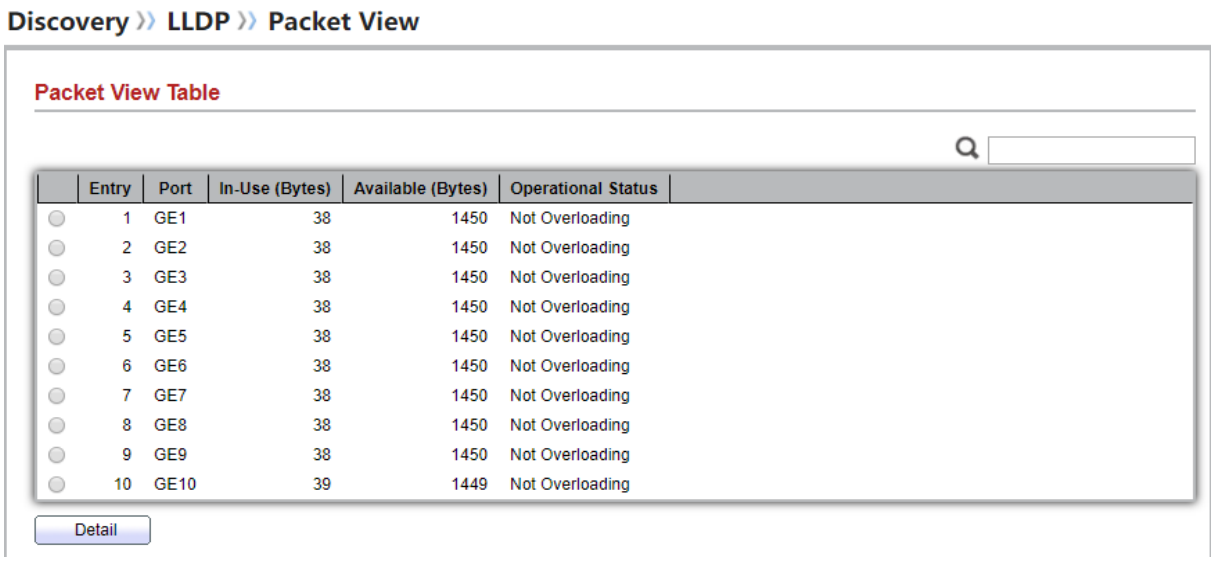
To edit a port page, select a port and click the “edit” button.



Field	Description
Port	The current port you wish to edit.
State	Enable or Disable the port setting.
Optional TLV	Select the optional TLVs to be carried. • **Network Policy** • **Location** • **Inventory**
Network Policy	Select the network policy IDs to be bound to the port. The network policy should have been created in the MED Network Policy page before it will appear here.
Field	Set the L2 priority. Range is from 0 to 7.

Field	Description
Coordinate	Set Coordinate
Civic	Set Civic
ECS ELIN	Set ECS ELIN

PACKET VIEW



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 in each packet.
Operational Status	Overloading or Not Overloading

To see the detail of a port, select a port and click the “Detail” button.

Packet View Detail

Port	GE1
Mandatory TLVs	
Size (Bytes)	21
Operational Status	Transmitted
MED Capabilities	
Size (Bytes)	9
Operational Status	Transmitted
MED Location	
Size (Bytes)	0
Operational Status	Transmitted
MED Network Policy	
Size (Bytes)	0
Operational Status	Transmitted
MED Inventory	
Size (Bytes)	0
Operational Status	Transmitted
MED Extended Power via MDI	
Size (Bytes)	0
Operational Status	Transmitted
802.3 TLVs	
Size (Bytes)	0
Operational Status	Transmitted
Optional TLVs	
Size (Bytes)	0
Operational Status	Transmitted
802.1 TLVs	
Size (Bytes)	8
Operational Status	Transmitted
Total	
In-Use (Bytes)	38
Available (Bytes)	1450

Close

Field	Description
Port	Port Name
Mandatory TLVs	Total mandatory TLV byte size.
MED Capabilities	Total MED Capabilities TLV byte size.
MED Location	Total MED Location byte size.
MED Network Policy	Total MED Network Policy byte size.
MED Inventory	Total MED Inventory byte size.
MED Extended Power via MDI	Total MED Extended Power via MDI byte size.
802.3 TLVs	Total 802.3 TLVs byte size.
Optional TLVs	Total Optional TLV byte size.
802.1 TLVs	Total 802.1 TLVs byte size.
Total	Total number of bytes of LLDP information in each packet.

LOCAL INFORMATION

Discovery » LLDP » Local Information

Device Summary

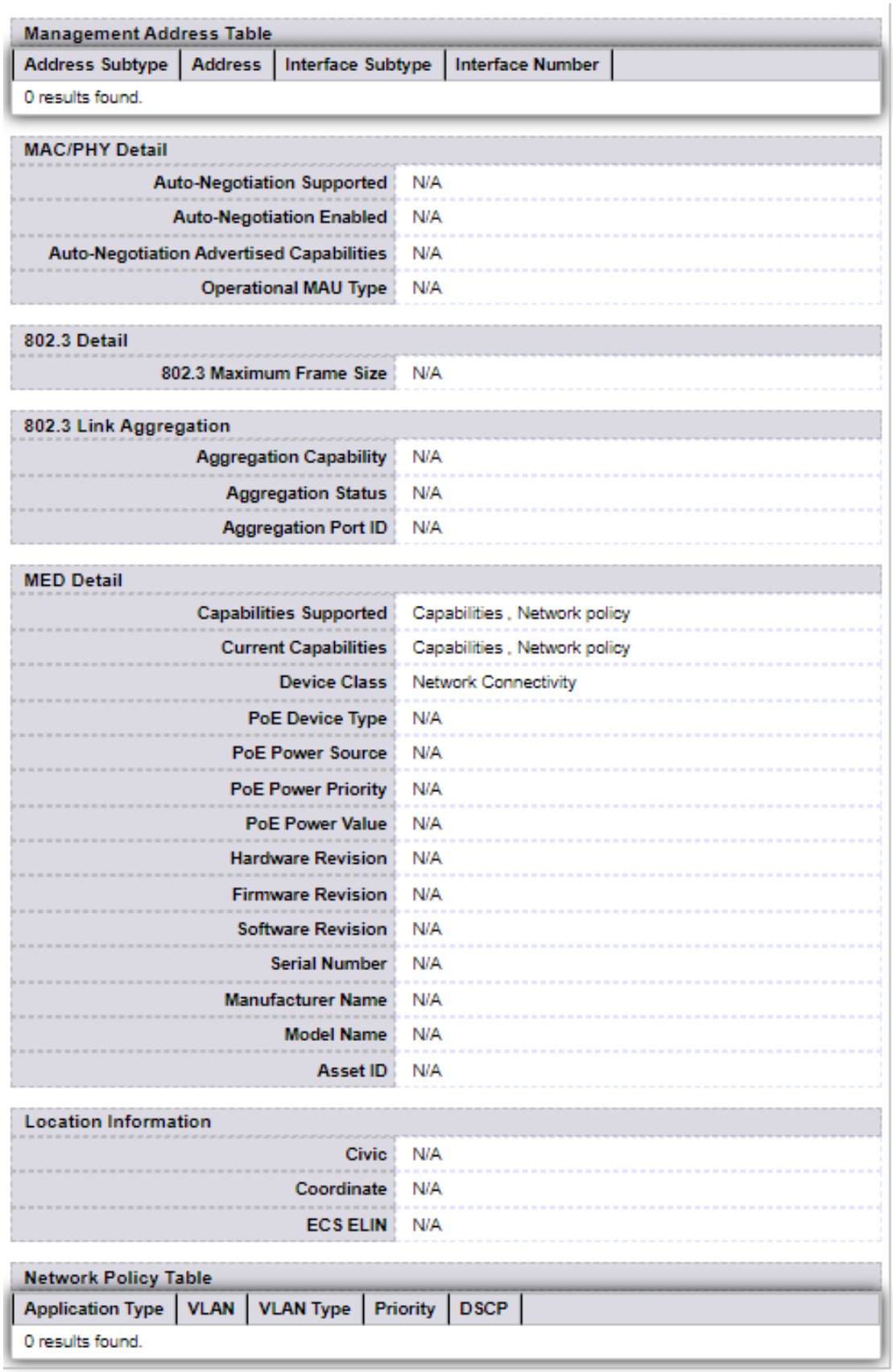
Chassis ID Subtype	MAC address
Chassis ID	50:11:EB:20:19:37
System Name	Switch
System Description	SIL 716E8C4M
Supported Capabilities	Bridge, Router
Enabled Capabilities	Bridge, Router
Port ID Subtype	Local

Port Status Table

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

Field	Description
Chassis ID	Port Name
Subtype	Total number of bytes of LLDP information in each packet.
System Name	Name of switch.
System Description	Description of the switch.
Capabilities Supported	Primary functions of the device, such as Bridge, WLAN AP, or Router.
Capabilities Enabled	Primary enabled functions of the device.
Port ID Subtype	Type of the port identifier that is shown.
LLDP Status	LLDP Tx and Rx abilities.
LLDP Med Status	LLDP MED enable state.

To see the detail of a port, select a port and click the “Detail” button.



Management Address Table

Address Subtype	Address	Interface Subtype	Interface Number
0 results found.			

MAC/PHY Detail

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

802.3 Detail

802.3 Maximum Frame Size	N/A

802.3 Link Aggregation

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

MED Detail

Capabilities Supported	Capabilities , Network policy
Current Capabilities	Capabilities , Network policy
Device Class	Network Connectivity
PoE Device Type	N/A
PoE Power Source	N/A
PoE Power Priority	N/A
PoE Power Value	N/A
Hardware Revision	N/A
Firmware Revision	N/A
Software Revision	N/A
Serial Number	N/A
Manufacturer Name	N/A
Model Name	N/A
Asset ID	N/A

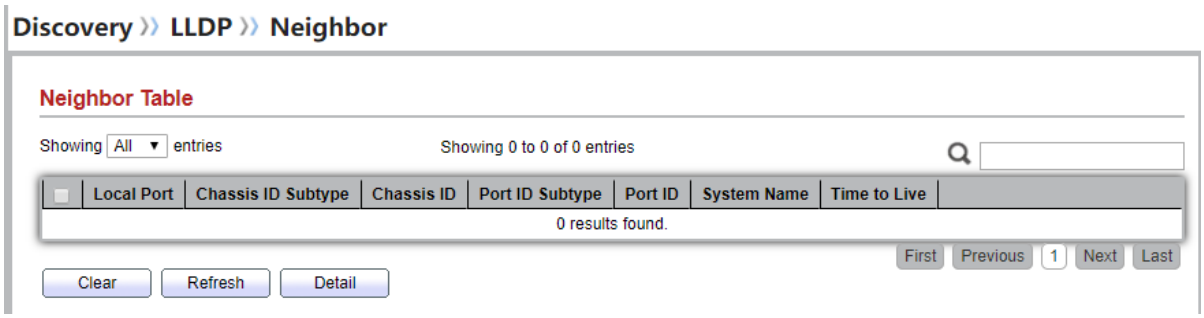
Location Information

Civic	N/A
Coordinate	N/A
ECS ELIN	N/A

Network Policy Table

Application Type	VLAN	VLAN Type	Priority	DSCP
0 results found.				

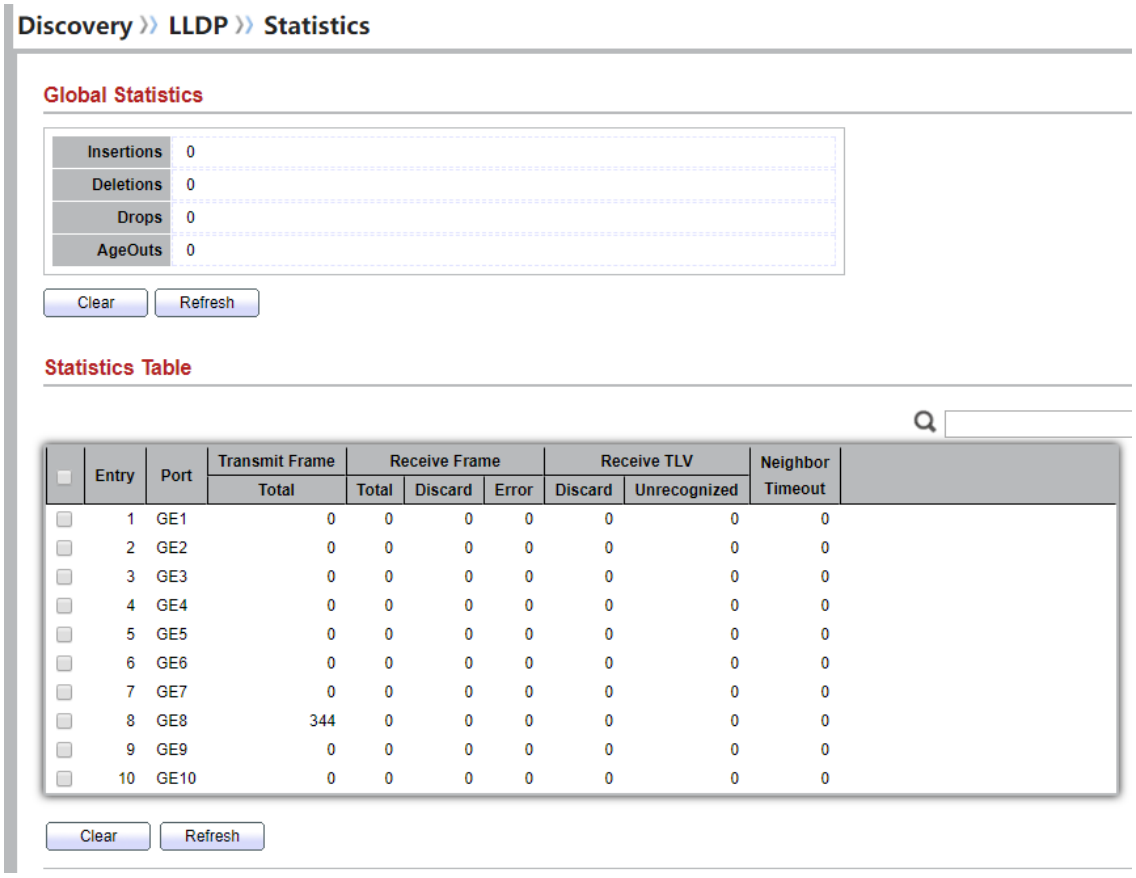
NEIGHBOUR



Field	Description
Local Port	Number of the local port to which the neighbour is connected.
Chassis ID Subtype	Type of chassis ID (for example, MAC address).
Chassis ID	Identifier of the 802 LAN neighbouring 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 neighbour is deleted.

To see the detail of a port, select a port and click the “Detail” button.

STATISTICS



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 systems 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.

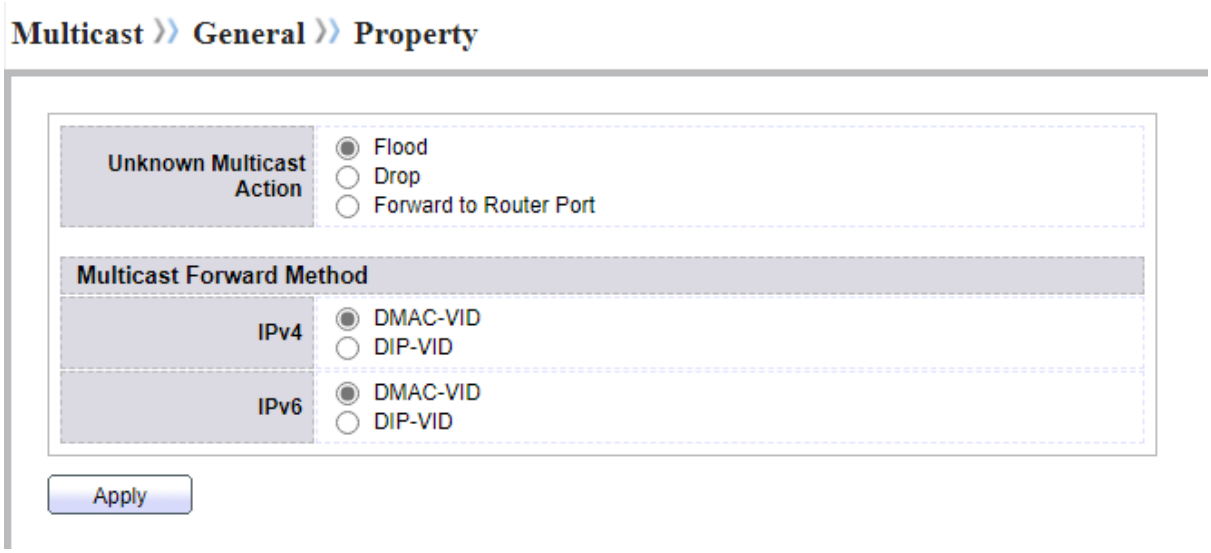
Receive Frame Error	Number of invalid LLDP frames received by the LLDP agent on the corresponding port, while the LLDP agent is enabled.
Receive TLV Discard	Number of TLVs of LLDP frames discarded for any reason by the LLDP agent on the corresponding port.
Receive TLV Unrecognized	Number of TLVs of LLDP frames that are unrecognised while the LLDP agent is enabled
Neighbour Timeout	Number of age out LLDP frames.

MULTICAST

These pages allow you to set multicast forwarding methods and unknown multicast actions.

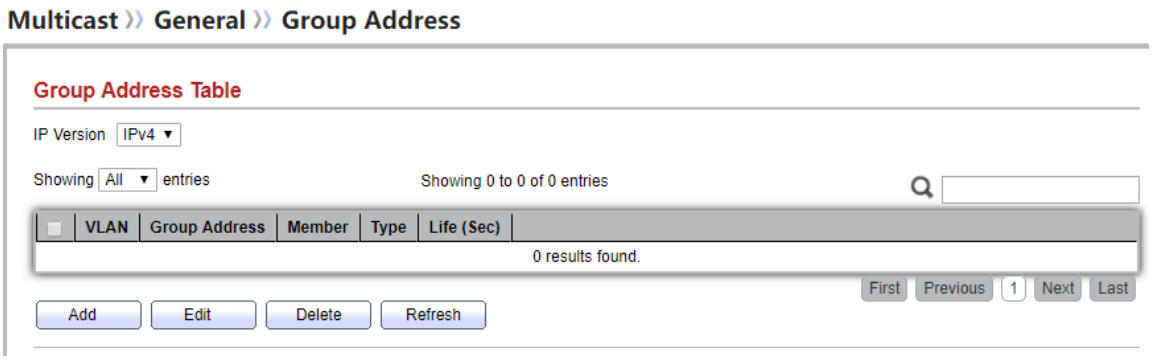
GENERAL

PROPERTY



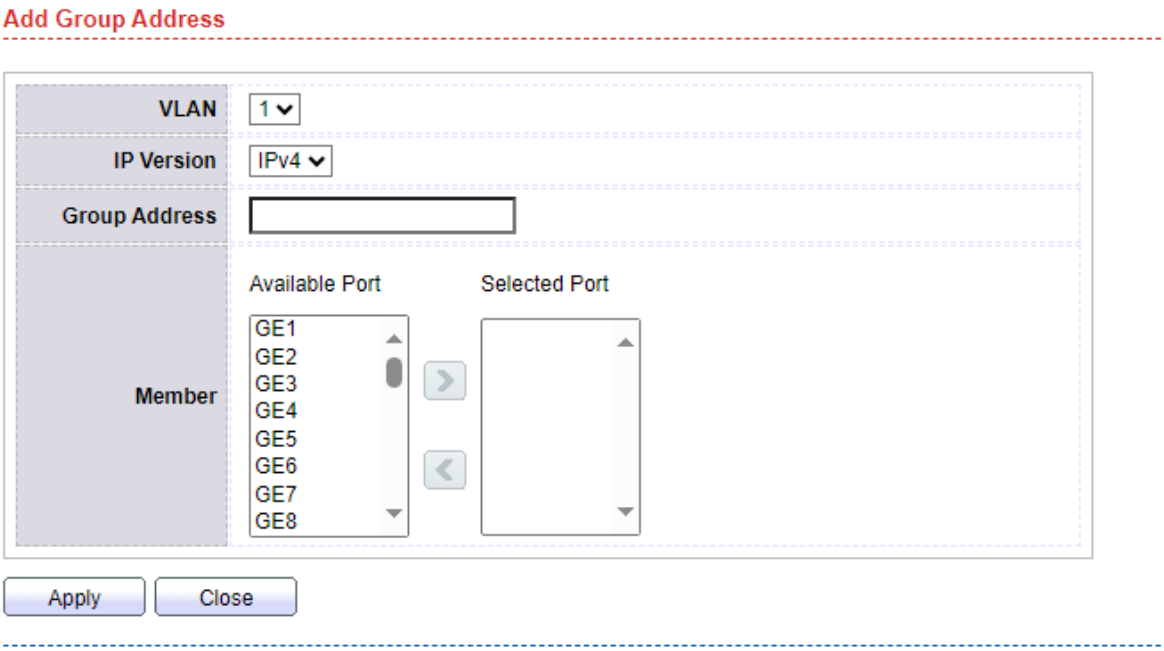
Field	Description
Unknown Multicast Action	Set the unknown multicast action. • **Drop:** drop the unknown multicast data. • **Flood:** flood the unknown multicast data. • **Router port:** forward the unknown multicast data to router port.
IPv4	Set the ipv4 multicast forward method. • **MAC-VID:** forward method dmac+vid. • **DIP-VID:** forward method dip+vid.
IPv6	Set the ipv6 multicast forward method. • **MAC-VID:** forward method dmac+vid. • **DIP-VID:** forward method dip+vid(dip is ipv6 low 32 bit).

GROUP ADDRESS



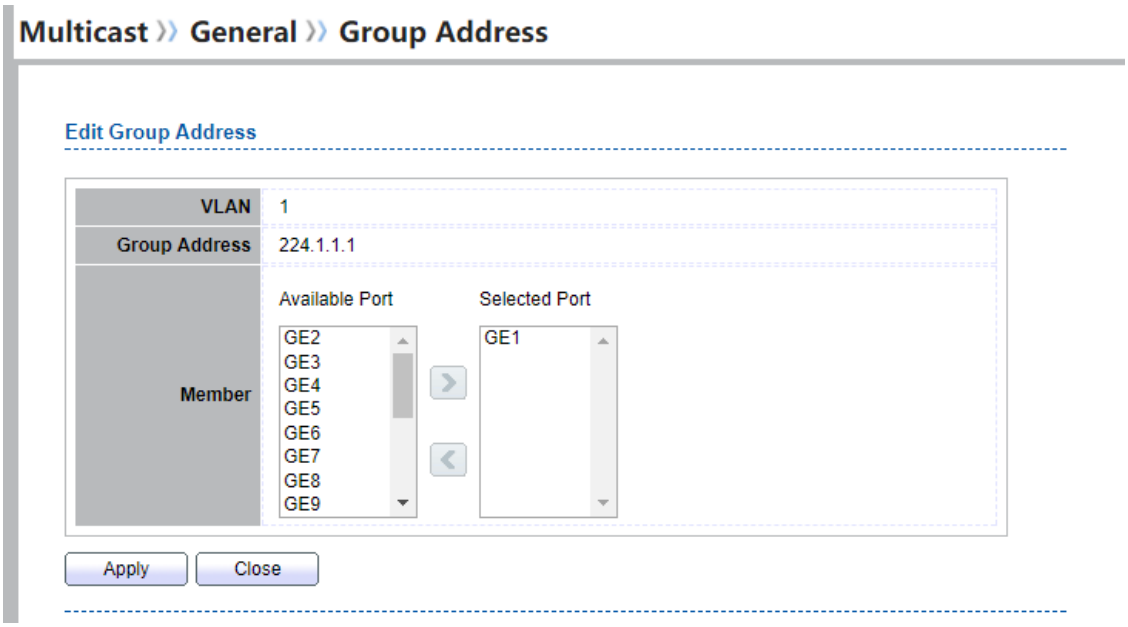
Field	Description
IP Version	IP Version • **IPv4:** ipv4 multicast group • **IPv6:** ipv6 multicast group
VLAN	The VLAN ID of group.
Group Address	The group IP address.
Member	The member ports of group.
Type	The type of group. Static or Dynamic.
Life (Sec)	The time of this dynamic group.

To add a Group Address, select a port and click the “add” button.



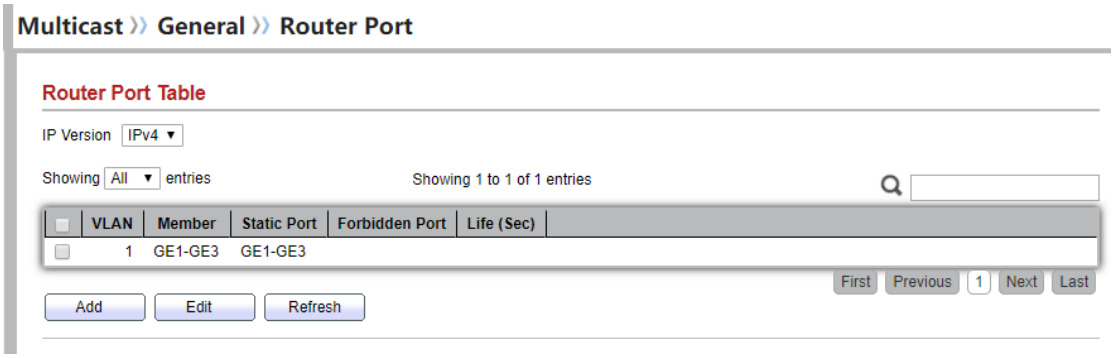
Field	Description
VLAN	The VLAN ID of group.
IP Version	IP Version • **IPv4:** ipv4 multicast group • **IPv6:** ipv6 multicast group
Group Address	The group IP address.
Member	The member ports of group. • **Available Port:** Optional port member • **Selected Port:** Selected port member

To edit a port page, select a port and click the “edit” button.



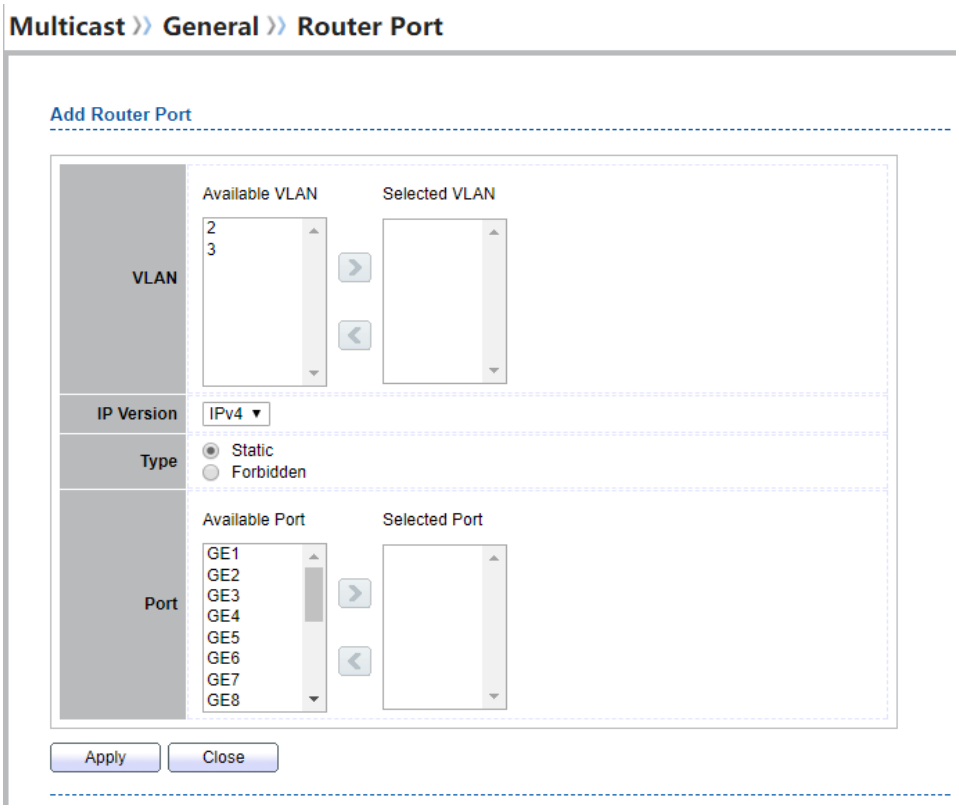
Field	Description
VLAN	The VLAN ID of group.
Group Address	The group IP address.
Member	The member ports of group. • **Available Port:** Optional port member • **Selected Port:** Selected port member

ROUTER PORT



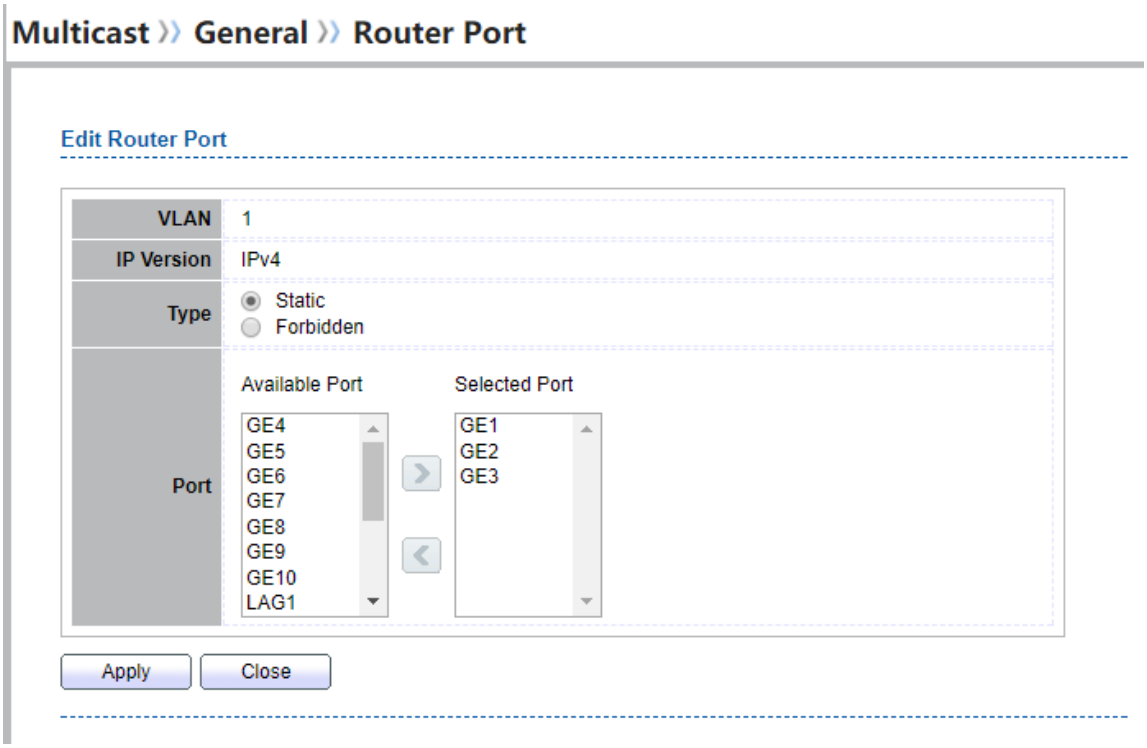
Field	Description
IP Version	IP Version • **IPv4:** ipv4 multicast group • **IPv6:** ipv6 multicast group
VLAN	The VLAN ID of group.
Member	Router Port member (includes static and learned port member).
Static Port	Static router port member.
Forbidden Port	Forbidden router port member.
Life (Sec)	The expiry time of the router entry.

To add a Router Port, select a port and click the “add” button.



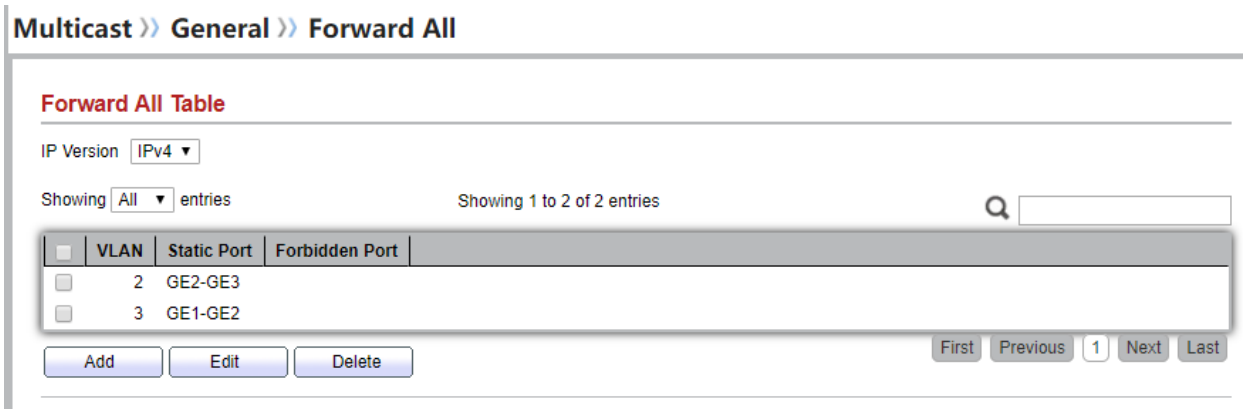
Field	Description
VLAN	The VLAN ID for router entry. • **Available VLAN:** Optional VLAN member • **Selected VLAN:** Selected VLAN member
IP Version	IP Version • **IPv4:** ipv4 multicast group • **IPv6:** ipv6 multicast group
Type	The router port type • **Static:** static router port • **Forbidden:** forbidden router port
Port	The member ports of router entry. • **Available Port:** Selectable port members • **Selected Port:** Selected port members

To edit a port page, select a port and click the “edit” button.



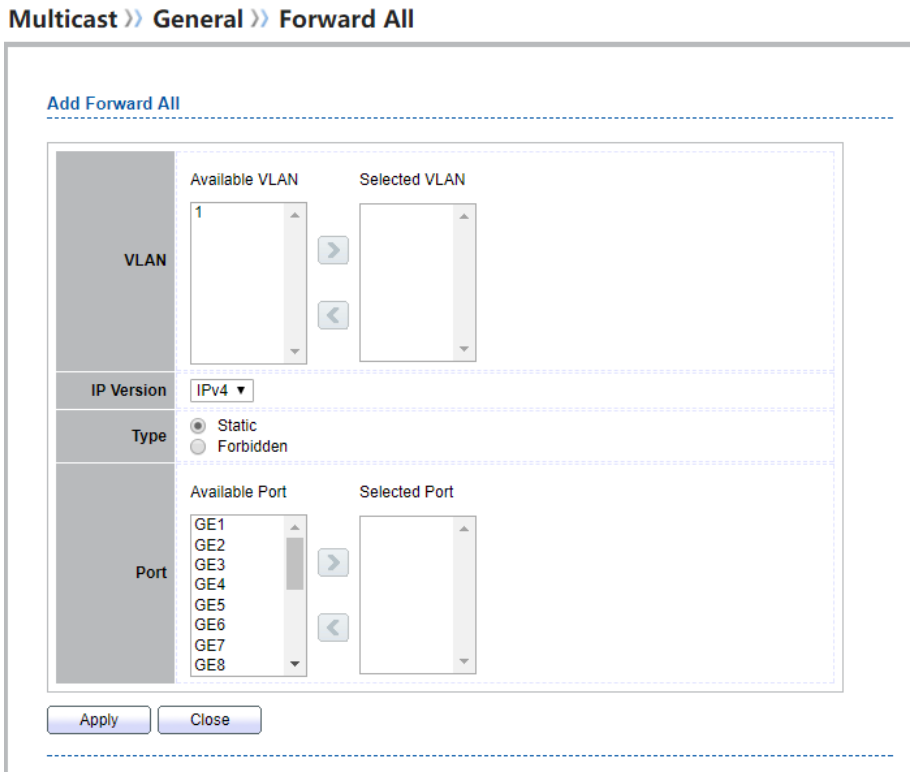
Field	Description
VLAN	The VLAN ID for router entry.
IP Version	Selected IP Version
Type	The router port type • **Static:** static router port • **Forbidden:** forbidden router port
Port	The member ports of router entry. • **Available Port:** Selectable port members • **Selected Port:** Selected port members

FORWARD ALL



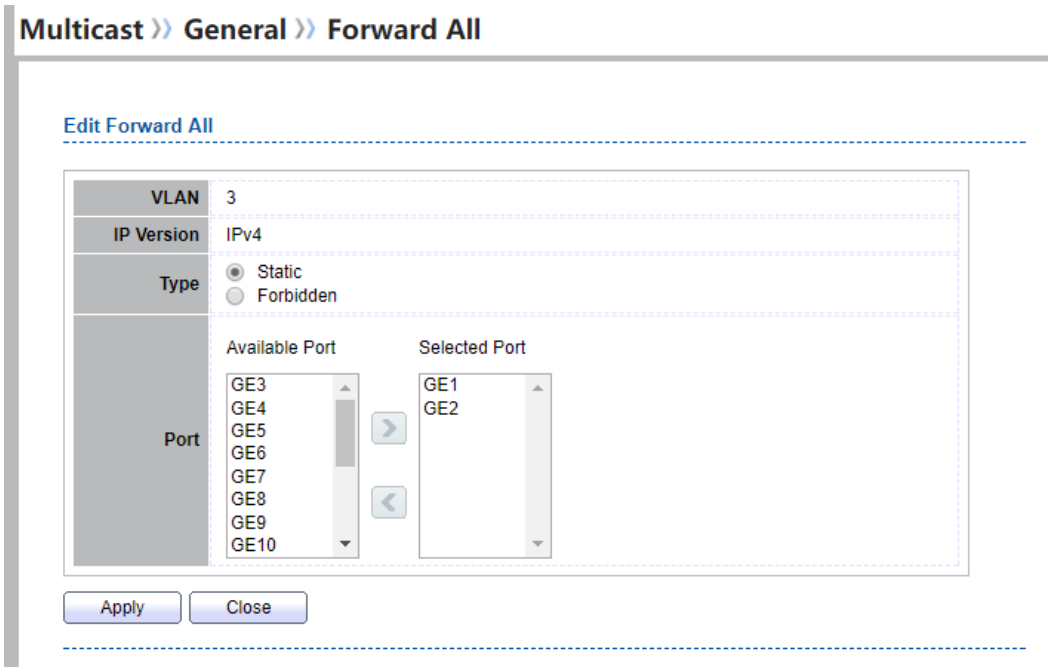
Field	Description
IP Version	IP Version • **IPv4:** ipv4 multicast forward all • **IPv6:** ipv6 multicast forward all
VLAN	The VLAN ID of the forward all entry
Static Port	Allowed Forward All port member.
Forbidden Port	Forbidden Forward All port member.

To add a Forward All rule, click the “add” button.



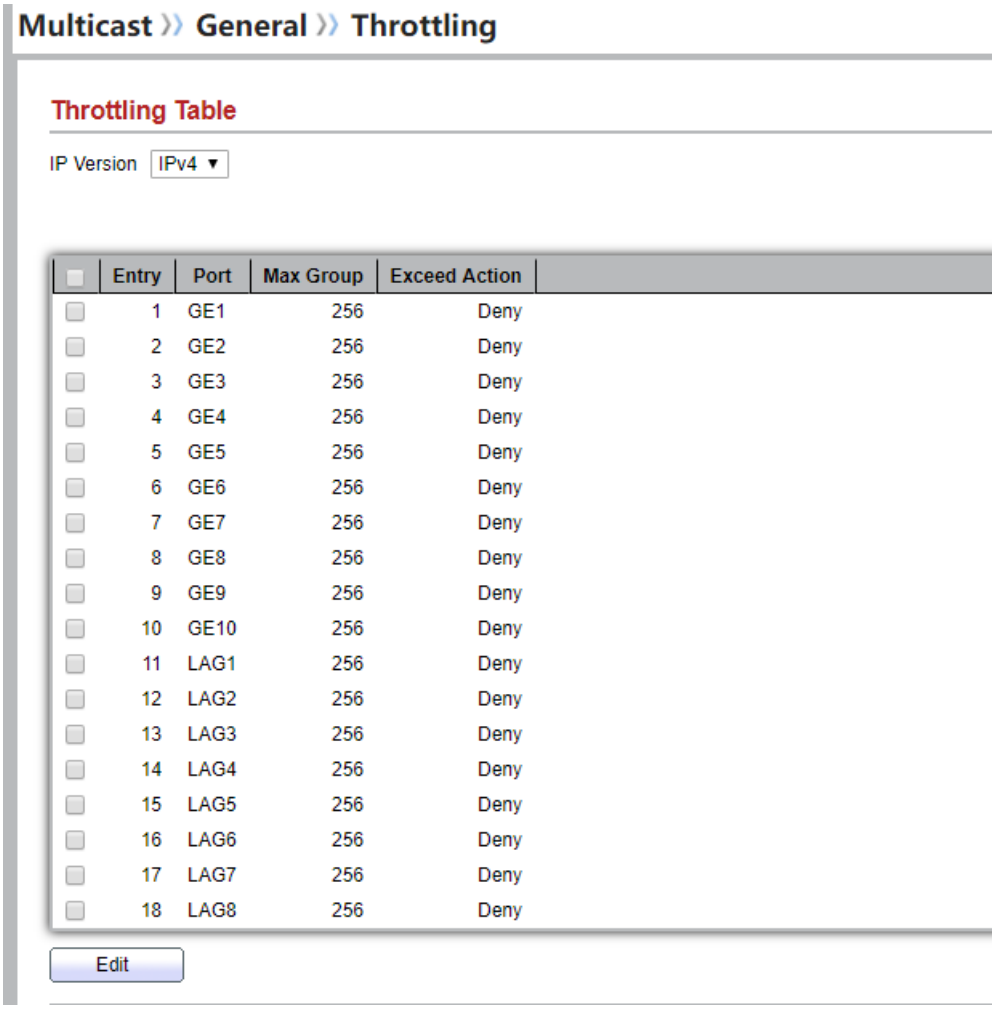
Field	Description
VLAN	The VLAN ID for router entry. • **Available VLAN:** Optional VLAN member • **Selected VLAN:** Selected VLAN member
IP Version	IP Version • **IPv4:** ipv4 multicast forward all • **IPv6:** ipv6 multicast forward all
Type	The router port type • **Static:** static forward all port • **Forbidden:** forbidden forward all port
Port	The member ports of router entry. • **Available Port:** Selectable port members • **Selected Port:** Selected port members

To edit a port page, select a port and click the “edit” button.



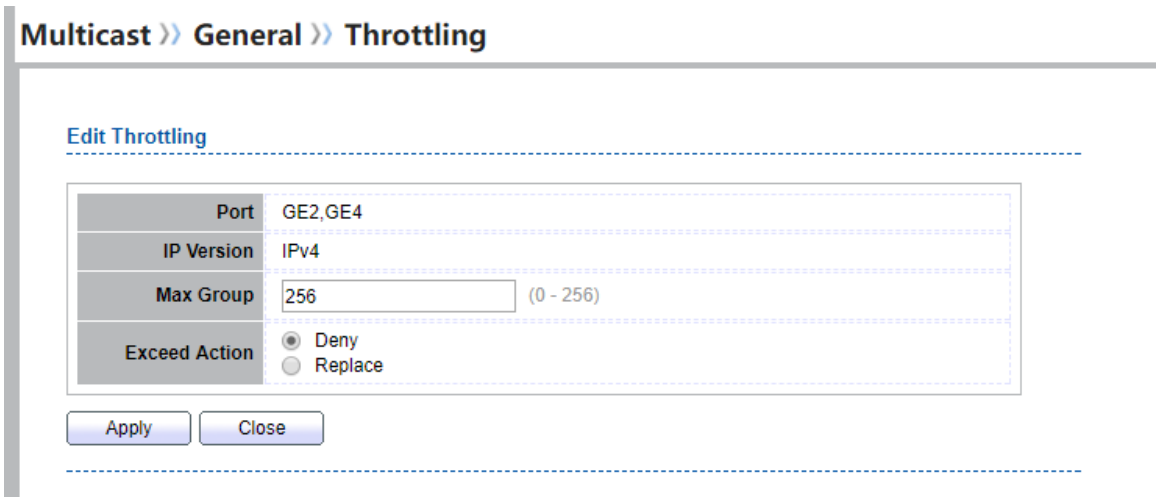
Field	Description
VLAN	The VLAN ID for forward all entry.
IP Version	Selected IP Version
Type	The router port type • **Static:** static router port • **Forbidden:** forbidden router port
Port	The member ports of router entry. • **Available Port:** Selectable port members • **Selected Port:** Selected port members

THROTTLING



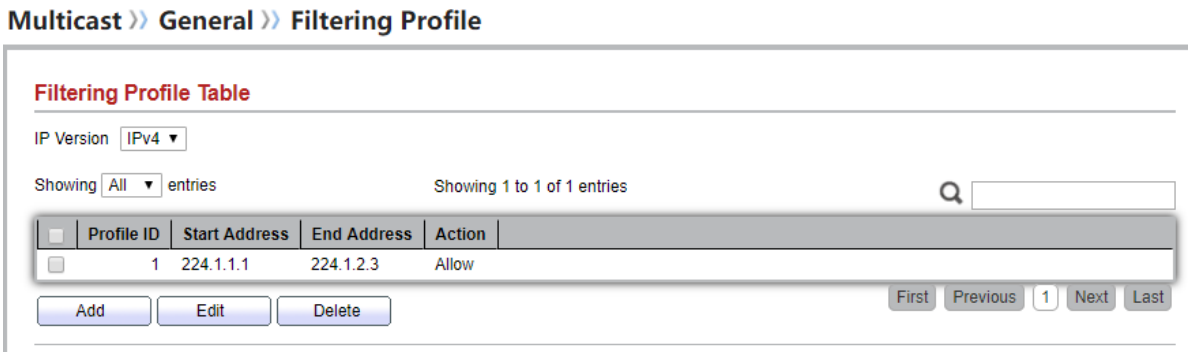
Field	Description
IP Version	IP Version • **IPv4:** ipv4 for igmp snooping throttling • **IPv6:** ipv6 for mld snooping throttling
Entry	Number of Entry.
Port	Port Name.
Max Group	Max group size.
Forbidden Port	Displays the Exceed Action

To edit an entry, select one and click the “edit” button.



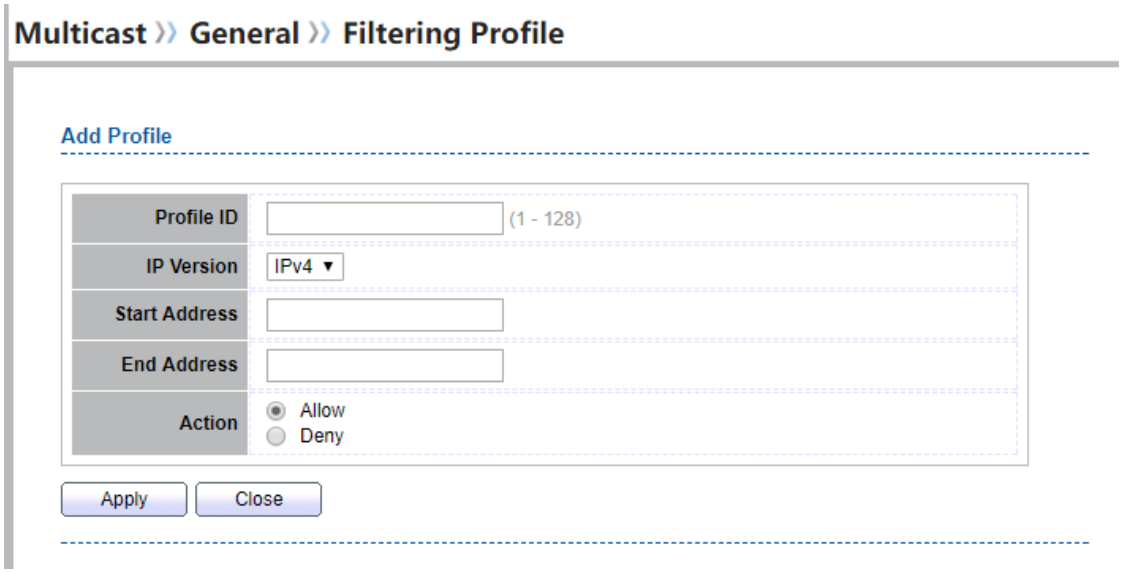
Field	Description
Port	Display the selected port list
IP Version	Display the selected IP version
Max Group	Max number of group for port
Exceed Action	Denies or replaces the existing group with the new group when the limit is reached.

FILTERING PROFILE



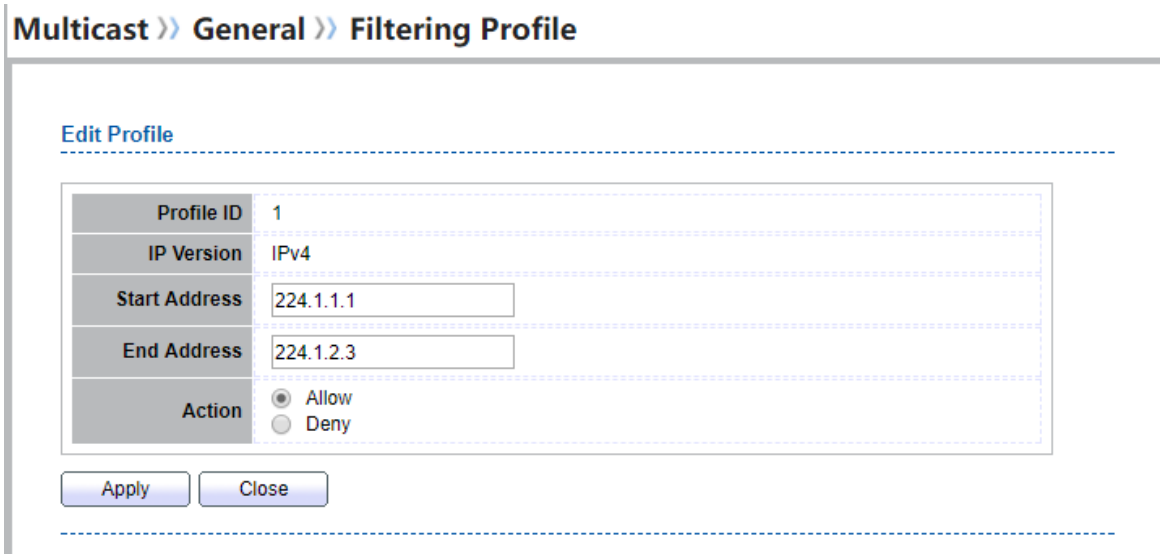
Field	Description
IP Version	IP Version • **IPv4:** ipv4 for igmp snooping profile • **IPv6:** ipv6 for mld snooping profile
Profile ID	Displays the profile ID
Start Address	The start address of the group profile
End Address	The end address of the group profile
Action	Displays the profil Action

To add a profile for IGMP or MLD snooping, click the “add” button.



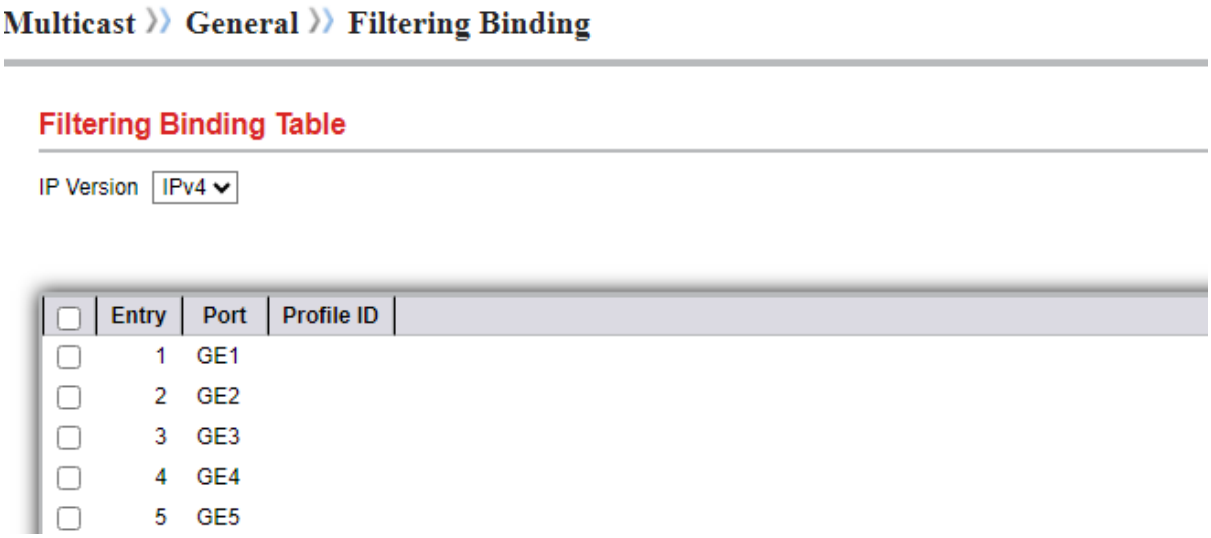
Field	Description
Profile ID	Displays the profile ID
IP Version	IP Version • **IPv4:** ipv4 for igmp snooping profile • **IPv6:** ipv6 for mld snooping profile
Start Address	The start address of the group profile
End Address	The end address of the group profile
Action	Displays the profil Action

To edit an entry, select one and click the “edit” button.



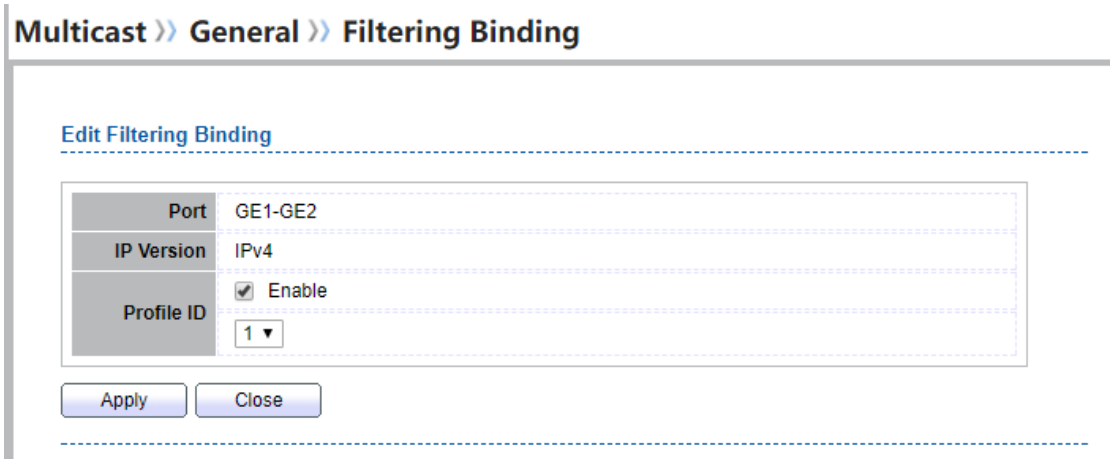
Field	Description
Profile ID	Displays the profile ID
IP Version	IP Version • **IPv4:** ipv4 for igmp snooping profile • **IPv6:** ipv6 for mld snooping profile
Start Address	The start address of the group profile
End Address	The end address of the group profile
Action	Displays the profil Action

FILTERING BINDING



Field	Description
IP Version	IP Version • **IPv4:** ipv4 for igmp snooping profile • **IPv6:** ipv6 for mld snooping profile
Entry	The number of the Entry
Port	Port name
Profile ID	Port binding profile ID

To edit a profile, select the entry and click the “edit” button.



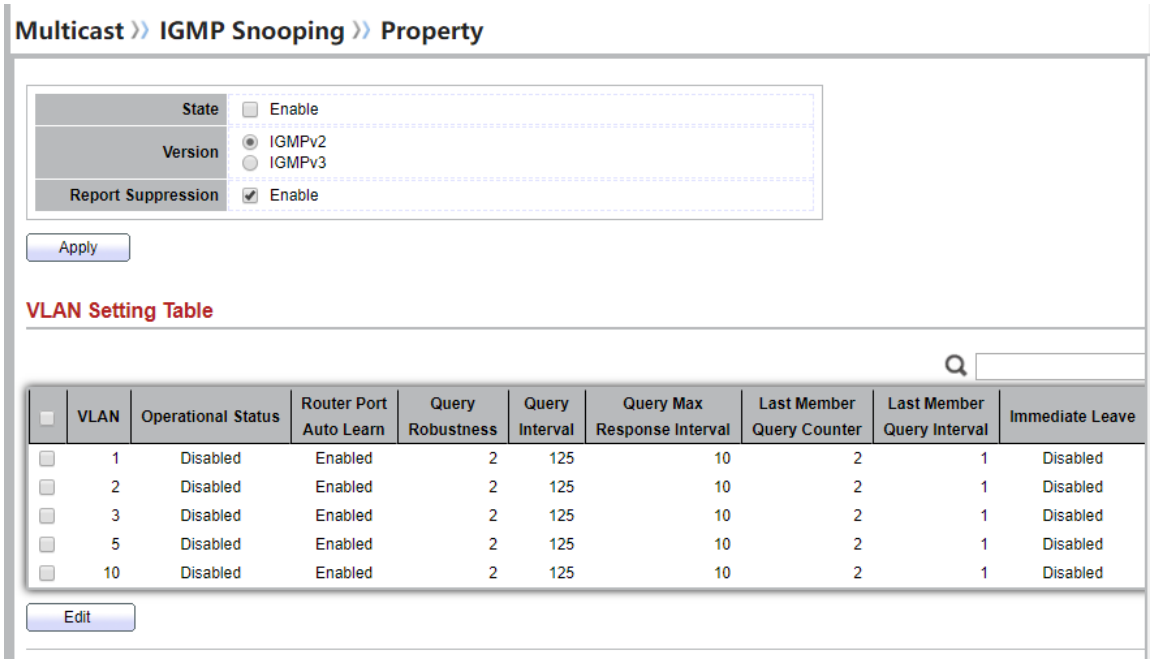
Field	Description
Port	Selected port list
IP Version	Displays the selected IP version
Profile ID	If enabled, allows you to select or change the Profile ID

IGMP SNOOPING

Use these pages to configure IGMP snooping.

PROPERTY

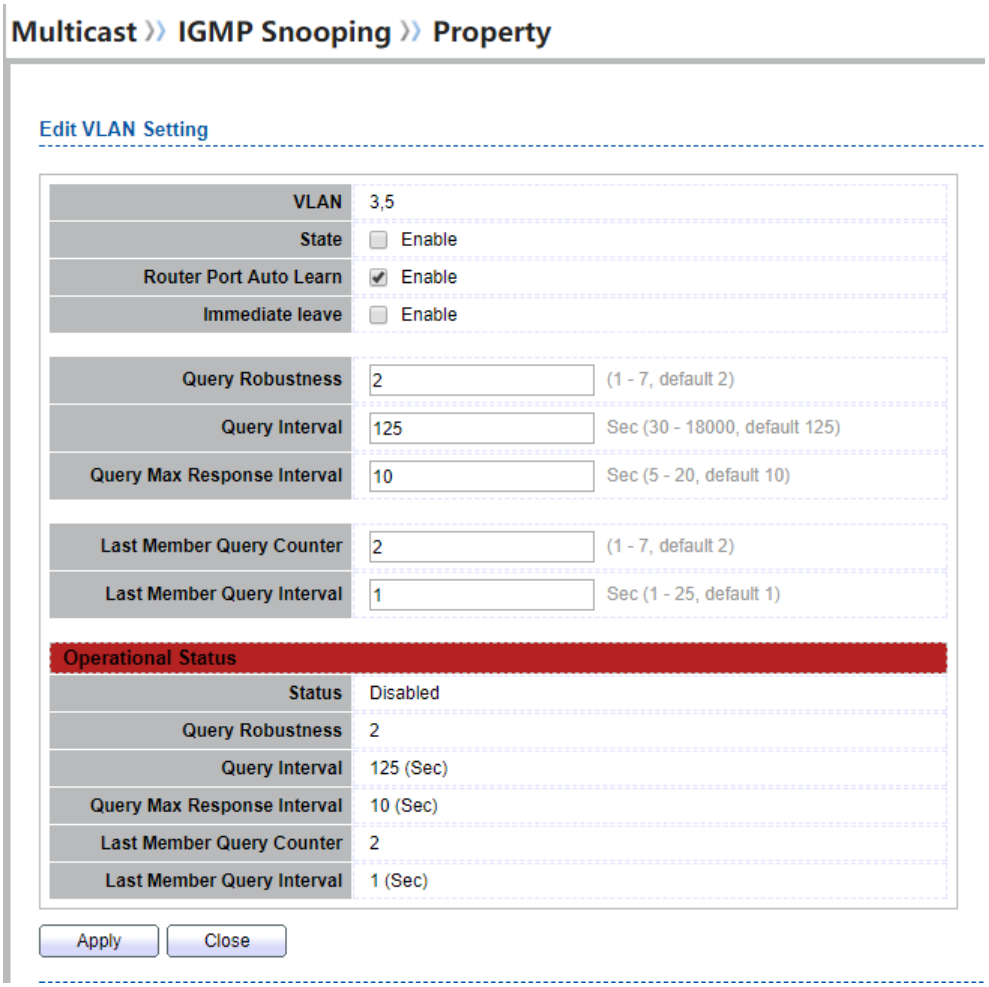
This page allows you to configure global settings for IGMP snooping and configure specific VLAN settings for IGMP Snooping



Field	Description
State	Enable/disable the IGMP Snooping functionality
Version	Set the igmp snooping version • IGMPv2: Only supports igmp v2. • IGMPv3: Support v3 basic and v2.
Report Suppression	Enable/disable the IGMP Snooping report suppression functionality
VLAN	The IGMP entry VLAN ID
Operation Status	Shows the status of the IGMP snooping VLAN functionality
Router Port Auto Learn	Shows the status of the IGMP snooping router port auto learning
Query Robustness	The Query Robustness allows tuning for the expected packet loss on a subnet.
Query Interval	The interval of querier to send general query
Query Max Response Interval	specifies the maximum allowed time before sending a responding report. Selectable in units of 1/10 second.
Last Member Query count	Shows the number of group-specific queries that a querier sends after receiving a leave message.

Last Member Query Interval	The interval at which the Group-Specific Queries are sent is called last member query interval.
Immediate leave	The immediate leave status. If enabled, the router will not send IGMP group-specific host queries when a leave group message is received from that interface.

To edit a profile, select the entry and click the “edit” button.

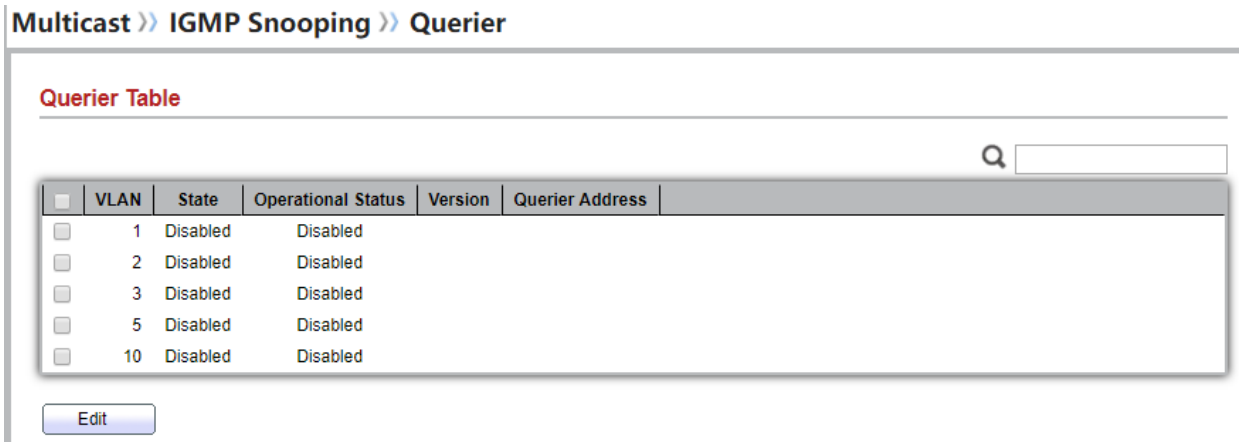


Field	Description
VLAN	Shows the Selected VLANs.
State	Enable/disable the IGMP Snooping functionality.
Router Port Auto Learn	Shows the status of the IGMP snooping router port auto learning.
Immediate leave	The immediate leave status. If enabled, the router will not send IGMP group-specific host queries when a leave group message is received from that interface.
Query Robustness	The Query Robustness allows tuning for the expected packet loss on a subnet.
Query Interval	The interval of querier to send general query.

Query Max Response Interval	specifies the maximum allowed time before sending a responding report. Selectable in units of 1/10 second.
Last Member Query count	Shows the number of group-specific queries that a querier sends after receiving a leave message.
Last Member Query Interval	The interval at which the Group-Specific Queries are sent is called last member query interval.

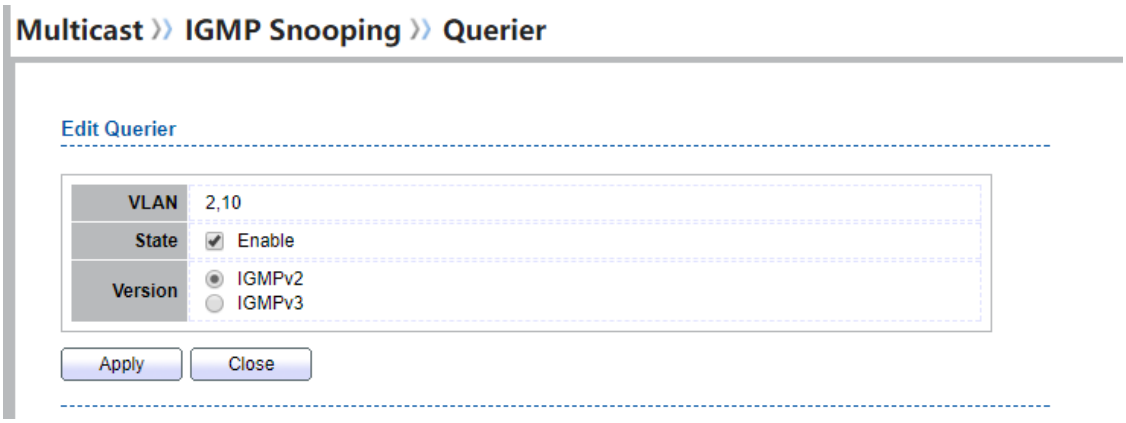
QUERIER

This page allows you to configure querier settings for specific VLAN settings for IGMP Snooping



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

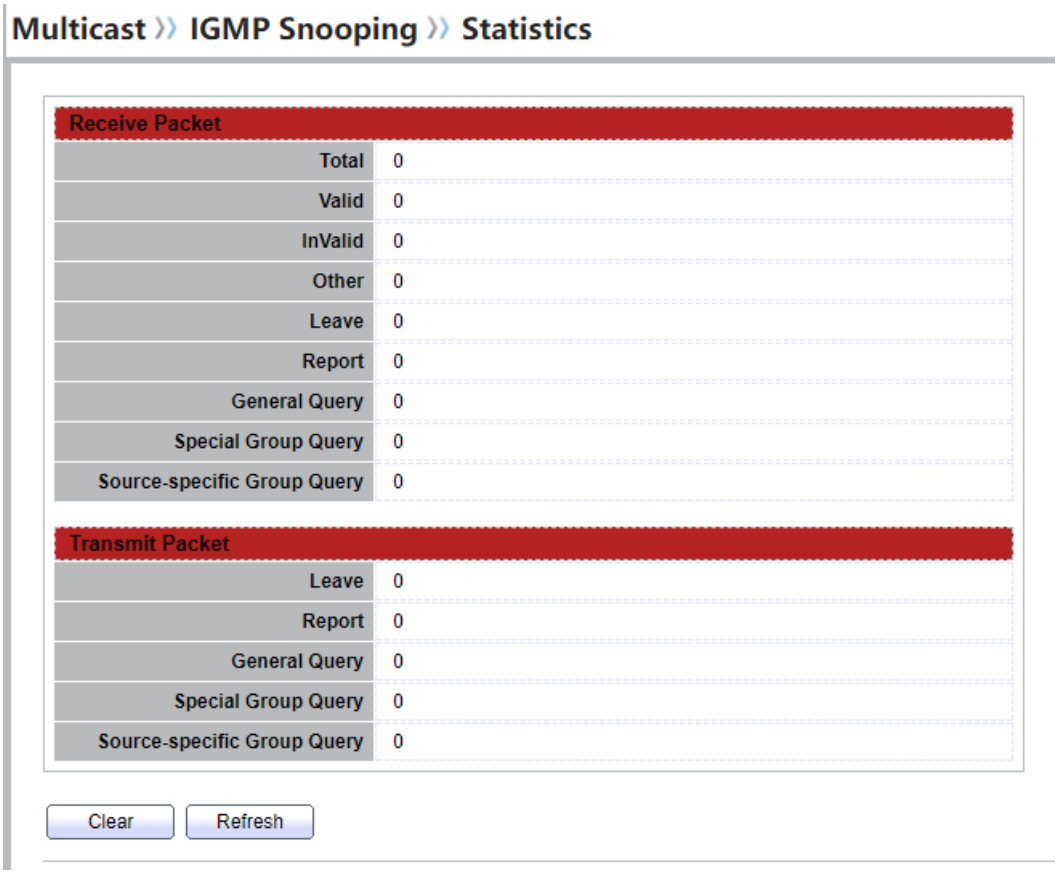
To edit a profile, select the entry and click the “edit” button.



Field	Description
VLAN	Shows the Selected VLANs list.
State	Enable/disable the IGMP Querier functionality.
Version	Select the version of IGMP.

STATISTICS

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



Field	Description
Total	All IGMP-related packets received by the CPU, including IPv4 multicast data packets.
Valid	Packets that successfully pass IGMP Snooping processing (correct format, correct IGMP type, valid checksum, valid group address).
Invalid	Packets that fail IGMP Snooping processing due to malformed structure, incorrect IGMP type, invalid checksum, or unsupported group address.
Other	Packets received that are not IGMP (type 2) and not IPv4 multicast data. Typically includes ICMP, unicast IPv4, or other L3 protocols.
Leave	IGMP Leave Group messages (host leaving a multicast group).
Report	IGMP Membership Report / Join messages (host joining or reporting membership in a multicast group).

General Query	IGMP General Query messages (querier asking all hosts to report membership for all groups).
Special Group Query	IGMP Group-Specific Query messages (querier asking hosts to report membership for one specific group).
Source-specific Group Query	IGMP Source-Specific Query messages (querier asking hosts to report membership for one group and one or more specific sources).
Transmit Packet	
Leave	IGMP Leave messages transmitted by the switch (rare; typically only forwarded, not generated).
Report	IGMP Membership Report / Join messages transmitted or forwarded.
General Query	General Query messages transmitted by the switch when acting as IGMP Querier.
Special Group Query	Group-Specific Query messages transmitted by the switch when acting as IGMP Querier.
Source-specific Group Query	Source-Specific Query messages transmitted by the switch when acting as IGMP Querier.

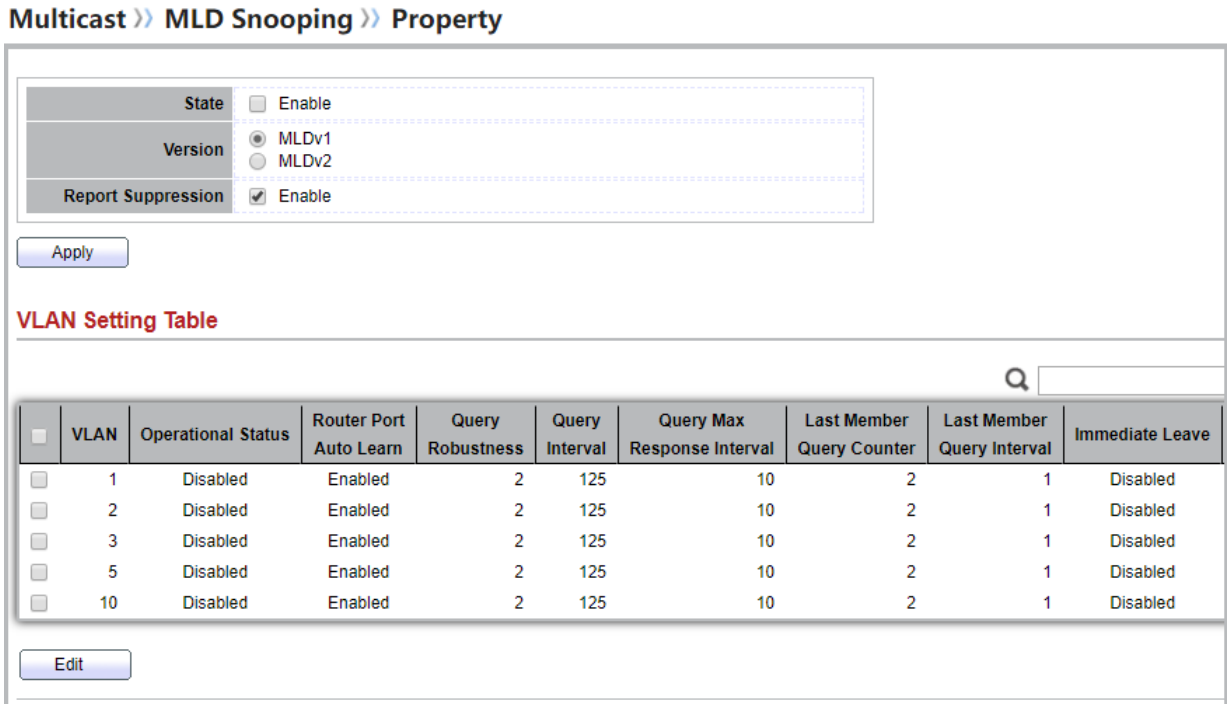
MLD SNOOPING

Use the MLD Snooping pages to configure settings for the MLD snooping function.

PROPERTY

To view the MLD Snooping Global Settings and VLAN Settings page, go to Multicast > MLD Snooping > Property.

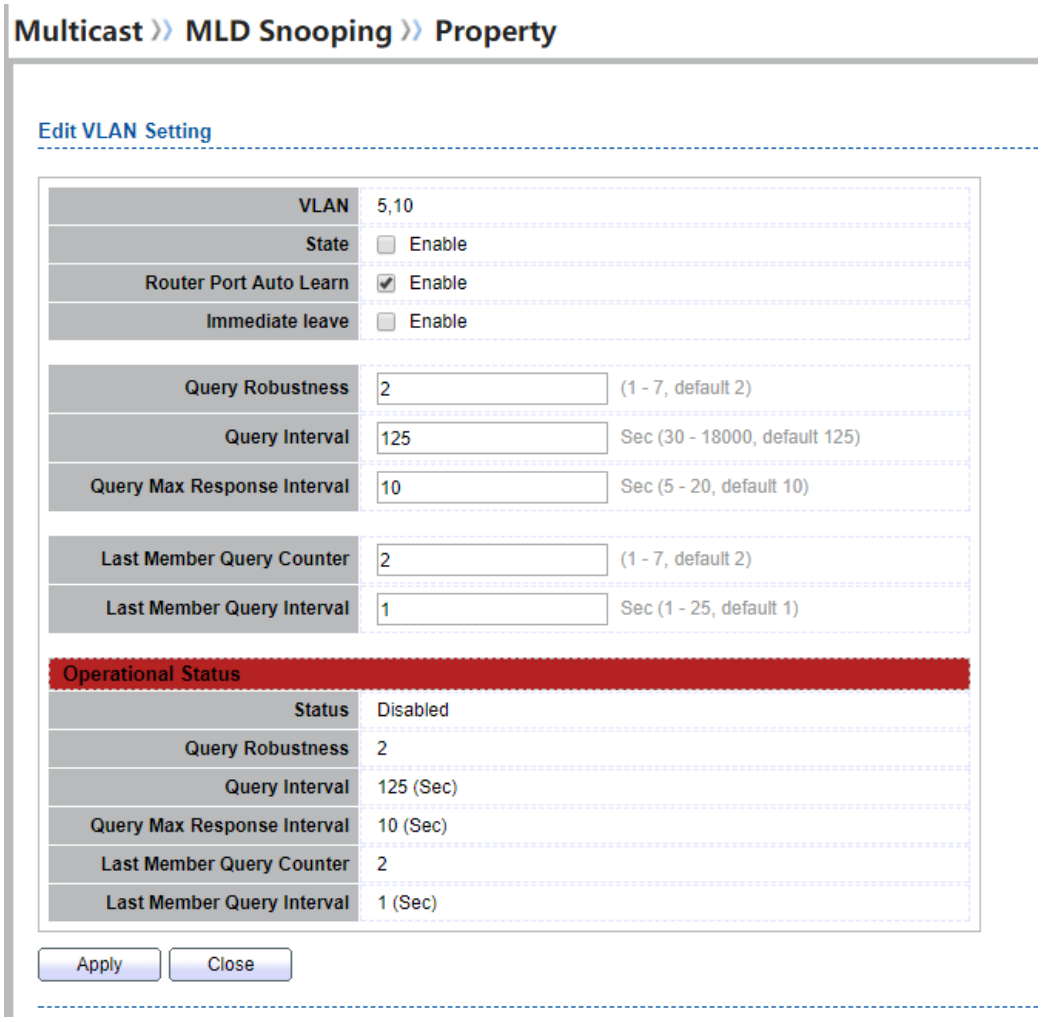
This page allows the user to configure the global MLD Snooping parameters and to set specific MLD Snooping options for individual VLANs.



Field	Description
State	Enable/disable the MLD Snooping functionality
Version	Set the MLD snooping version • MLDv1: Only supports MLD v1 packets. • MLDv2: Supports v2 basic and v1.
Report Suppression	Enable/disable the MLD Snooping report suppression functionality
VLAN	The MLD entry VLAN ID
Operation Status	Shows the status of the MLD snooping VLAN functionality
Router Port Auto Learn	Shows the status of the MLD snooping router port auto learning
Query Robustness	The Query Robustness allows tuning for the expected packet loss on a subnet.
Query Interval	The interval of querier to send general query
Query Max Response Interval	specifies the maximum allowed time before sending a responding report. Selectable in units of 1/10 second.

Last Member Query count	Shows the number of group-specific queries that a querier sends after receiving a leave message.
Last Member Query Interval	The interval at which the Group-Specific Queries are sent is called last member query interval.
Immediate leave	When enabled, the switch immediately removes the port from the group upon receiving an MLD Leave message.

To edit a VLAN click the “edit” button.



Field	Description
VLAN	VLANs selected for configuration.
State	Enables or disables MLD Snooping on the selected VLAN.
Router Port Auto Learn	Enables automatic learning of router ports.
Immediate Leave	Enables immediate leave behaviour for the VLAN.
Query Robustness	Admin robustness value (1–7, default 2).
Query Interval	Admin query interval (30–18000 seconds, default 125).
Query Max Response Interval	Admin maximum response interval (5–20 seconds, default 10).

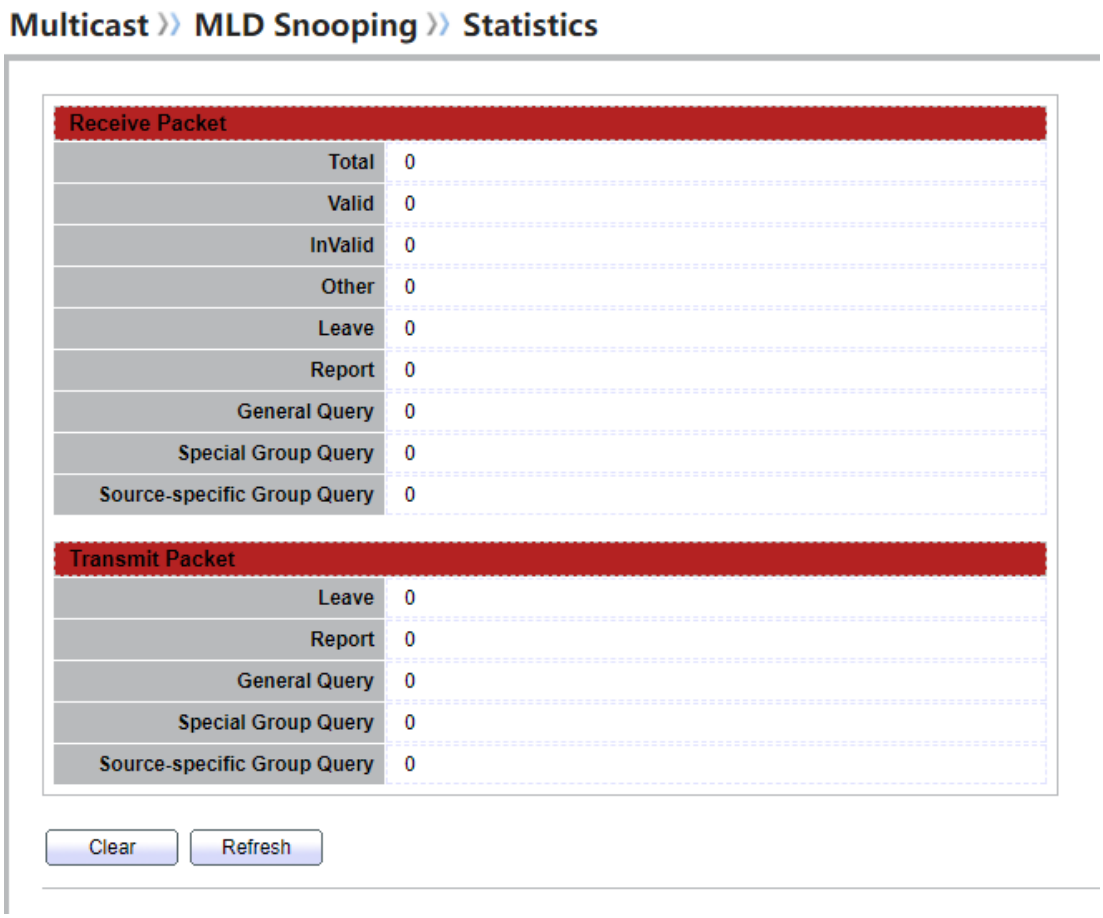
Last Member Query Counter	Admin last member query count (1–7, default 2).
Last Member Query Interval	Admin last member query interval (1–25 seconds, default 1).
Operational Status	
Status	Indicates whether MLD Snooping is operational.
Query Robustness	Operational robustness value.
Query Interval	Operational query interval.
Query Max Response Interval	Operational maximum response interval.
Last Member Query Counter	Operational last member query count.

STATISTICS

Use this page to view MLD Snooping packet counters and operational statistics.

To view the MLD Snooping Global Settings and VLAN Settings page, go to Multicast > MLD Snooping > Statistics.

This page also allows you to clear counters.



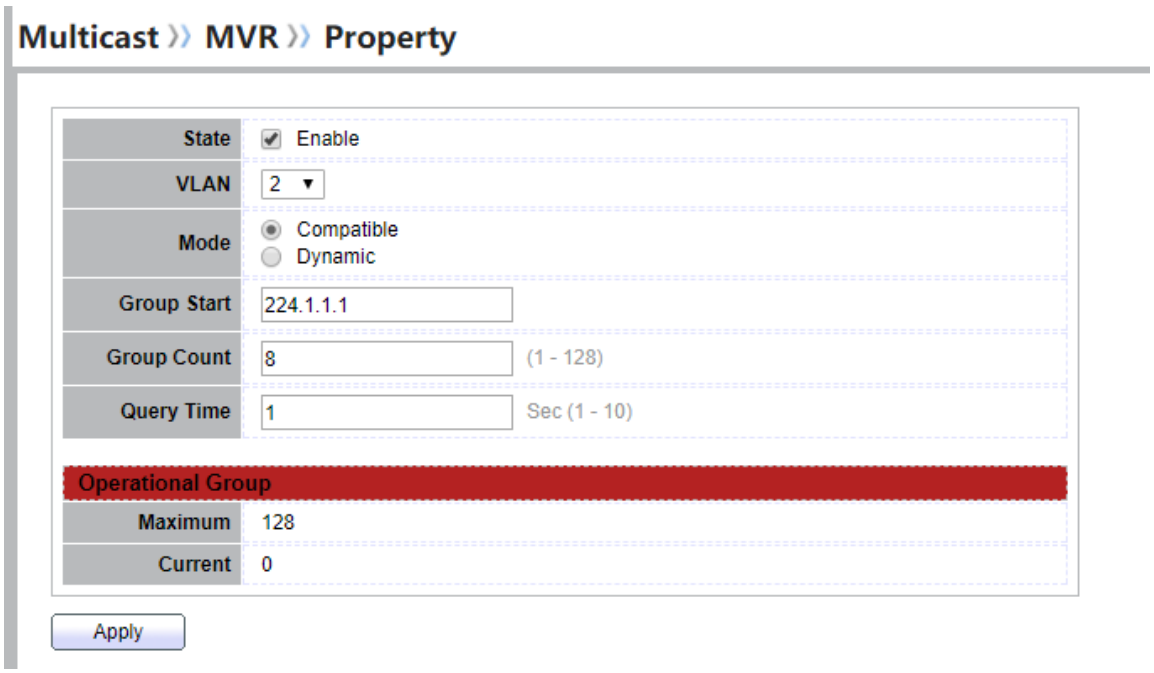
Field	Description
Total	Total received MLD packets, including IPv6 multicast packets sent to CPU.
Valid	Valid MLD Snooping packets processed.
Invalid	Invalid packets that failed MLD Snooping processing.
Other	Packets that are not MLD, not IPv6 multicast, and not IPv6 router protocol.
Leave	MLD Leave messages.
Report	MLD Join and Report messages.
General Query	General MLD Query packets.
Special Group Query	Group-specific MLD Query packets.
Source-specific Group Query	Source-specific MLD Query packets.
Transmit Packet	
Leave	Transmitted MLD Leave messages.
Report	Transmitted MLD Join and Report messages.
General Query	Transmitted general MLD Query packets.
Special Group Query	Transmitted group-specific MLD Query packets.
Source-specific Group Query	Transmitted source-specific MLD Query packets.

MVR

Use this page to configure the global MVR parameters, including VLAN assignment, operating mode, multicast group range, and query behaviour.

PROPERTY

To view the MVR Global Settings go to Multicast > MVR > Property.

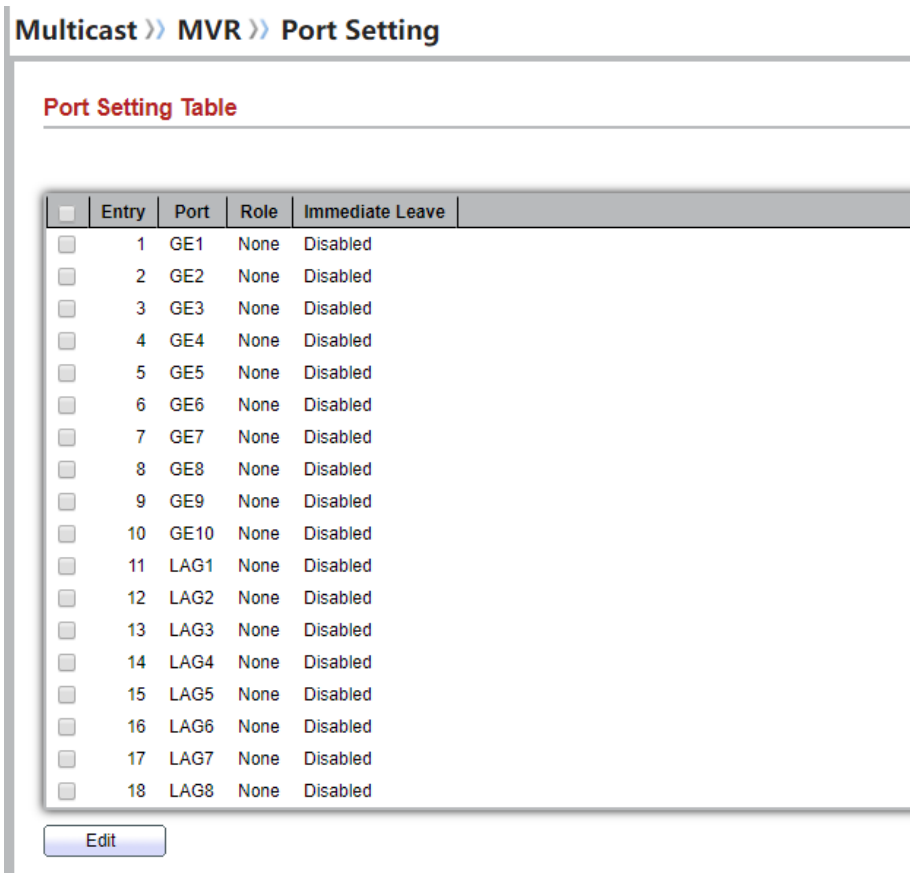


Field	Description
State	Enables or disables MVR globally. When disabled, all MVR forwarding stops.
VLAN	Specifies the VLAN used as the MVR multicast VLAN.
Mode	Selects the MVR operating mode: Compatible (receiver-only membership) or Dynamic (learns group membership on source ports).
Group Start	Defines the starting IPv4 multicast address for the MVR group range.
Group Count	Number of consecutive multicast addresses included in the MVR group range (1–128).
Query Time	Time interval used when sending MVR queries after receiving a leave message.
Maximum	Maximum number of MVR groups supported by the switch.
Current	Number of MVR groups currently learned.

PORT SETTING

Use this page to configure the role of each port within the MVR domain and to enable or disable immediate leave behaviour.

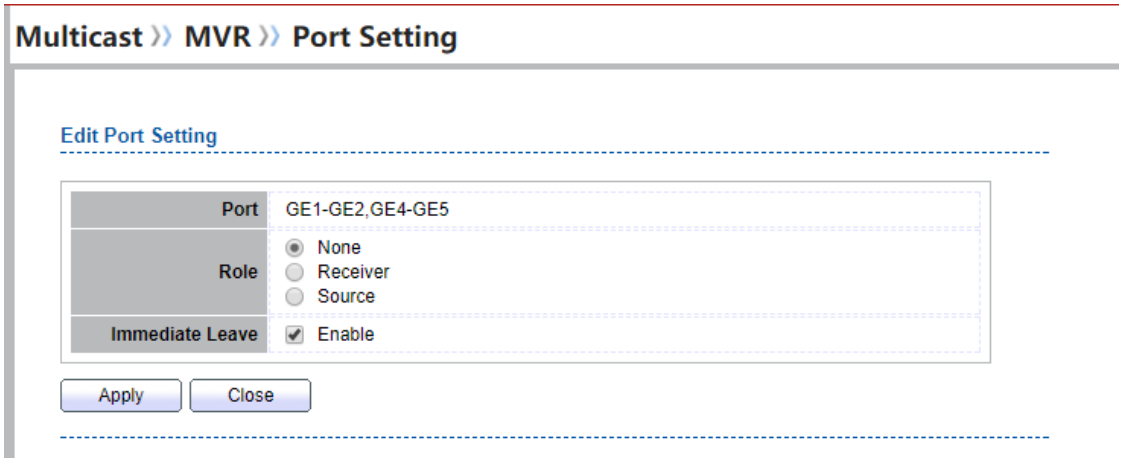
To view go to Multicast > MVR > Port Setting.



Field	Description
Entry	Entry index number.
Port	Port name (GE1–GE10, LAG1–LAG8 depending on model).
Role	Defines the port's MVR role: None, Receiver, or Source.
Immediate Leave	Enables immediate leave behaviour for the port. When enabled, the port is removed from the group immediately upon receiving a leave message.

Editing Port Settings

Selecting one or more ports and clicking **Edit** allows configuration of port roles and immediate leave.

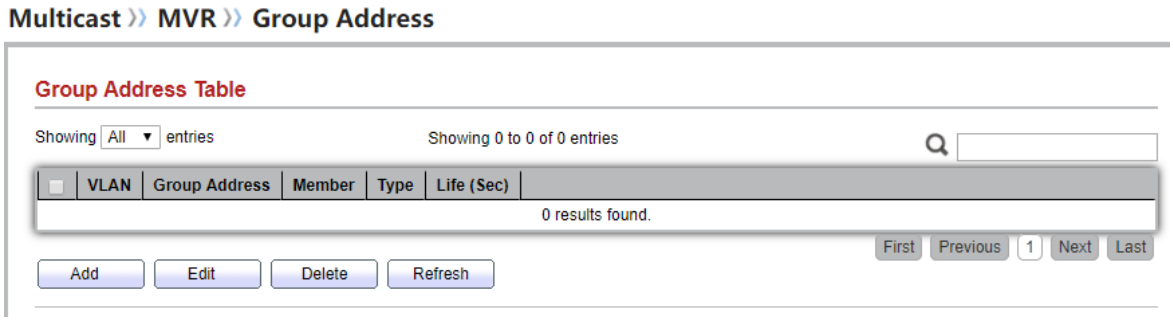


Field	Description
Port	Displays the selected port list.
Role	Sets the port role: None, Receiver, or Source.
Immediate Leave	Enables or disables immediate leave behaviour for the selected ports.

GROUP ADDRESS

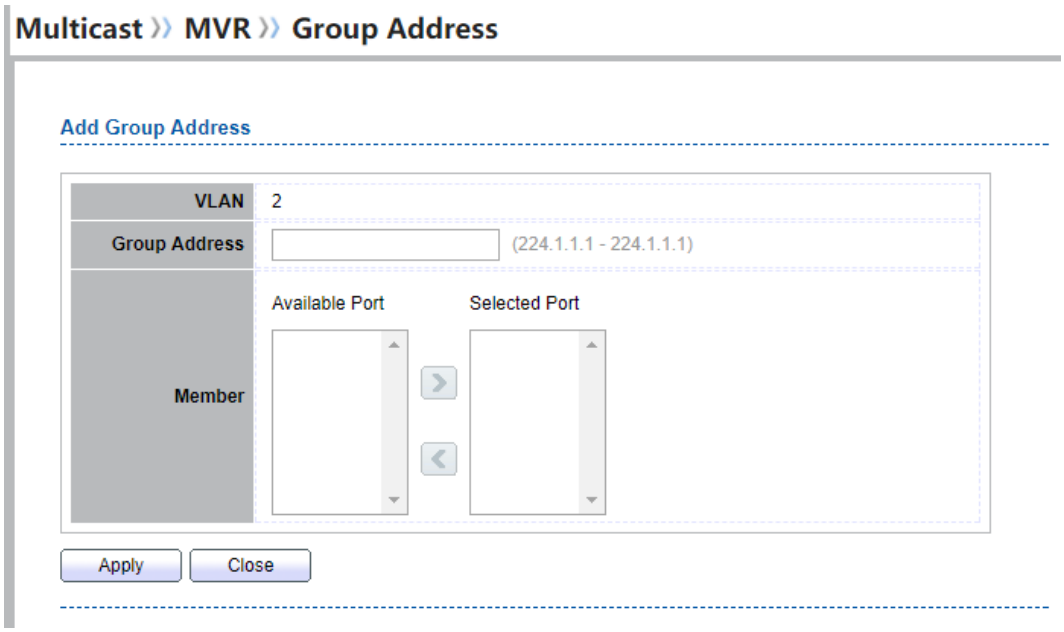
Use this page to view, add, or edit multicast group entries associated with MVR.

To view go to Multicast > MVR > Group Address



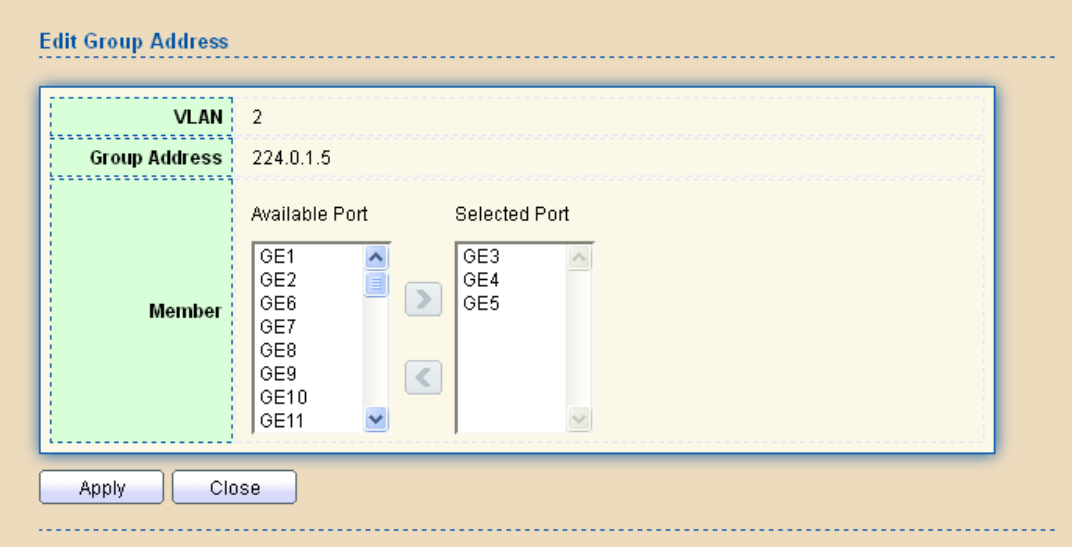
Field	Description
VLAN	VLAN ID associated with the MVR group.
Group Address	IPv4 multicast address of the group.
Member	Ports participating in the group.
Type	Indicates whether the group is **Static** or **Dynamic**.
Life (Sec)	Remaining lifetime for dynamic groups.

When adding a new group:



Field	Description
VLAN	VLAN ID for the new MVR group.
Group Address	Multicast address within the configured MVR range.
Available Port	Ports eligible to join the group. In Compatible mode, only receiver ports are shown; in Dynamic mode, source ports are also included.
Selected Port	Ports selected as members of the group.

Editing allows modification of the group address and member ports.



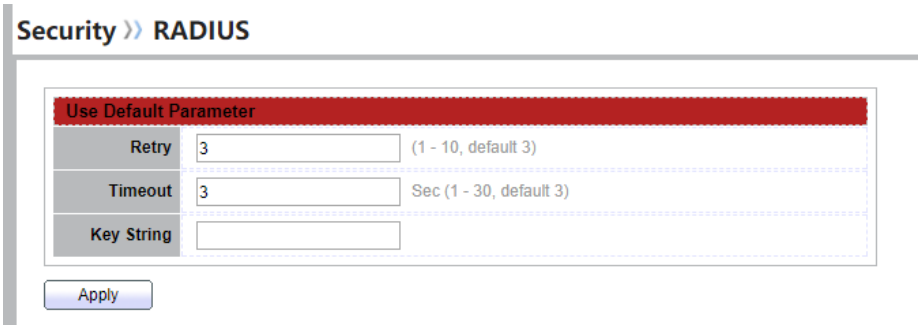
Field	Description
VLAN	VLAN ID of the group being edited.
Group Address	Updated multicast address.
Member	Updated list of ports participating in the group.

SECURITY

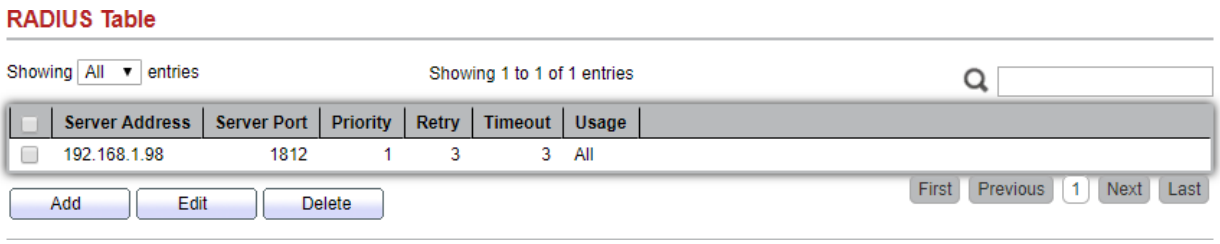
The Security pages allow you to configure authentication, access control, protection features, and packet-level security mechanisms for the switch. These functions ensure that only authorised users and devices can access the network and that malicious or abnormal traffic is detected and mitigated.

RADIUS

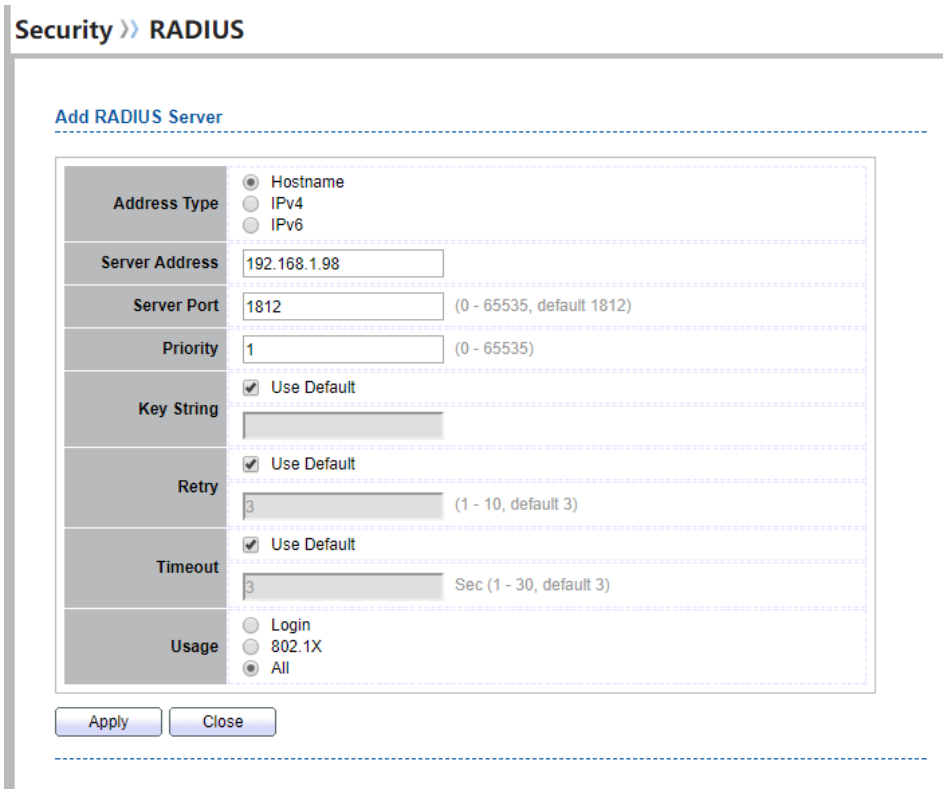
Use this page to configure RADIUS authentication servers and default RADIUS parameters.
Navigation: Security → RADIUS

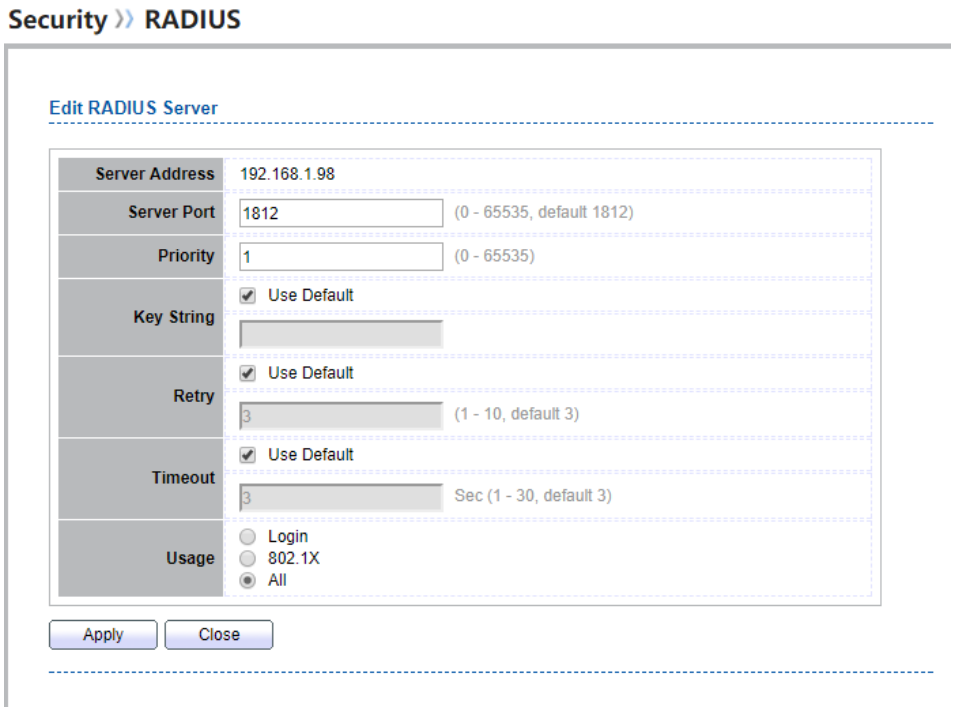


Field	Description
Retry	Sets the number of retry attempts when contacting the RADIUS server.
Timeout	Sets the timeout period (in seconds) for RADIUS server responses.
Key String	Defines the shared secret used for RADIUS authentication.



Field	Description
Server Address	IPv4 address of the RADIUS server.
Server Port	UDP port used for RADIUS authentication (default 1812).
Priority	Determines server selection order. Lower values have higher priority.
Retry	Retry count for this specific server.
Timeout	Timeout value for this server.
Usage	Specifies the authentication type: **Login**, **802.1X**, or **All**.





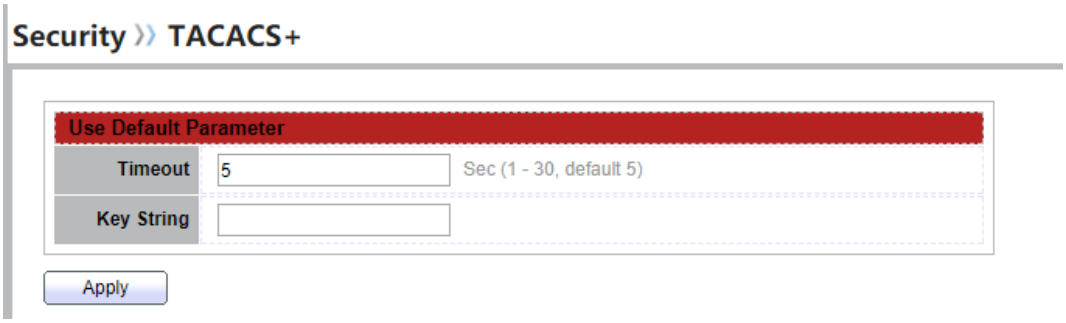
Field	Description
Address Type	Selects the type of address used for the RADIUS server. • Hostname – Uses a DNS hostname. • IPv4 – Uses an IPv4 address. • IPv6 – Uses an IPv6 address.
Server Address	Specifies the server address based on the selected address type. In edit mode, this field displays the current configured address.
Server Port	Sets the UDP port used for RADIUS authentication (default 1812).

Priority	Determines the order in which servers are contacted. Lower values have higher priority. The switch attempts the highest-priority server first; if it fails, it automatically tries the next server.
Retry	Number of retry attempts before the switch considers the server unreachable.
Timeout	Maximum time (in seconds) the switch waits for a response before retrying or failing over to the next server.
Usage	Defines the authentication role of the server: • Login – Used for management login authentication. • 802.1X – Used for port-based authentication. • All – Used for both login and 802.1X authentication.

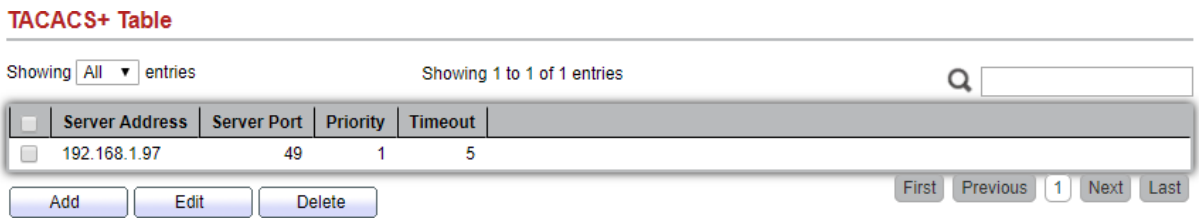
TACACS+

Use this page to configure TACACS+ authentication servers for centralised user management.

Navigation: Security → TACACS+



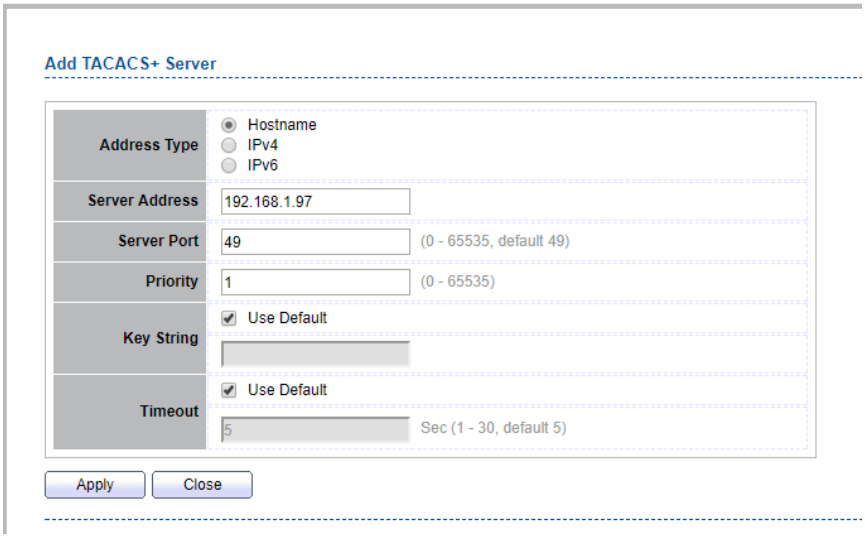
Field	Description
Timeout	Timeout period for TACACS+ server responses.
Key String	Shared secret used for TACACS+ authentication.



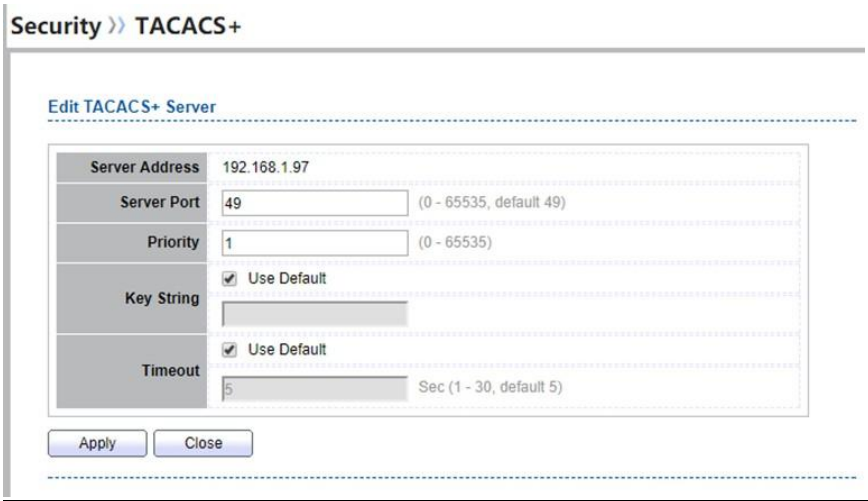
Field	Description
Server Address	IPv4 address of the TACACS+ server.
Server Port	TCP port used for TACACS+ (default 49).
Priority	Sets the TACACS+ server priority. Lower values have higher priority. The switch always attempts to authenticate with the

	highest-priority server first; if that server does not respond, it automatically fails over to the next server with a higher priority value.
Timeout	Timeout period for TACACS+ server responses.

Security ›› TACACS+



Security ›› TACACS+



Field	Description
Address Type	Selects the type of address used for the RADIUS server. • Hostname – Uses a DNS hostname. • IPv4 – Uses an IPv4 address. • IPv6 – Uses an IPv6 address.
Server Address	Specifies the server address based on the selected address type. In edit mode, this field displays the current configured address.
Server Port	Sets the UDP port used for RADIUS authentication (default 1812).
Priority	Determines the order in which servers are contacted. Lower values have higher priority. The switch attempts the highest-priority server first; if it fails, it automatically tries the next server.
Timeout	Number of retry attempts before the switch considers the server unreachable.

Timeout	Maximum time (in seconds) the switch waits for a response before retrying or failing over to the next server.
Usage	Defines the authentication role of the server: • Login – Used for management login authentication. • 802.1X – Used for port-based authentication. • All – Used for both login and 802.1X authentication.

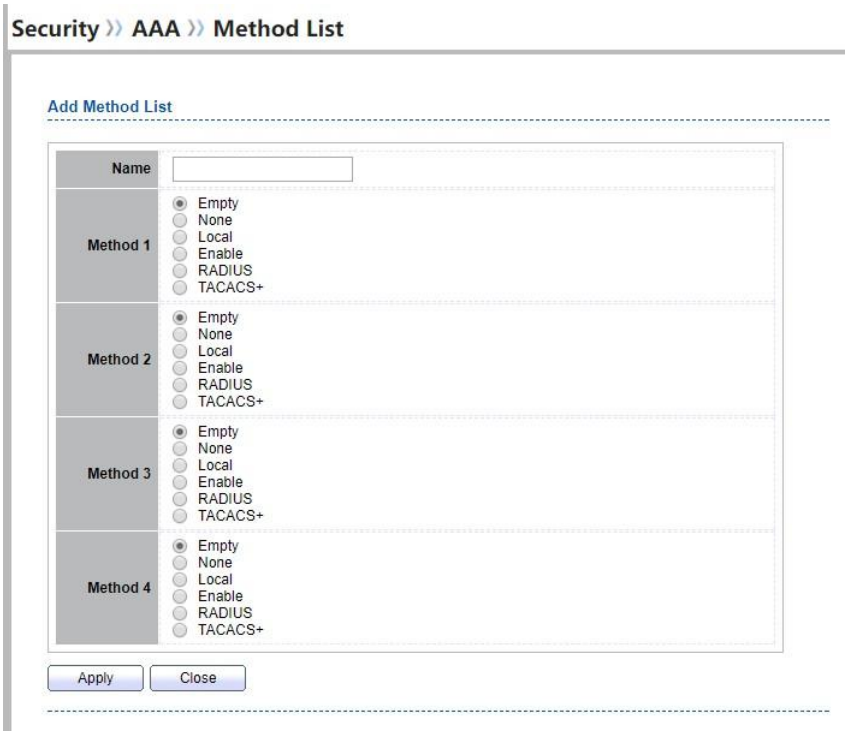
AAA (Authentication, Authorization, Accounting)

Use this page to configure AAA method lists and authentication behaviour for login and management access.

Navigation: Security → AAA

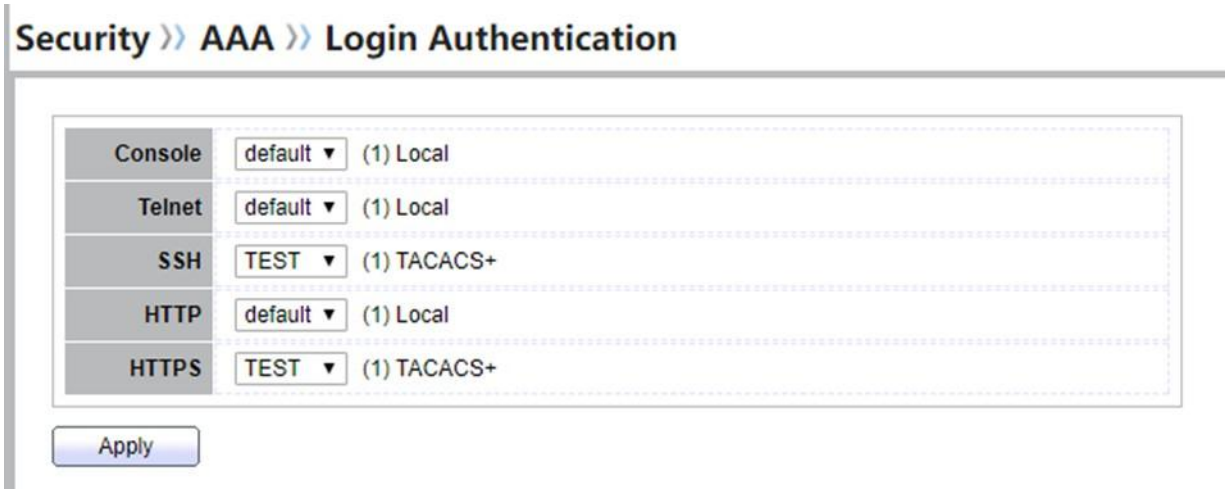
METHOD LIST

Field	Description
Name	Name of the AAA method list.
Sequence	Authentication method sequence (e.g., RADIUS → Local).



Field	Description
Name	Name of the login authentication list. Must be unique and not used by any other list.
Method 1	First-priority authentication method: • • **None** – No authentication required. • **Local** – Uses the local user database. • **TACACS+** – Authenticates via TACACS+ server . • **RADIUS** – Authenticates via RADIUS server. • **Enable** – Uses the local enable password.
Method 2	Second-priority authentication method. Options identical to Method 1.
Method 3	Third-priority authentication method. Options identical to Method 1.

LOGIN AUTHENTICATION



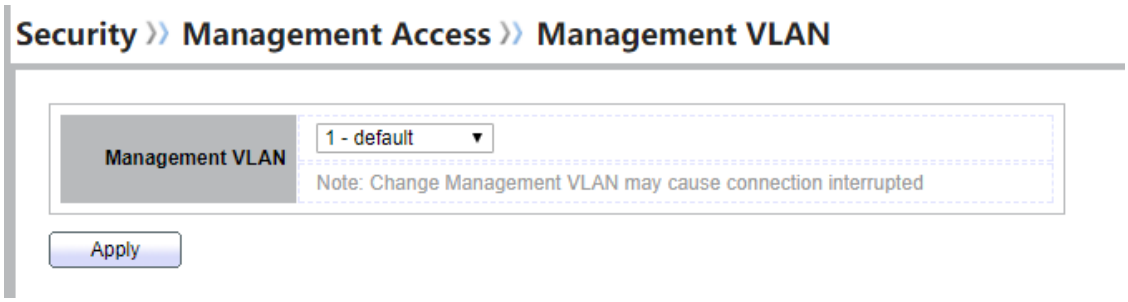
Field	Description
Console	Specifies the login authentication list applied to console (local serial) access.
Telnet	Specifies the login authentication list applied to Telnet sessions.
SSH	Specifies the login authentication list applied to SSH sessions.
HTTP	Specifies the login authentication list applied to HTTP (web) access.
HTTPS	Specifies the login authentication list applied to HTTPS (secure web) access.

Management Access

Use this page to configure management VLANs, management services, and ACLs that restrict access to the switch's control plane.

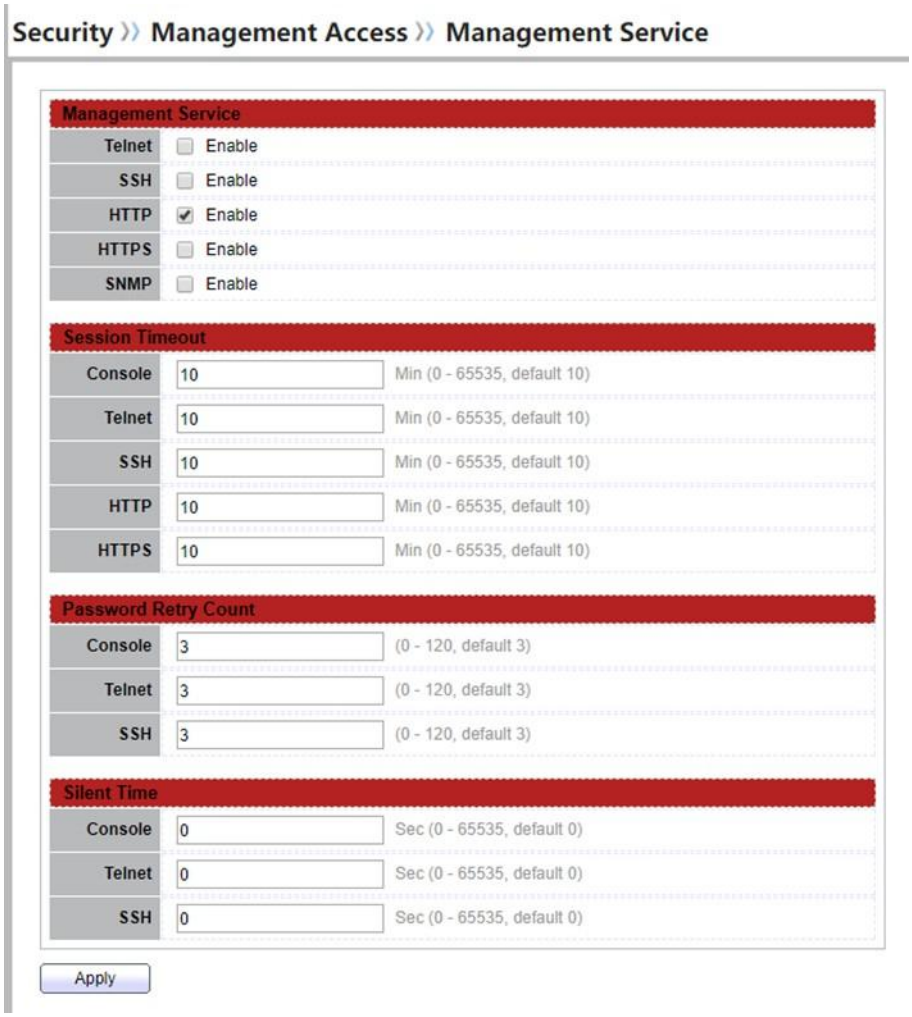
Navigation: Security → Management Access

MANAGEMENT VLAN



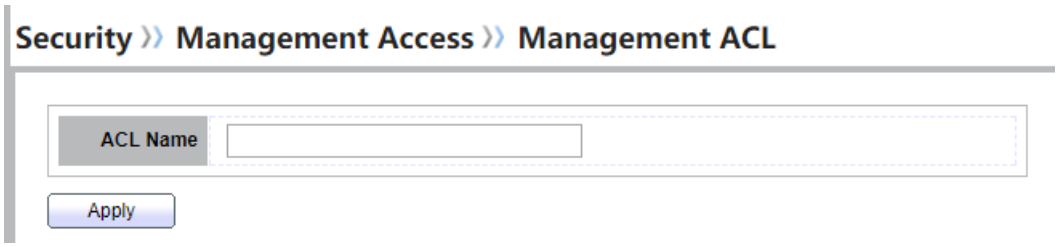
Field	Description
VLAN	VLAN ID used exclusively for management traffic.

MANAGEMENT SERVICES

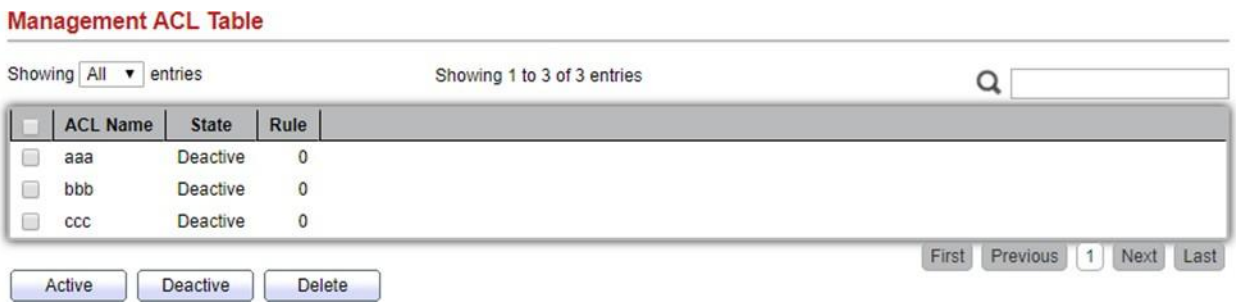


Field	Description
Telnet/SSH	Enables or disables CLI access.
HTTP/HTTPS	Enables or disables web management access.
SNMP	Enables or disables SNMP management.
Session Timeout	Sets the inactivity timeout (in minutes) for user sessions accessing the management interface. A value of **0** disables timeout and allows sessions to remain open indefinitely.
Password Retry Count	Defines how many incorrect password attempts are allowed before the CLI locks the session. Once the number of failed attempts exceeds this value, the CLI enters a silent (lockout) period.
Silent Time	Duration (in seconds or minutes, depending on model) that the CLI remains locked after exceeding the password retry count. During this silent time, login attempts are ignored.

MANAGEMENT ACL



Field	Description
ACL Name	Input MAC ACL Name

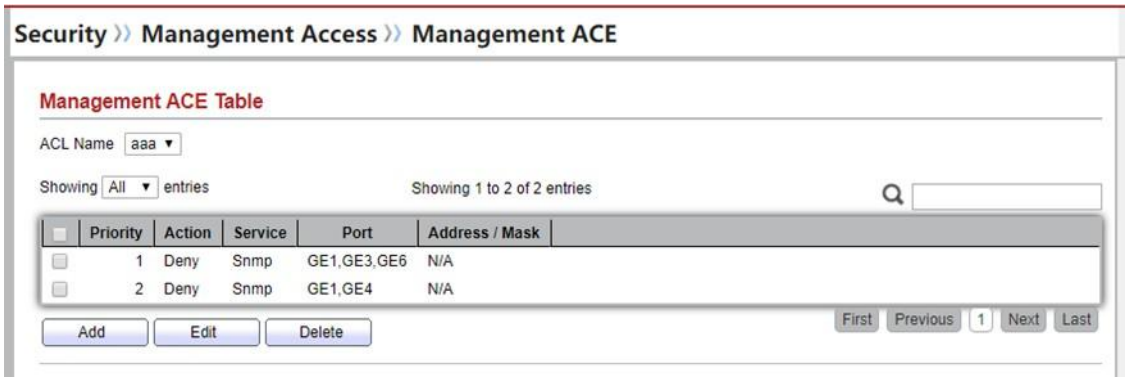


Field	Description
ACL Name	Displays the name of the Management ACL applied to management services.
State	Indicates whether the Management ACL is active or inactive.
Rule	Shows the number of Management ACE (Access Control Entry) rules contained within the ACL.

Management Access – Management ACE

This page allows you to add, edit, and delete ACE rules within a Management ACL. An ACE cannot be edited or deleted while its ACL is active, and new ACEs cannot be added to an active ACL.

Navigation: Security → Management Access → Management ACE



Field	Description
ACL Name	Selects the Management ACL to which the ACE belongs.

Priority	Displays the ACE priority (sequence). Lower numbers are processed first.
Action	Displays the ACE action (Permit or Deny).
Service	Displays the service to which the ACE applies (HTTP, HTTPS, SSH, Telnet, SNMP, or All).
Port	Displays the port list associated with the ACE.
Address / Mask	Displays the source IP address and mask matched by the ACE.

Add / Edit Management ACE

This dialog is used to create or modify individual ACE rules within a Management ACL.

Field	Description
ACL Name	Shows the ACL to which the ACE is being added or edited.
Priority	Specifies the ACE priority. ACEs with lower sequence numbers are processed first (1 is highest). Available when adding a new ACE.
Service	Selects the service the rule applies to: • All – All management services. • HTTP – WebUI over HTTP. • HTTPS – WebUI over HTTPS. • SNMP – SNMP management. • SSH – SSH CLI access. • Telnet – Telnet CLI access.
Action	Defines what happens when traffic matches the ACE: • • Permit – Allows matching packets. • Deny – Drops matching packets.
Port	Selects the ports to which the ACE applies.
IP Version	Selects the type of source IP address: • • All – Any IP address.

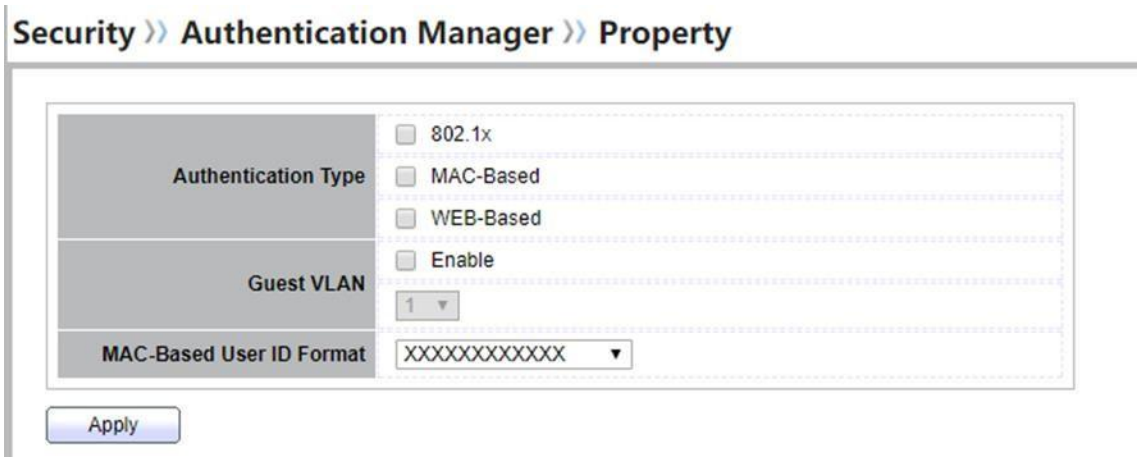
	• IPv4 – IPv4 addresses only. • IPv6 – IPv6 addresses only.
IPv4	When IPv4 is selected, specifies the source IPv4 address and mask to match.
IPv6	When IPv6 is selected, specifies the source IPv6 address and mask to match.

AUTHENTICATION MANAGER

Use this page to configure port-based authentication, MAC-based accounts, and web-based local accounts.

Navigation: Security → Authentication Manager

PROPERTY



Field	Description
Authentication Type	Enables or disables supported authentication mechanisms: • **802.1X** – Uses IEEE 802.1X port-based authentication. • **MAC-Based** – Authenticates devices using their MAC address. • **Web-Based** – Redirects users to a captive portal login page for authentication.
Guest VLAN	Enables or disables Guest VLAN. When enabled, select a VLAN ID to assign unauthenticated or failed-authentication clients.
MAC-Based User ID Format	Selects the username/password format used when performing MAC-based RADIUS authentication.

Port Mode Table

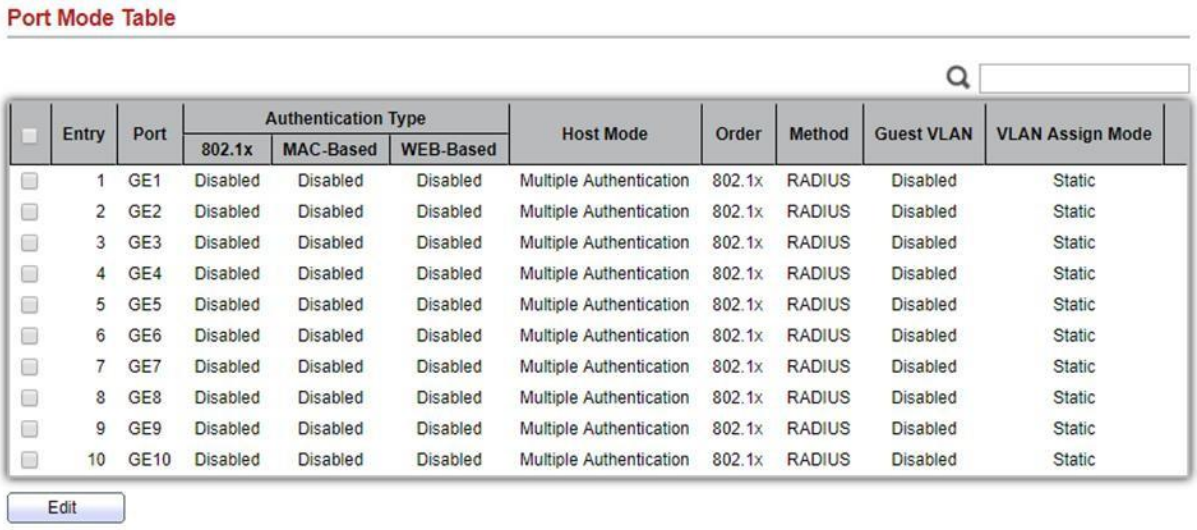
Entry	Port	Authentication Type			Host Mode	Order	Method	Guest VLAN	VLAN Assign Mode
		802.1x	MAC-Based	WEB-Based					
1	GE1	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
2	GE2	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
3	GE3	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
4	GE4	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
5	GE5	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
6	GE6	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
7	GE7	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
8	GE8	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
9	GE9	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
10	GE10	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static

Edit

Field	Description
Port	Displays the port name.
Authentication Type (802.1X)	• Enables or disables 802.1X authentication on the port: **Enabled** – 802.1X authentication is active. • **Disabled** – 802.1X authentication is not used.
Authentication Type (MAC-Based)	Enables or disables MAC-Based authentication: • **Enabled** – MAC-Based authentication is active. • **Disabled** – MAC-Based authentication is not used.
Authentication Type (Web-Based)	Enables or disables Web-Based authentication: • **Enabled** – Web-Based authentication is active. • **Disabled** – Web-Based authentication is not used.
Host Mode	Defines how multiple hosts are authenticated on the port: • • **Multiple Authentication** – Each client must authenticate individually. • **Multiple Hosts** – Only one client must authenticate; all others inherit access. Web-auth cannot be enabled in this mode. • **Single Host** – Only one authenticated host is allowed (equivalent to Multi-Auth with max hosts = 1).
Order	Defines the authentication type order. The switch moves to the next type if the current type is disabled or fails. Web-Auth must always be last.
Method	Defines the authentication method order (applies only to MAC-Based and Web-Based; 802.1X always uses RADIUS). Supported methods: • **Local** – Uses local user database. • **Radius** – Uses RADIUS server. • **Local → Radius** • **Radius → Local**

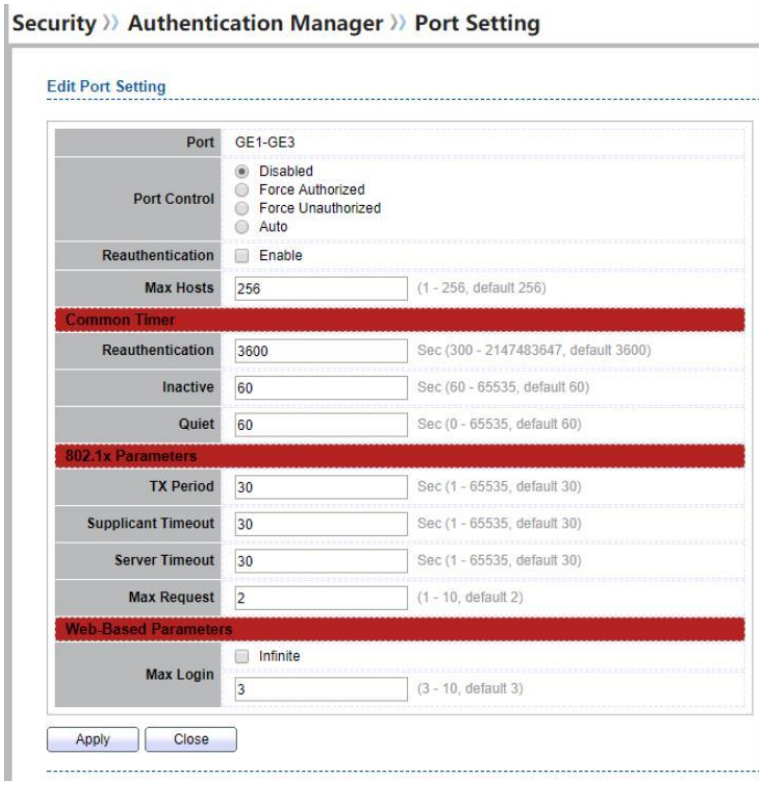
Guest VLAN	Enables or disables Guest VLAN on the port: • **Enabled** – Guest VLAN is active. • **Disabled** – Guest VLAN is not used.
VLAN Assign Mode	Defines how VLAN assignment behaves when RADIUS provides VLAN attributes: • • **Disable** – Ignore RADIUS VLAN assignment; keep original VLAN. • **Reject** – Use RADIUS VLAN if provided; if not provided, reject the host. • **Static** – Use RADIUS VLAN if provided; if not provided, keep original VLAN.

PORT SETTING



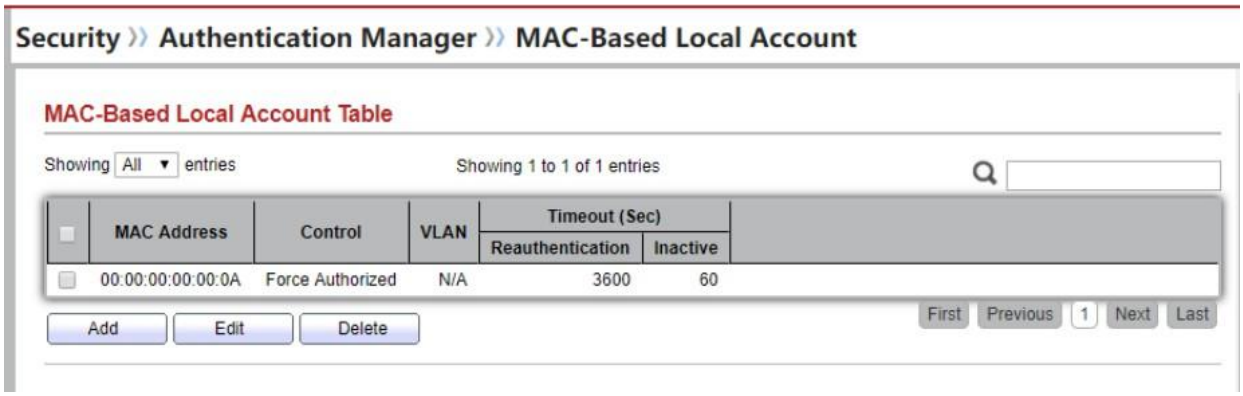
Field	Description
Port	Displays the port name.
Port Control	Defines how authentication controls port access: • **Disable** – Authentication disabled; all clients have network access. • **Force Authorized** – Port is always authorized; all clients have access. • **Force Unauthorized** – Port is always unauthorized; no clients have access. • **Auto** – Clients must pass authentication to gain network access.
Reauthentication	Controls whether authenticated hosts must periodically reauthenticate: • **Enabled** – Hosts reauthenticate after the configured reauthentication period.

	• **Disabled** – Hosts remain authenticated indefinitely unless disconnected.
Max Hosts	In Multiple Authentication mode, defines the maximum number of authenticated hosts allowed on the port.
Common Timer (Reauthentication)	After the reauthentication period expires, the host returns to the initial state and must authenticate again.
Common Timer (Inactive)	Tracks inactivity for authenticated hosts. If no packets are received before the inactivity timeout expires, the host becomes unauthorized and its session is deleted. In Multi-Host mode, only packets from the authorized host are counted.
Common Timer (Quiet)	When a port enters Locked state due to repeated authentication failures, the host remains locked for the quiet period. After this period, the host may attempt authentication again.
802.1X Params (TX Period)	Number of seconds the switch waits for a response to an EAP Request/Identity frame before resending the request.
802.1X Params (Supplicant Timeout)	Maximum number of EAP requests sent before restarting the authentication process if no response is received.
802.1X Params (Server Timeout)	Number of seconds before EAP requests are resent to the supplicant.
802.1X Params (Max Request)	Maximum number of times the switch resends a request to the authentication server.
Web-Based Param (Max Login)	Maximum number of failed Web-Auth login attempts allowed. After exceeding this limit, the host enters Locked state and cannot authenticate until the quiet period expires.

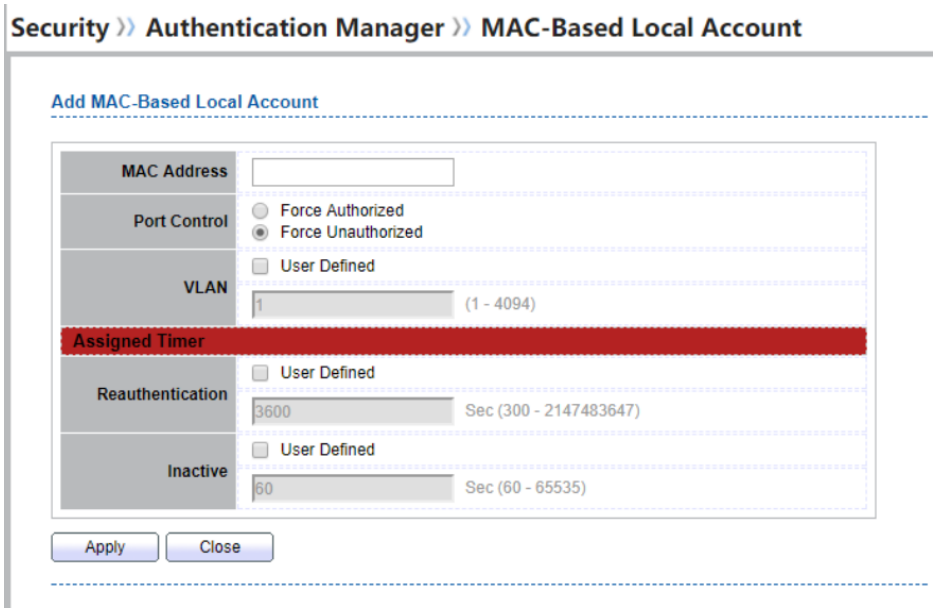


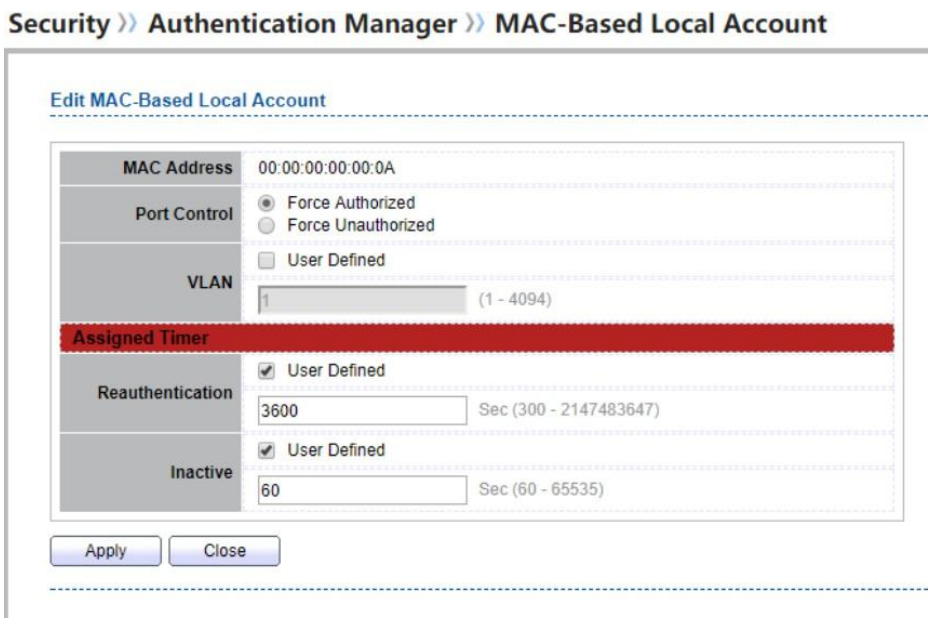
Field	Description
Port	Displays the port name.
Port Control	Defines how authentication controls port access: • **Disable** – Authentication disabled; all clients have network access. • **Force Authorized** – Port is always authorized; all clients have access. • **Force Unauthorized** – Port is always unauthorized; no clients have access. • **Auto** – Clients must pass authentication to gain network access.
Reauthentication	Enables or disables periodic reauthentication. When enabled, hosts must reauthenticate after the configured reauthentication period.
Max Hosts	In Multiple Authentication mode, defines the maximum number of authenticated hosts allowed on the port.
Common Timer (Reauthentication)	After the reauthentication period expires, the host returns to the initial state and must authenticate again.
Common Timer (Inactive)	Tracks inactivity for authenticated hosts. If no packets are received before the inactivity timeout expires, the host becomes unauthorized and its session is deleted. In Multi-Host mode, only packets from the authorized host are counted.
Common Timer (Quiet)	When a port enters Locked state due to repeated authentication failures, the host remains locked for the quiet period. After this period, the host may attempt authentication again.
802.1X Params (TX Period)	Number of seconds the switch waits for a response to an EAP Request/Identity frame before resending the request.
802.1X Params (Supplicant Timeout)	Maximum number of EAP requests sent before restarting the authentication process if no response is received.
802.1X Params (Server Timeout)	Number of seconds before EAP requests are resent to the supplicant.
802.1X Params (Max Request)	Maximum number of times the switch resends a request to the authentication server.
Web-Based Param (Max Login)	Configures the maximum number of failed Web-Auth login attempts. When the limit is exceeded, the host enters Locked state and cannot authenticate until the quiet period expires. Can be set to **infinite** or a specific number.

MAC-BASED LOCAL ACCOUNT



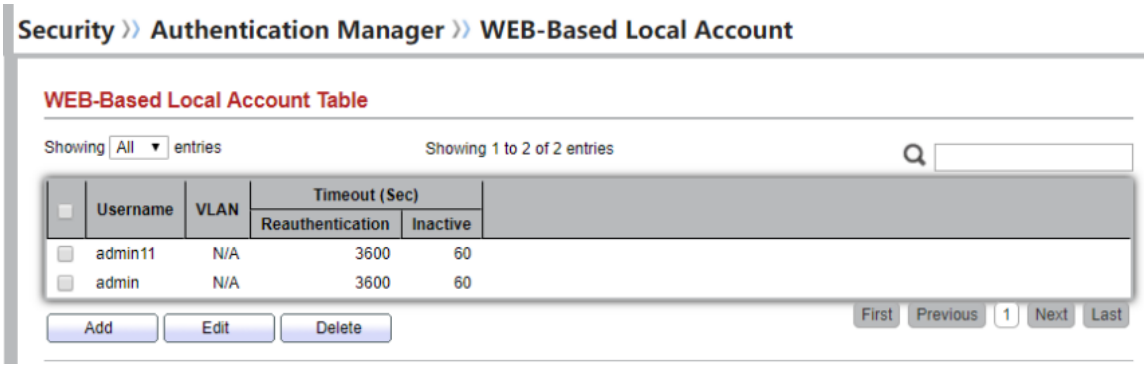
Field	Description
MAC Address	MAC address of the authenticated host. Each MAC address is allowed only one entry in the local database.
Control	Host-specific control type: • **Force Authorized** – Host is forced to remain authorized. • **Force Unauthorized** – Host is forced to remain unauthorized.
VLAN	VLAN ID assigned to the authenticated host.
Timeout (Reauthentication)	Reauthentication period assigned to the host. After this period, the host must reauthenticate.
Timeout (Inactive)	Inactivity timeout assigned to the host. If no traffic is seen before this timeout expires, the host is de-authenticated and its session removed.





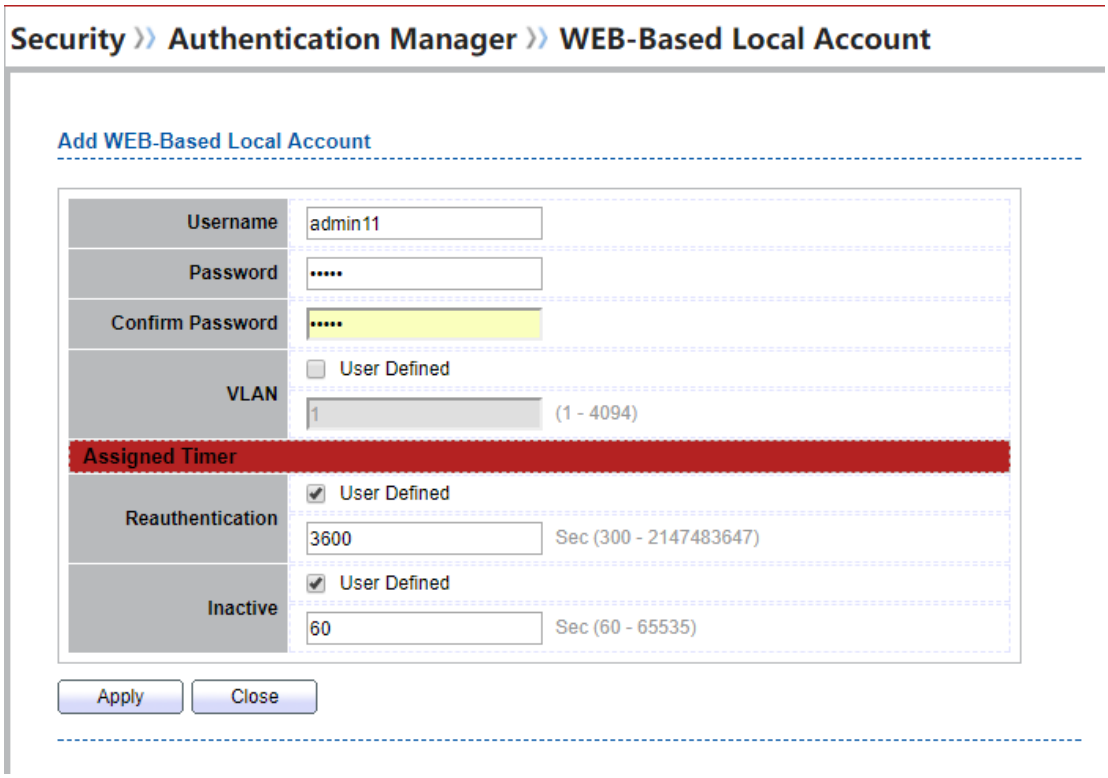
Field	Description
MAC Address	MAC address of the authenticated host. Each MAC address is allowed only one entry in the local database.
Control	Host-specific authorization control: • **Force Authorized** – Host is forced to remain authorized. • **Force Unauthorized** – Host is forced to remain unauthorized.
VLAN	VLAN ID assigned to the authenticated host.
Timeout (Reauthentication)	Reauthentication period assigned to the host. After this period expires, the host must reauthenticate.
Timeout (Inactive)	Inactivity timeout assigned to the host. If no traffic is detected before the timeout expires, the host becomes unauthorized and its session is removed.

WEB-BASED LOCAL ACCOUNT



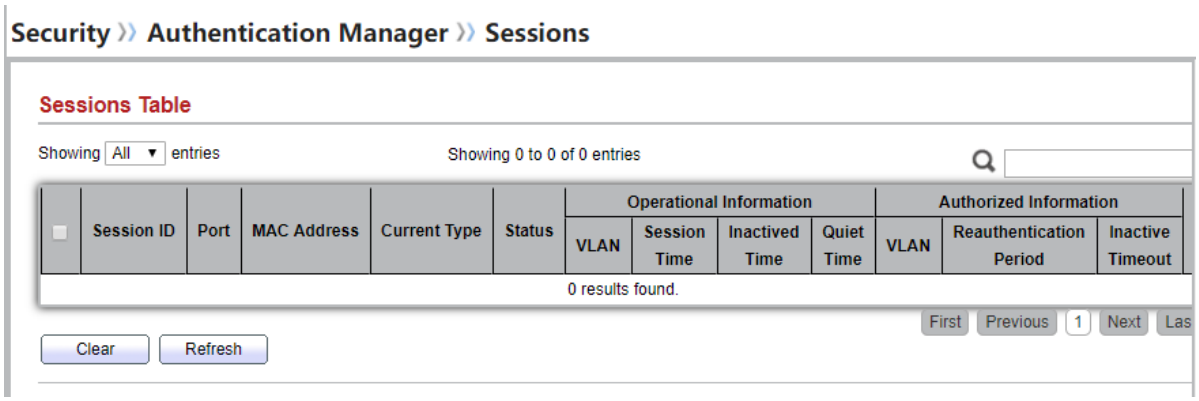
Field	Description
Username	Username of the authenticated account.

VLAN	VLAN ID assigned to the authenticated user.
Timeout (Reauthentication)	Reauthentication period assigned to the user. After this period expires, the user must reauthenticate.
Timeout (Inactive)	Inactivity timeout assigned to the user. If no activity is detected before the timeout expires, the user session is removed.



Field	Description
Username	Username of the authenticating account.
Password	Password used for authentication.
Confirm Password	Confirms the password entered above. Both fields must match.
VLAN	VLAN ID assigned to the authenticated user.
Timeout (Reauthentication)	Reauthentication period assigned to the user. After this period expires, the user must reauthenticate.
Timeout (Inactive)	Inactivity timeout assigned to the user. If no activity is detected before the timeout expires, the user session is removed.

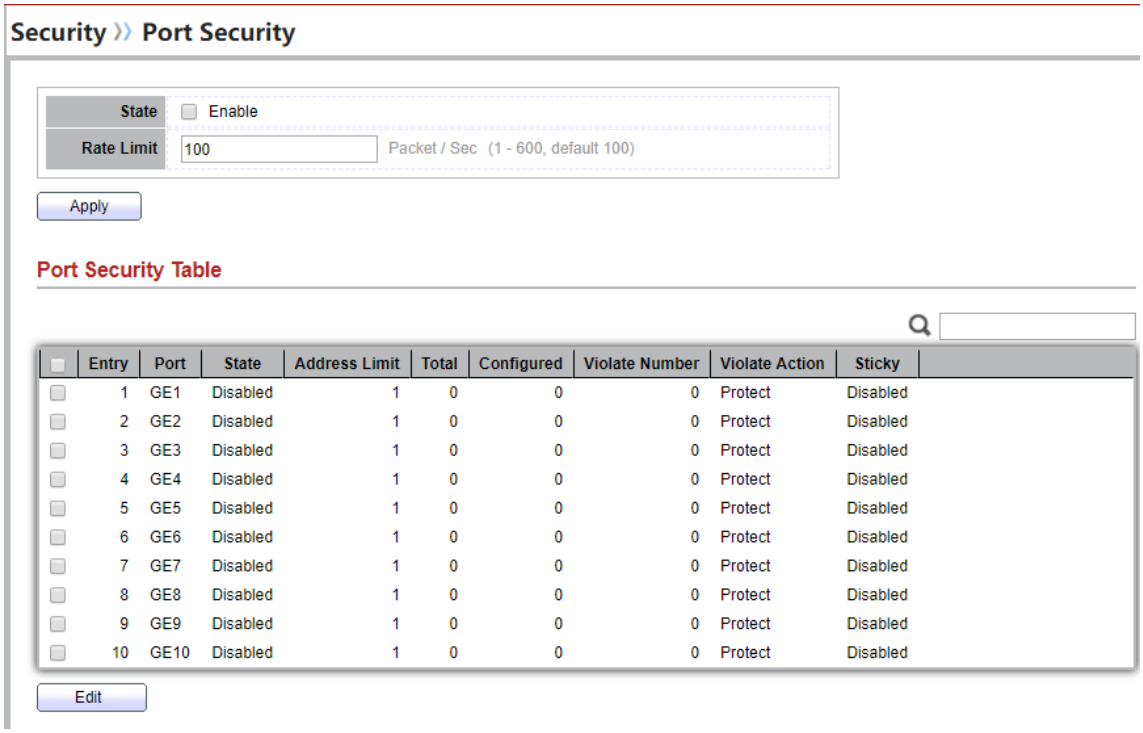
SESSIONS



Field	Description
Session ID	Unique identifier for each authentication session.
Port	Port on which the host is connected.
MAC Address	MAC address of the host participating in the authentication session.
Current Type	Shows the current authentication method being used: • **802.1X** – IEEE 802.1X authentication. • **MAC-Based** – MAC-Based authentication. • **Web-Based** – Web-Based authentication.
Status	Displays the current authentication state: • **Disable** – Session is ready to be deleted. • **Running** – Authentication process is in progress. • **Authorized** – Authentication passed; host has network access. • **UnAuthorized** – Authentication failed; host has no network access. • **Locked** – Host is locked due to repeated failures; cannot authenticate until quiet period expires. • **Guest** – Host is placed in the Guest VLAN.
Operational (VLAN)	VLAN ID currently applied to the host during operation.
Operational (Session Time)	In **Authorized** state, shows total time elapsed since authorization.
Operational (Inactived)	In **Authorized** state, shows how long the host has been inactive (no packets sent).
Operational (Quiet Time)	In **Locked** state, shows total time elapsed since the host entered quiet period.
Authorized (VLAN)	VLAN ID assigned during the authorization process.
Authorized (Reauthentication Period)	Reauthentication period provided by the authorization procedure.
Authorized (Inactive Timeouts)	Inactivity timeout provided by the authorization procedure.

PORT SECURITY

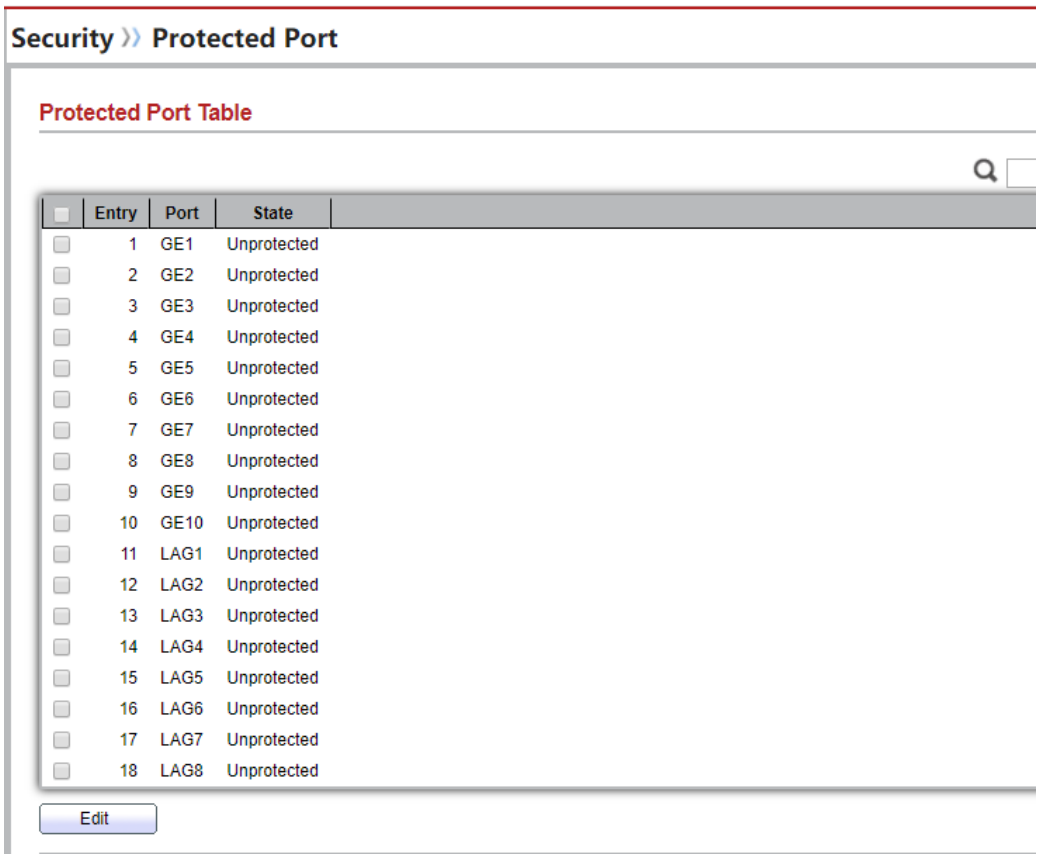
Use this page to configure per-port security features that restrict MAC address behaviour.
Navigation: Security → Port Security



Field	Description
Port	Select one or multiple ports to configure.
State	Enables or disables port security: • **Disable** – Port security is turned off. • **Enable** – Port security is active.
MAC Address	Specifies the maximum number of MAC addresses the port is allowed to learn.
Action	Defines the action taken when a new source MAC address is detected and exceeds the learning limit: • **Forward** – Forward the packet even though the MAC exceeds the limit. • **Discard** – Drop packets from MAC addresses exceeding the limit. • **Shutdown** – Shut down the port when a packet arrives with a MAC address exceeding the limit.

PROTECTED PORT

Protected ports cannot forward traffic to other protected ports, enhancing isolation.
Navigation: Security → Protected Port

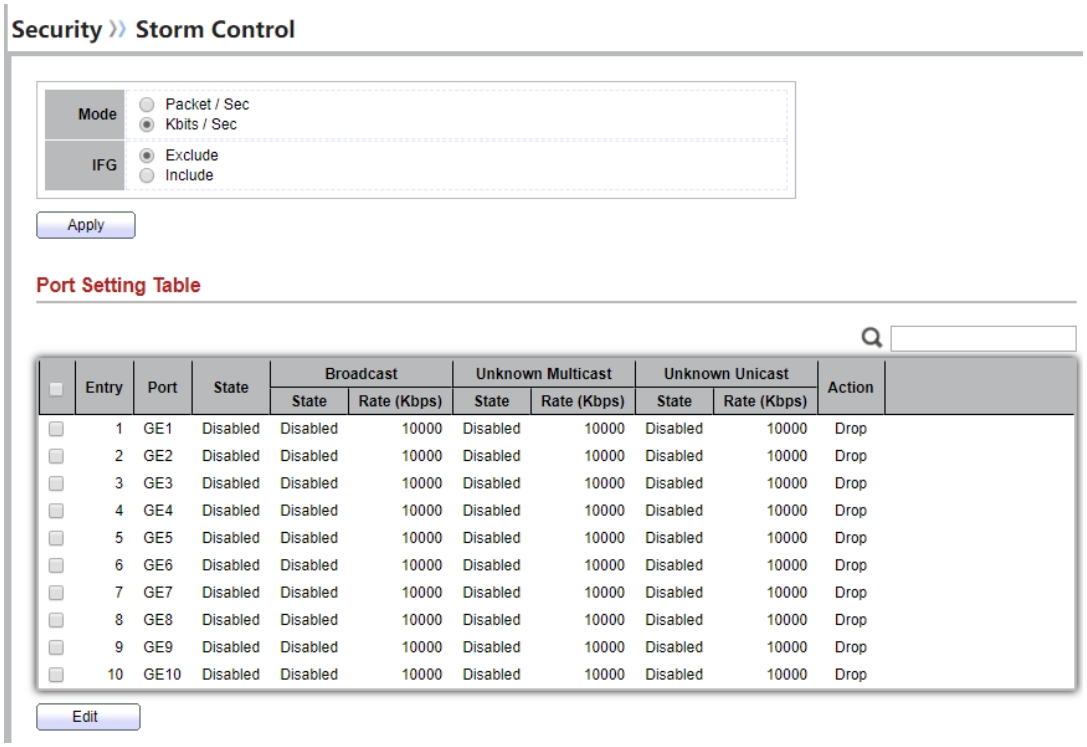


Field	Description
Port	Displays the port name.
State	Shows the protected state of the port: • **Protected** – Port is protected. • **Unprotected** – Port is not protected.

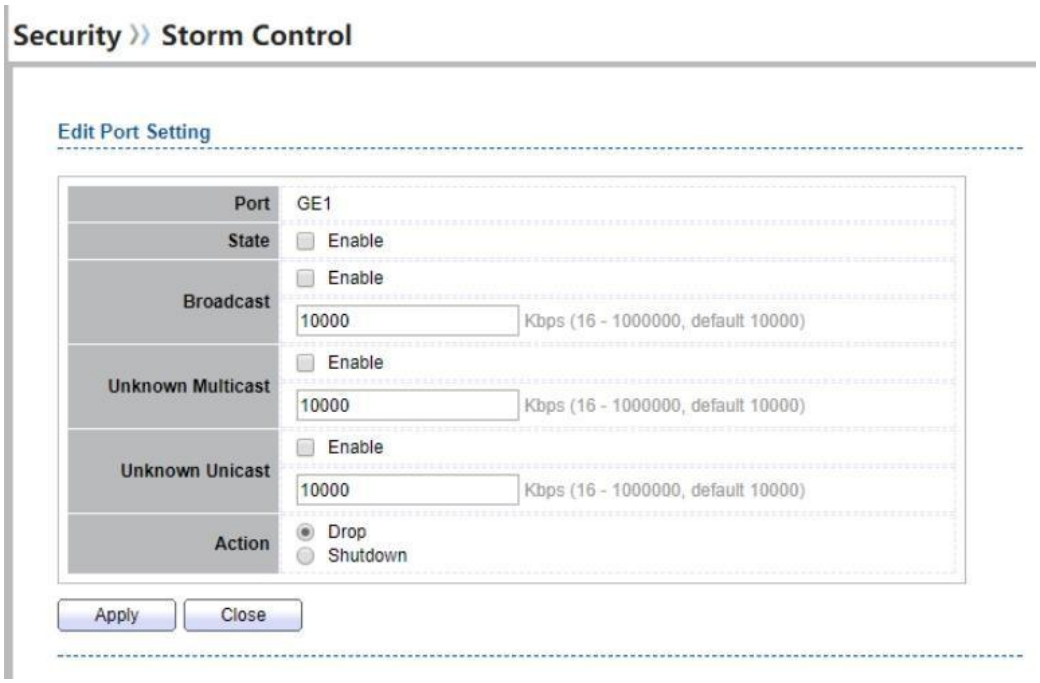
STORM CONTROL

Storm Control prevents excessive broadcast, multicast, or unknown unicast traffic.

Navigation: Security → Storm Control



Field	Description
Unit	Selects the measurement unit used for storm control rate: • **Packet / Sec** – Rate is calculated based on packets per second. • **Kbits / Sec** – Rate is calculated based on octets (kilobits per second).
IFG	Determines whether preamble and IFG (20 bytes total) are included in the ingress storm control rate calculation: • **Excluded** – Preamble and IFG are not counted. • **Included** – Preamble and IFG are counted.



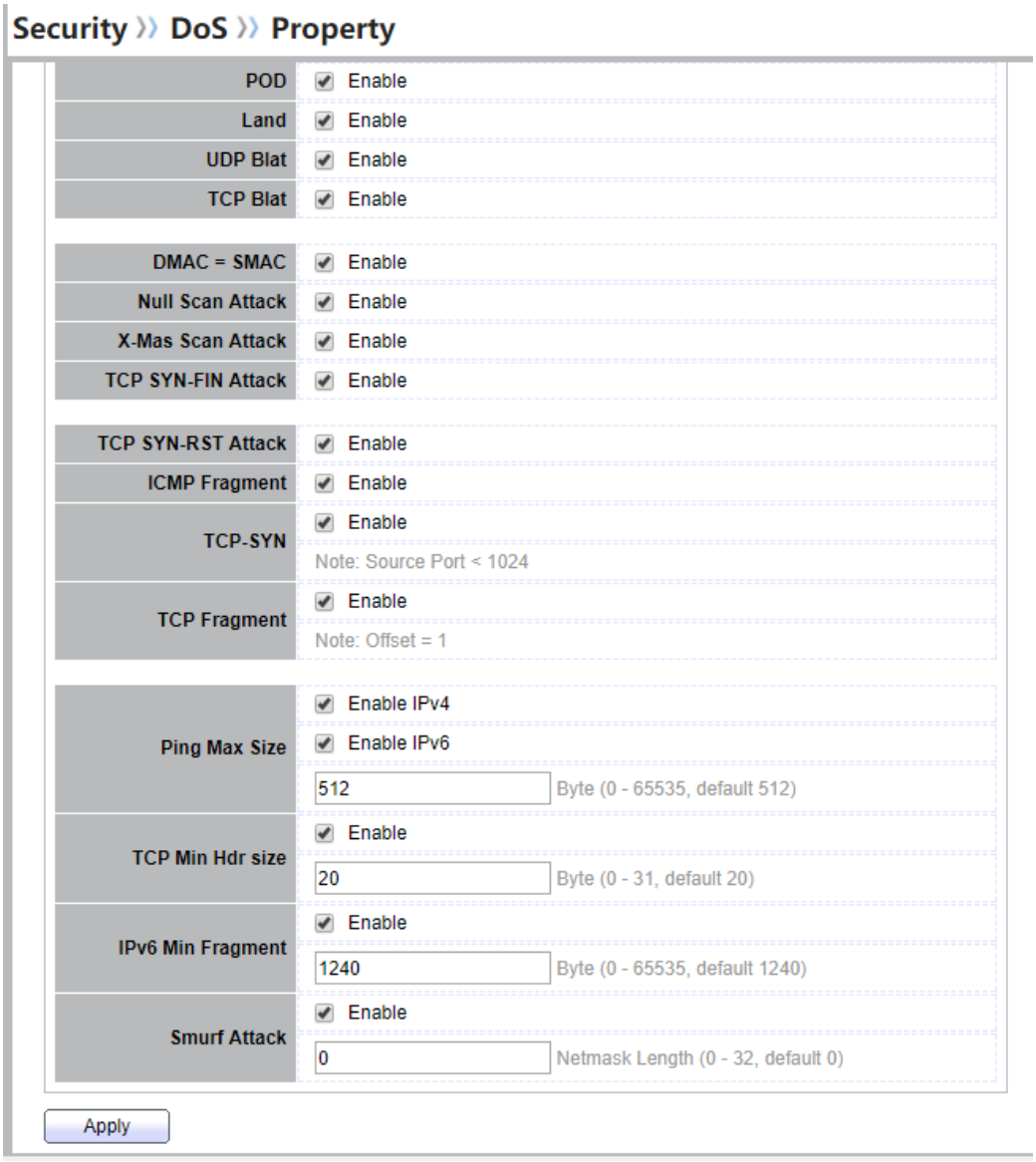
Field	Description
Port	Select the ports to configure.
State	Enables or disables storm control on the selected ports: • **Enable** – Storm control is active. • **Disable** – Storm control is inactive.
Broadcast	Enables storm control for broadcast packets. The rate value depends on the global unit setting: • **pps** (1–262143 packets per second) • **Kbps** (16–1,000,000 kilobits per second)
Unknown Multicast	Enables storm control for unknown multicast packets. Rate value follows the global unit setting: • **pps** (1–262143) • **Kbps** (16–1,000,000)
Unknown Unicast	Enables storm control for unknown unicast packets. Rate value follows the global unit setting: • **pps** (1–262143) • **Kbps** (16–1,000,000)
Action	Defines the action taken when traffic exceeds the configured storm control rate: • **Drop** – Excess packets are discarded. • **Shutdown** – The port is shut down when the storm threshold is exceeded.

DoS Protection

Use this page to configure Denial-of-Service protection mechanisms.

Navigation: Security → DoS

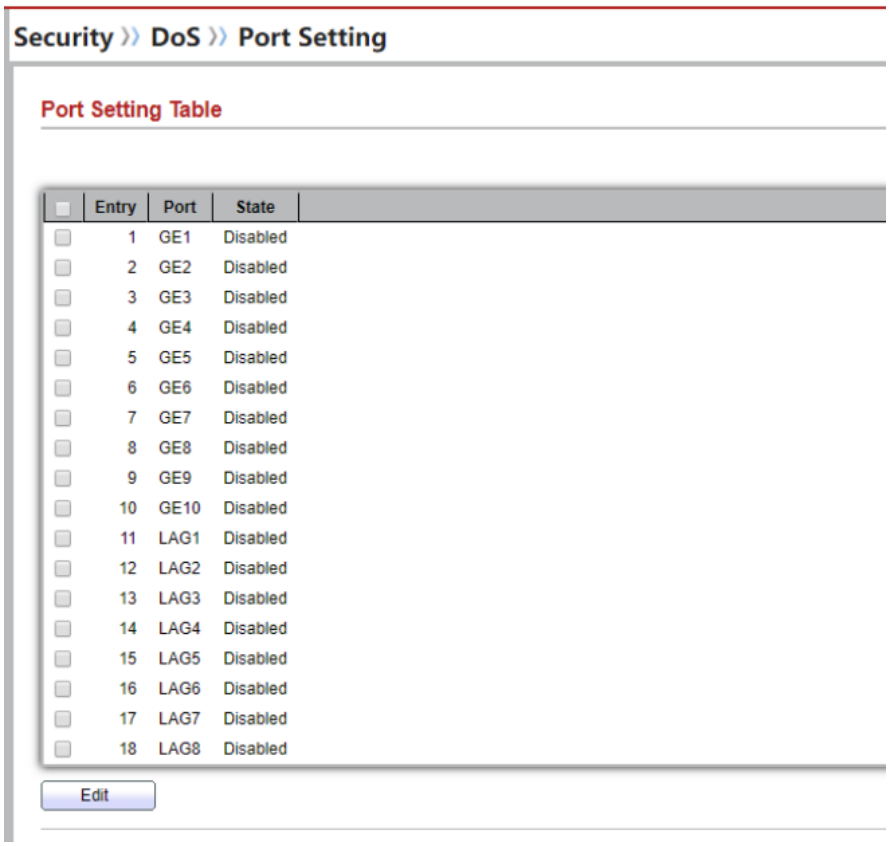
PROPERTY



Field	Description
POD	Protects against Ping-of-Death attacks.
Land	Drops packets where the source IP address equals the destination IP address.
UDP Blat	Drops packets where the UDP source port equals the UDP destination port.

TCP Blat	Drops packets where the TCP source port equals the TCP destination port.
DMAC = SMAC	Drops packets where the destination MAC equals the source MAC.
Null Scan Attack	Drops packets with NULL scan characteristics (no TCP flags set).
X-Mas Scan Attack	Drops packets with FIN, URG, and PSH flags set and sequence number zero.
TCP SYN-FIN Attack	Drops packets with both SYN and FIN flags set.
TCP SYN-RST Attack	Drops packets with both SYN and RST flags set.
ICMP Fragment	Drops fragmented ICMP packets.
TCP SYN (SPORT < 1024)	Drops TCP SYN packets where the source port is less than 1024.
TCP Fragment (Offset = 1)	Drops TCP fragments where the fragment offset equals 1.
Ping Max Size	Specifies the maximum allowed ICMPv4/ICMPv6 ping packet size (0–65535 bytes). Default: **512 bytes**.
IPv4 Ping Max Size	Drops ICMPv4 packets larger than the configured maximum size.
IPv6 Ping Max Size	Drops ICMPv6 packets larger than the configured maximum size.
TCP Min Hdr Size	Drops TCP packets with a header smaller than the configured minimum size (0–31 bytes). Default: **20 bytes**.
IPv6 Min Fragment	Drops IPv6 fragments smaller than the configured minimum size (0–65535 bytes). Default: **1240 bytes**.
Smurf Attack	Protects against Smurf attacks. Netmask length range: **0–323 bytes**, default **0 bytes**.

PORT SETTING



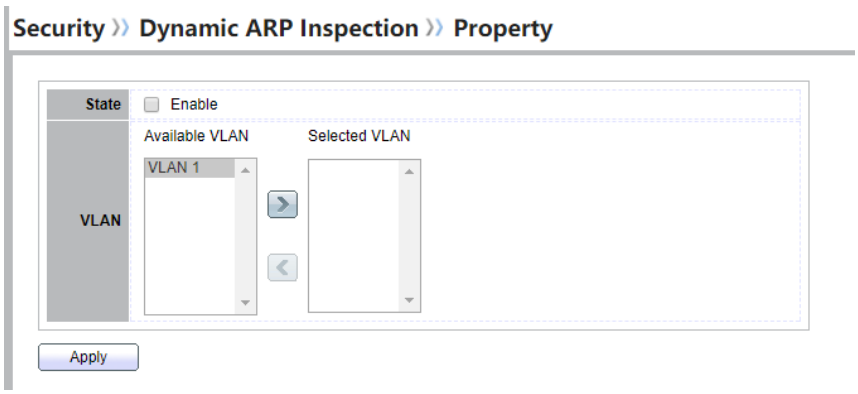
Field	Description
Port	Port name.
State	Enables or disables DoS protection on the port.

Dynamic ARP Inspection (DAI)

DAI prevents ARP spoofing by validating ARP packets.

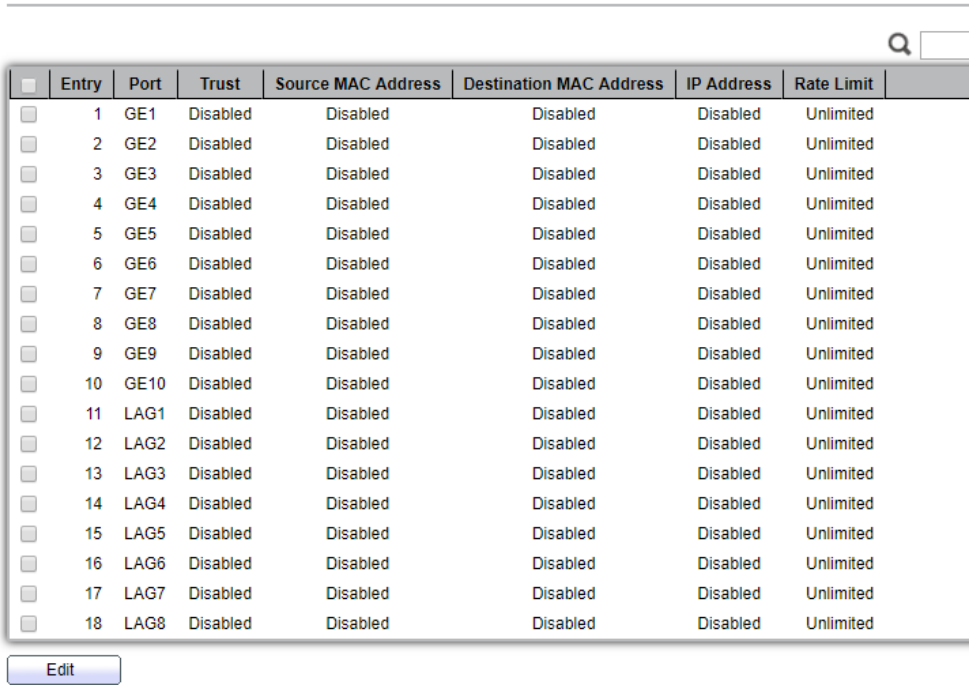
Navigation: Security → Dynamic ARP Inspection

PROPERTY



Field	Description
State	Enables or disables Dynamic ARP Inspection.
VLAN	Select VLANs to enable or disable DAI: Move VLANs **from left to right** to enable DAI. Move VLANs **from right to left** to disable DAI.

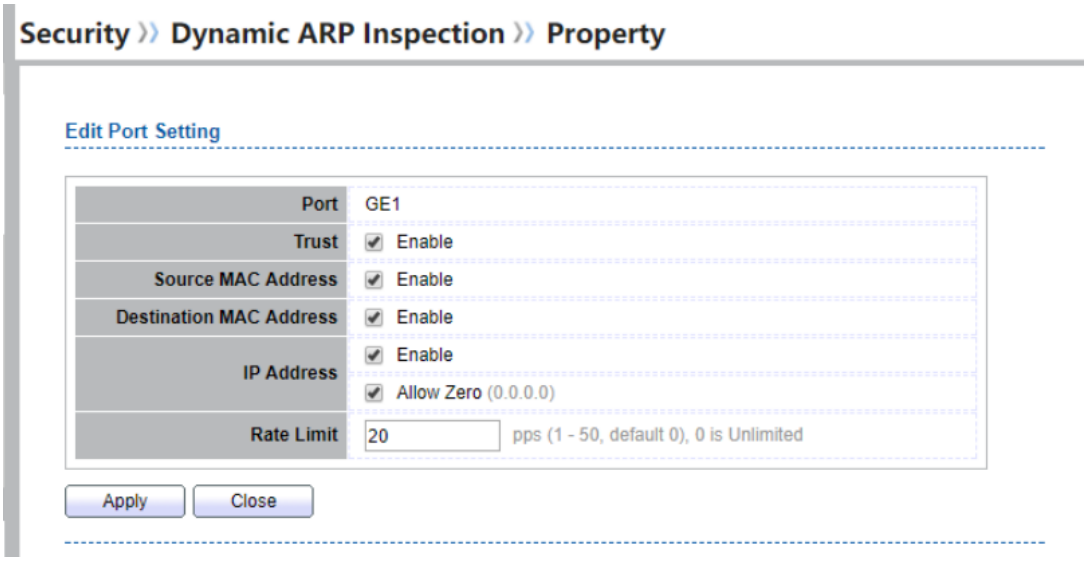
Port Setting Table



Entry	Port	Trust	Source MAC Address	Destination MAC Address	IP Address	Rate Limit
1	GE1	Disabled	Disabled	Disabled	Disabled	Unlimited
2	GE2	Disabled	Disabled	Disabled	Disabled	Unlimited
3	GE3	Disabled	Disabled	Disabled	Disabled	Unlimited
4	GE4	Disabled	Disabled	Disabled	Disabled	Unlimited
5	GE5	Disabled	Disabled	Disabled	Disabled	Unlimited
6	GE6	Disabled	Disabled	Disabled	Disabled	Unlimited
7	GE7	Disabled	Disabled	Disabled	Disabled	Unlimited
8	GE8	Disabled	Disabled	Disabled	Disabled	Unlimited
9	GE9	Disabled	Disabled	Disabled	Disabled	Unlimited
10	GE10	Disabled	Disabled	Disabled	Disabled	Unlimited
11	LAG1	Disabled	Disabled	Disabled	Disabled	Unlimited
12	LAG2	Disabled	Disabled	Disabled	Disabled	Unlimited
13	LAG3	Disabled	Disabled	Disabled	Disabled	Unlimited
14	LAG4	Disabled	Disabled	Disabled	Disabled	Unlimited
15	LAG5	Disabled	Disabled	Disabled	Disabled	Unlimited
16	LAG6	Disabled	Disabled	Disabled	Disabled	Unlimited
17	LAG7	Disabled	Disabled	Disabled	Disabled	Unlimited
18	LAG8	Disabled	Disabled	Disabled	Disabled	Unlimited

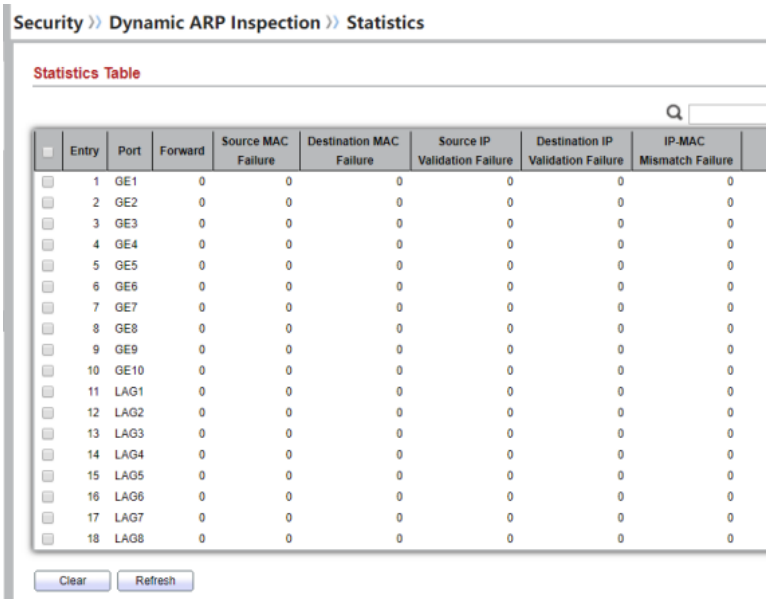
Edit

Field	Description
Port	Displays the port ID.
Trust	Shows whether the interface is trusted or untrusted for ARP inspection. Trusted ports bypass DAI validation.
Source MAC Address	Shows whether source MAC address validation is enabled or disabled on the interface.
Destination MAC Address	Shows whether destination MAC address validation is enabled or disabled on the interface.
IP Address	Shows whether IP address validation is enabled or disabled on the interface. Allows zero-IP (0.0.0.0) when enabled.
Rate Limit	Displays the ARP rate-limit value configured for the interface.



Field	Description
Port	Displays the selected port being edited.
Trust	Enables or disables trust on the interface. When trust is enabled, all ARP packets are forwarded without inspection. Default: **Disabled**.
Source MAC Address	Enables or disables source MAC validation. When enabled, ARP packets are checked to ensure the sender MAC matches the source MAC in the Ethernet header. Default: **Disabled**.
Destination MAC Address	Enables or disables destination MAC validation. When enabled, ARP packets are checked to ensure the target MAC matches the destination MAC in the Ethernet header. Default: **Disabled**.
IP Address	Enables or disables IP address validation. When enabled, ARP packets are checked to ensure the IP address is not 0.0.0.0, 255.255.255.255, or a multicast address. Default: **Disabled**.
IP Address – Allow Zero	Enables or disables acceptance of 0.0.0.0 as a valid IP address. When enabled, ARP packets with 0.0.0.0 are permitted. Default: **Disabled**.
Rate Limit	Sets the ARP packet rate limit (pps). A value of **0** means unlimited. Default: **Unlimited**.
IP Address	Enables or disables IP address validation. When enabled, ARP packets are checked to ensure the IP address is not 0.0.0.0, 255.255.255.255, or a multicast address. Default: **Disabled**.

STATISTICS



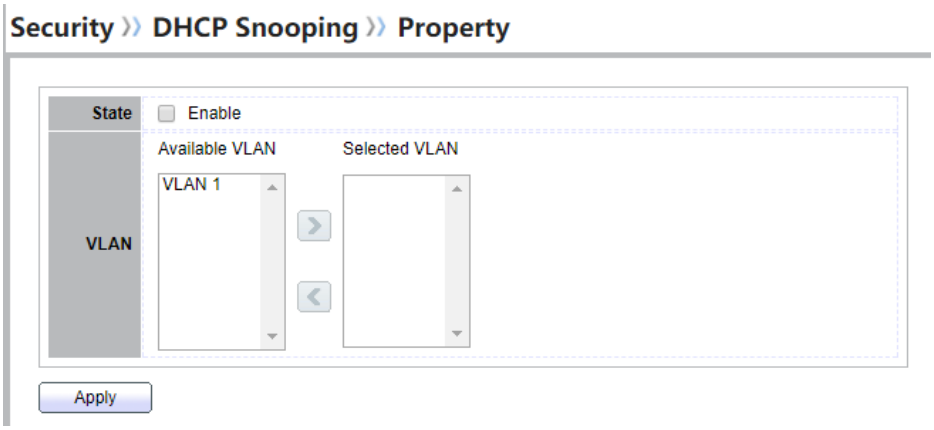
Field	Description
Port	Displays the port ID.
Forwarded	Shows the number of ARP packets forwarded normally.
Source MAC Failures	Shows how many ARP packets were dropped due to source MAC validation failure.
Destination MAC Failures	Shows how many ARP packets were dropped due to destination MAC validation failure.
Source IP Validation Failures	Shows how many ARP packets were dropped due to source IP validation failure.
Destination IP Validation Failures	Shows how many ARP packets were dropped due to destination IP validation failure.
IP-MAC Mismatch Failures	Shows how many ARP packets were dropped because the IP-MAC binding did not match the IP Source Guard binding table.

DHCP SNOOPING

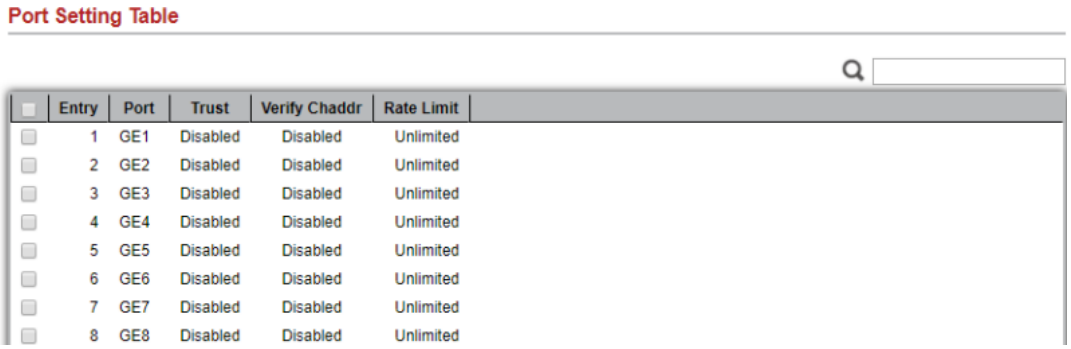
DHCP Snooping protects against rogue DHCP servers.

Navigation: Security → DHCP Snooping

PROPERTY



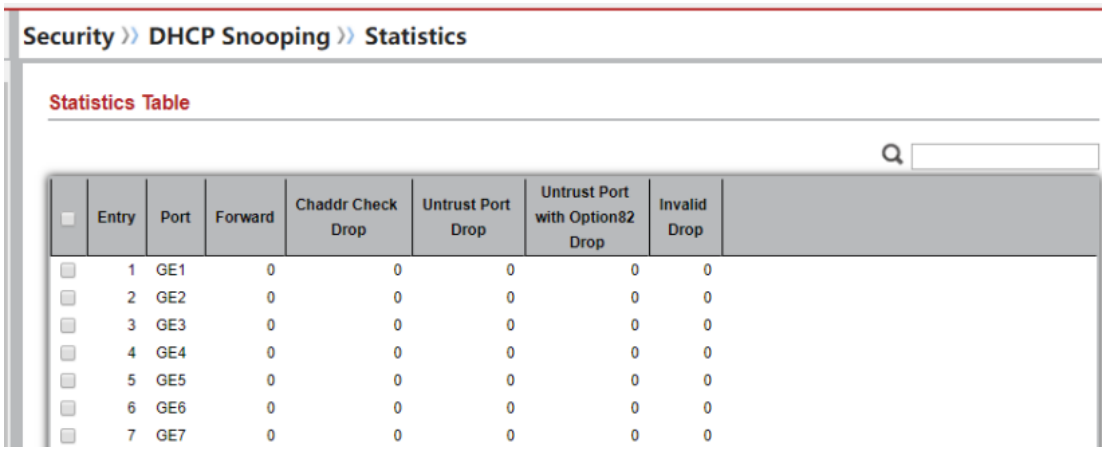
Field	Description
State	Enables or disables Dynamic ARP Inspection.
VLAN	Select VLANs to enable or disable DAI: Move VLANs **from left to right** to enable DAI. Move VLANs **from right to left** to disable DAI.



Field	Description
Port	Displays the selected port being edited.
Trust	Enables or disables trust on the interface. When trust is enabled, all DHCP packets are forwarded directly without inspection. Default: **Disabled**.

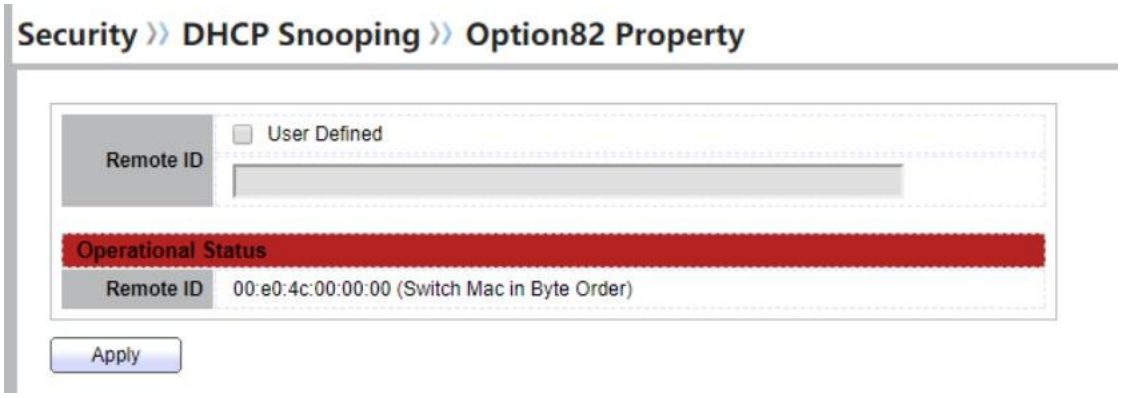
Verify Chaddr	Enables or disables chaddr (client hardware address) validation. When enabled, DHCP packets are checked to ensure the client hardware MAC address matches the source MAC in the Ethernet header. Default: **Disabled**.
Rate Limit	Sets the DHCP packet rate limit (pps). A value of **0** means unlimited. Default: **Unlimited**.

STATISTICS

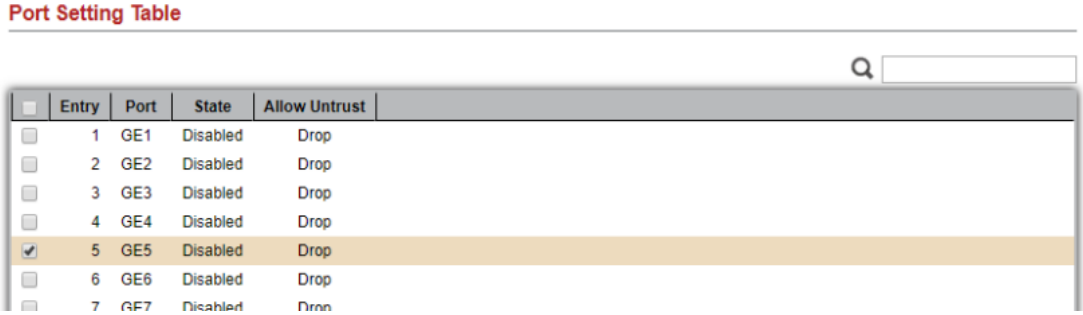


Field	Description
Port	Displays the port ID.
Forwarded	Shows how many DHCP packets were forwarded normally.
Chaddr Check Drop	Shows how many DHCP packets were dropped due to chaddr (client hardware address) validation failure.
Untrusted Port Drop	Shows how many DHCP server packets received on an untrusted port were dropped.
Untrusted Port with Option-82 Drop	Shows how many DHCP packets were dropped due to Option-82 checks on an untrusted port.
Invalid Drop	Shows how many DHCP packets were dropped due to general invalid packet checking.
Port	Displays the port ID.

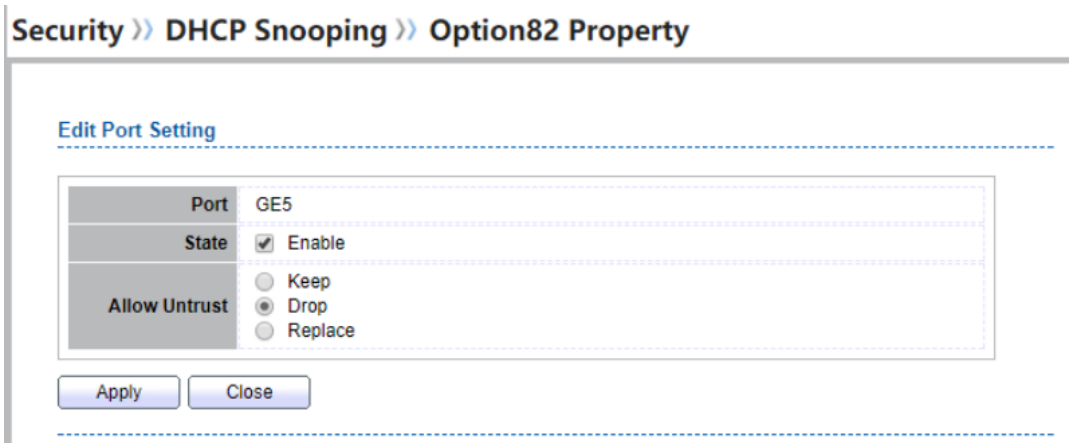
OPTION 82 PROPERTY



Field	Description
User Defined	Enables or disables the use of a user-defined Remote-ID. When disabled, the switch MAC address is used by default.
Remote ID	Specifies the user-defined Remote-ID value. This field is only available when **User Defined** is enabled.

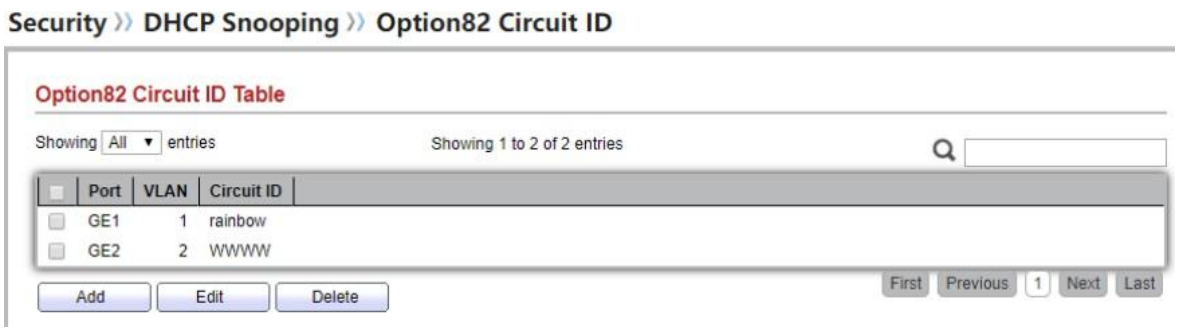


Field	Description
Port	Displays the port ID.
Enable	Shows whether Option-82 is enabled or disabled on the interface.
Allow Untrusted	Shows whether untrusted ports are allowed to process Option-82 information.

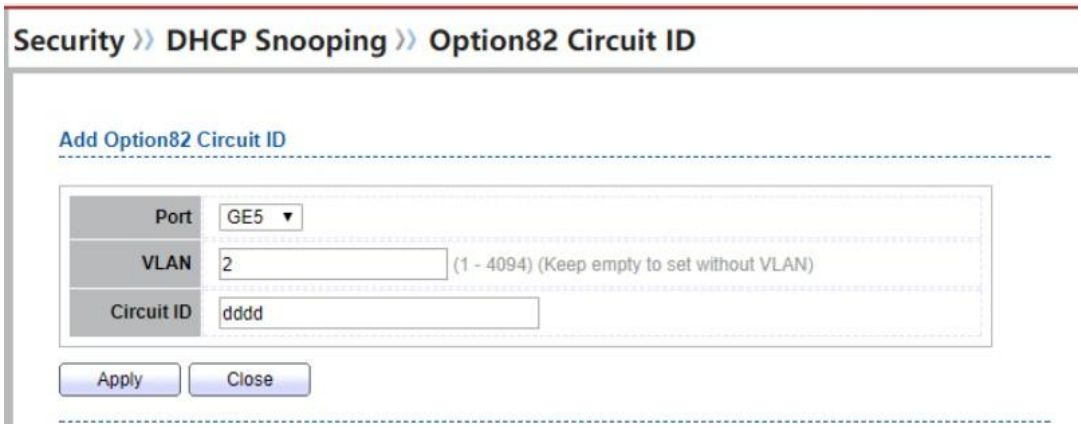


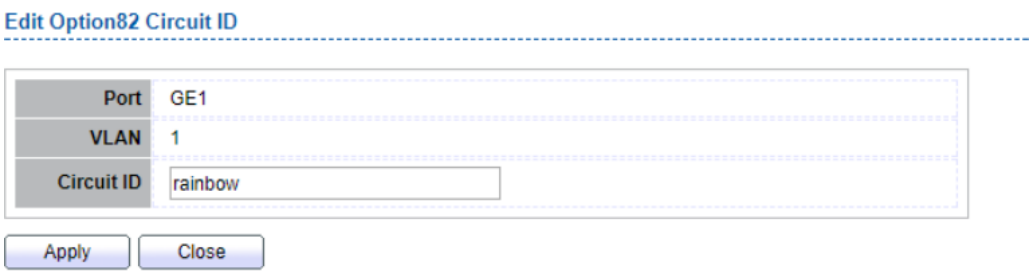
Field	Description
Port	Displays the selected port being edited.
State	Enables or disables Option-82 processing on the interface.
Allow Untrusted	Defines how the interface handles DHCP packets containing Option-82 when received on an untrusted port. Default: **Drop**. • **Keep** – Keep the original Option-82 content. • **Replace** – Replace Option-82 content with the switch's configured Option-82 settings. • **Drop** – Drop packets containing Option-82.

OPTION 82 CIRCUIT ID



Field	Description
Port	Displays the port ID associated with the binding entry.
VLAN	Displays the VLAN ID associated with the binding entry.
Circuit ID	Displays the Circuit-ID string for the entry, as provided by Option-82.



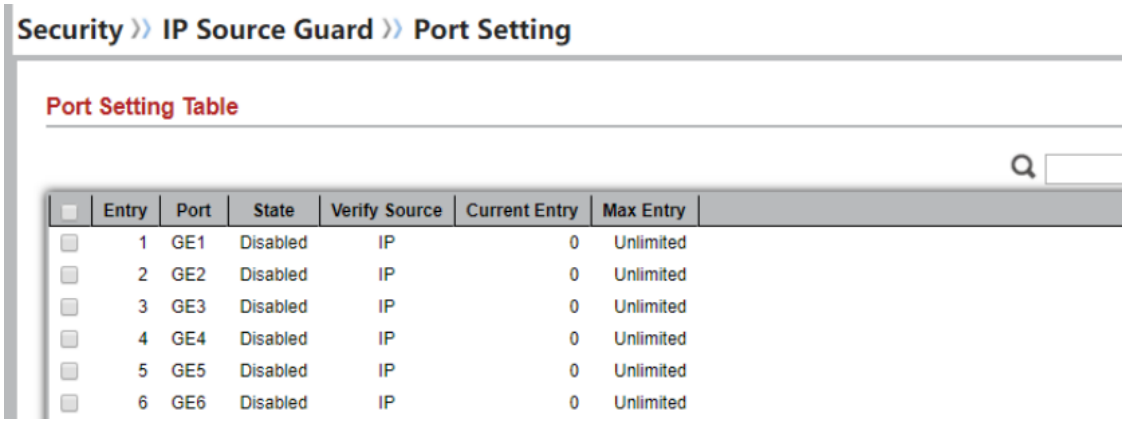


Field	Description
Port	Selects the port to associate with the Circuit-ID entry. This field is only available in the **Add** dialog.
VLAN	Specifies the VLAN ID to associate with the Circuit-ID entry. VLAN is optional. This field is only available in the **Add** dialog.
Circuit ID	Specifies the Circuit-ID string. DHCP packets matching the selected port and VLAN will have this Circuit-ID inserted.

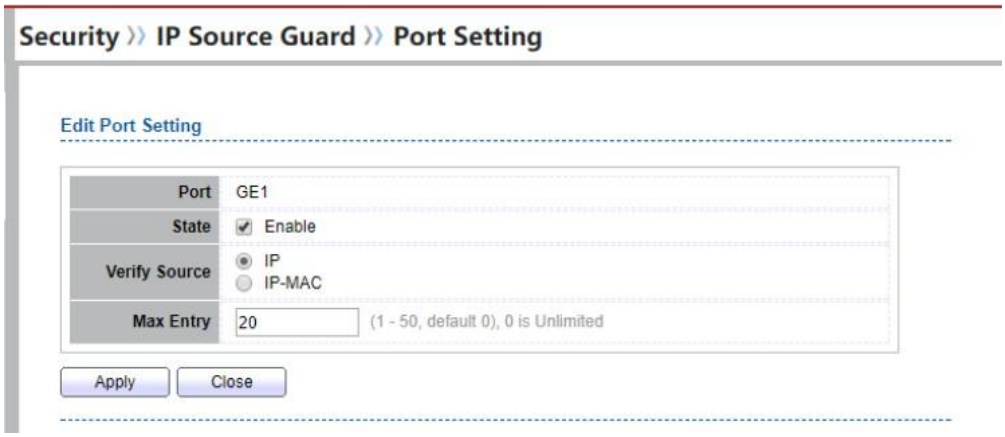
IP Source Guard

IP Source Guard prevents IP spoofing by binding IP/MAC/Port combinations.
Navigation: Security → IP Source Guard

PORT SETTING

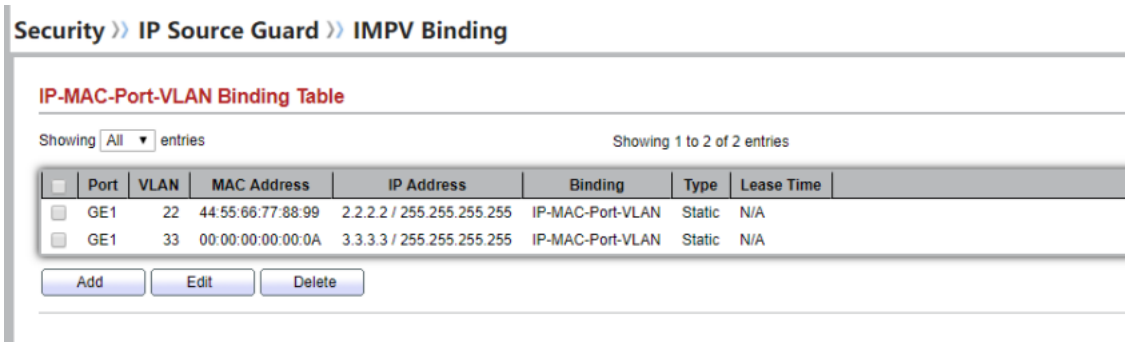


Field	Description
Port	Displays the port ID.
State	Shows whether IP Source Guard is enabled or disabled on the interface.
Verify Source	Displays the verification mode used by IP Source Guard (e.g., IP, MAC, or IP-MAC binding checks).
Current Binding Entry	Shows the number of active binding entries currently associated with the interface.
MAX Binding Entry	Displays the maximum number of binding entries supported for the interface.



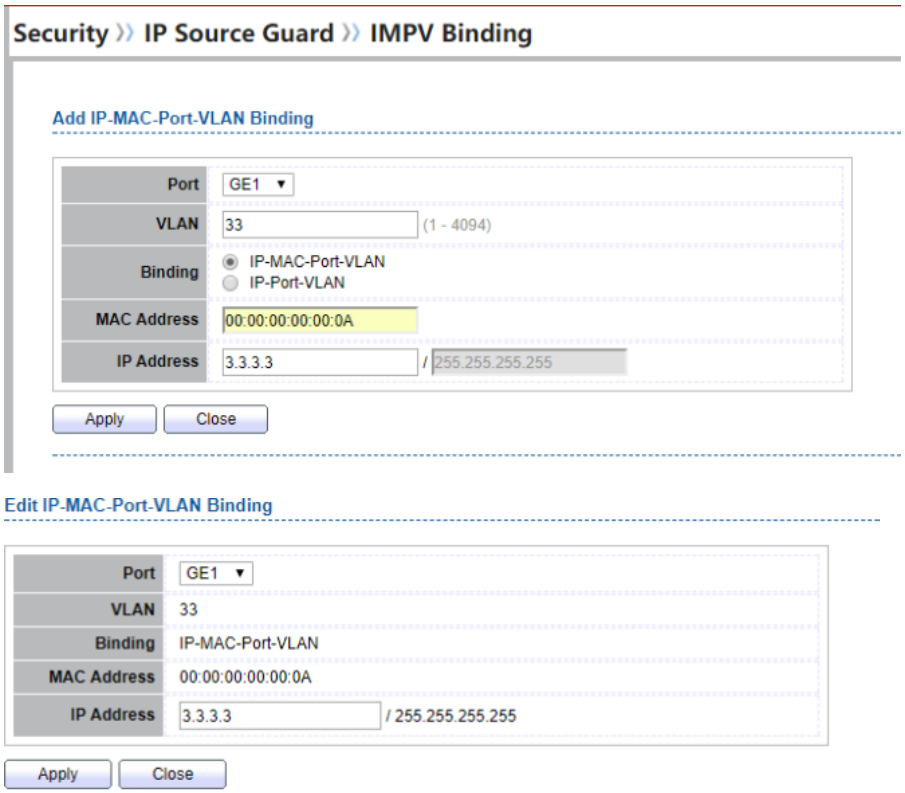
Field	Description
Port	Displays the selected port being edited.
Status	Enables or disables IP Source Guard on the interface. Default: **Disabled**.
Verify Source	Selects the verification mode used by IP Source Guard: • **IP** – Verifies only the source IP address of packets. • **IP-MAC** – Verifies both the source IP and source MAC address of packets.
Max Binding Entry	Specifies the maximum number of binding entries allowed on the port. Default: **Unlimited**. When the limit is reached, no additional entries will be bound.

IMPV BINDING



Field	Description
Port	Displays the port ID associated with the binding entry.
VLAN	Displays the VLAN ID associated with the binding entry.
MAC Address	Displays the MAC address of the entry. Only shown for **IP-MAC** binding entries.
IP Address	Displays the IP address of the entry. For IP-MAC bindings, the mask is always **255.255.255.255**. For IP-only bindings, the mask reflects the user-configured value.

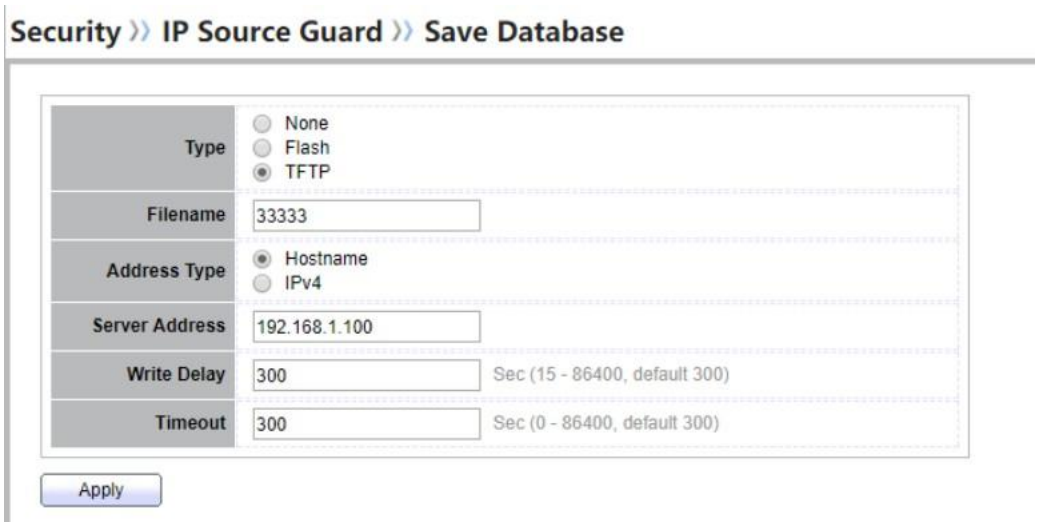
Binding Type	Displays the type of binding entry.
Type	Indicates how the entry was created: • **Static** – Entry added manually by the user. • **Dynamic** – Entry learned automatically via DHCP Snooping.
Lease Time	Shows the remaining lease time for DHCP Snooping dynamic entries. When the lease expires, the entry is removed. Only available for **dynamic** entries.



Field	Description
Port	Selects the port associated with the binding entry.
VLAN	Specifies the VLAN ID for the binding entry.
Binding	Selects the matching mode for the binding entry: • **IP-MAC-Port-VLAN** – Packet must match IP address, MAC address, port, and VLAN ID. • **IP-Port-VLAN** – Packet must match IP address or subnet, port, and VLAN ID.
MAC Address	Specifies the MAC address for the binding entry. Only available when **IP-MAC-Port-VLAN** mode is selected.
IP Address	Specifies the IP address and mask for the binding entry. The mask is only available when using **IP-MAC-Port** mode.

SAVE DATABASE

Stores the current binding table to flash.



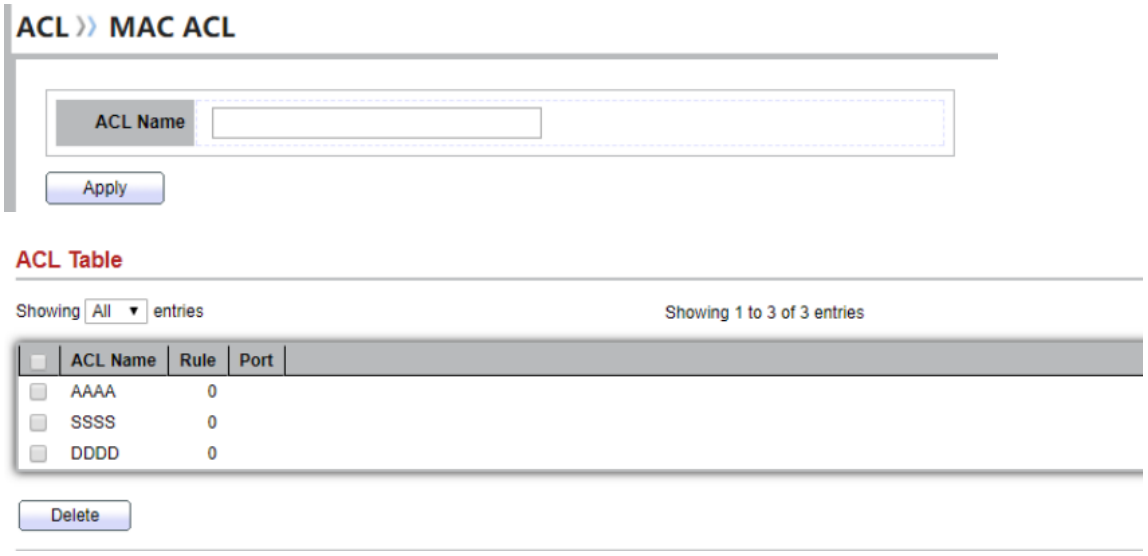
Field	Description
Type	Selects the database agent type: • **None** – Disables the database agent service. • **Flash** – Saves DHCP dynamic binding entries to flash. • **TFTP** – Saves DHCP dynamic binding entries to a remote TFTP server.
Filename	Specifies the filename for the backup file. Available only when **Flash** or **TFTP** is selected.
Address Type	Selects the address type for the TFTP server: • **Hostname** – TFTP server address is a hostname. • **IPv4** – TFTP server address is an IPv4 address.
Server Address	Specifies the remote TFTP server hostname or IP address. Available only when **TFTP** is selected.
Write Delay	Sets the delay timer before performing a backup after a change occurs. Default: **300 seconds**.
Timeout	Sets the timeout for aborting a backup operation if it fails. Default: **300 seconds**.

ACCESS CONTROL LISTS (ACL)

ACLs allow you to classify, filter, and control traffic based on MAC, IPv4, or IPv6 criteria. They provide granular control over which packets are permitted or denied, enabling enhanced security, traffic shaping, and policy enforcement across the switch.
ACLs are applied to interfaces or globally, depending on the configuration. Each ACL consists of one or more ACEs (Access Control Entries), which define the matching conditions and actions.

MAC ACL

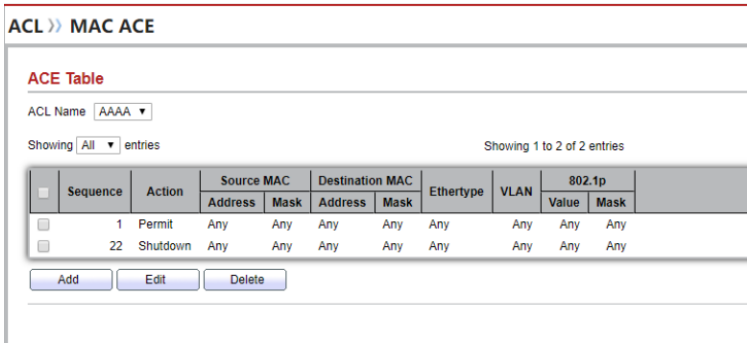
Use this page to configure MAC-based ACLs, which filter traffic based on Layer 2 attributes such as MAC addresses, EtherType, and VLAN information.
Navigation: ACL → MAC ACL



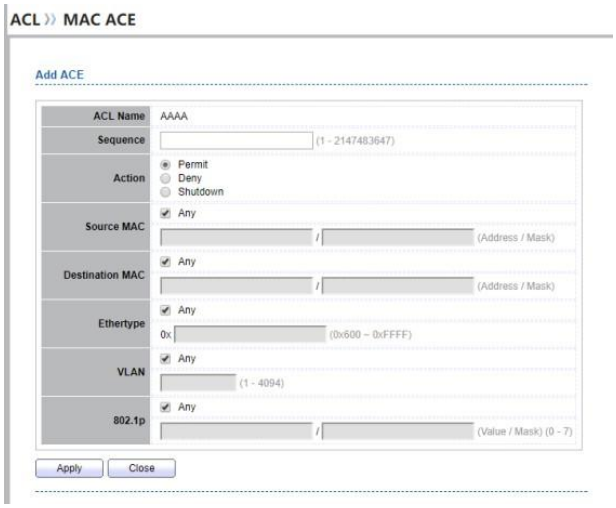
Field	Description
ACL Name	Displays the name of the MAC ACL. This identifies the ACL and is used when binding it to ports or adding ACE rules.
Rule	Shows the total number of ACE (Access Control Entry) rules currently defined within this ACL. This helps indicate ACL complexity and processing order.
Port	Lists all ports where this ACL is currently bound. The ACL will only take effect on the ports shown here.

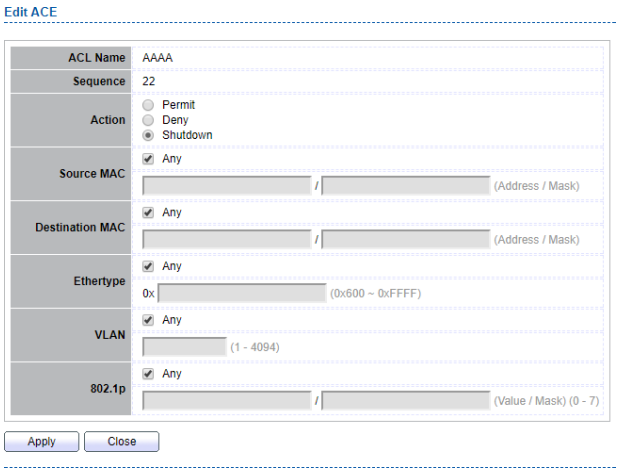
MAC ACE

MAC ACEs define individual match rules within a MAC ACL.
Navigation: ACL → MAC ACE



Field	Description
ACL Name	Displays the name of the MAC ACL this ACE belongs to. All ACEs inside the ACL are evaluated in priority order.
Priority	Shows the ACE's processing order. Lower numbers have higher priority and are matched first. This determines which ACE is evaluated before others.
Action	Indicates the action applied when the ACE matches traffic. Options are **Permit** (forward the packet) or **Deny** (drop the packet).
Service	Displays the management service type matched by the ACE. This may include HTTP, HTTPS, SNMP, SSH, Telnet, or **All** services.
Port	Shows the list of ports to which this ACE applies. Only traffic entering these ports is evaluated by this ACE.
Address / Mask	Displays the source IP address and mask used for matching. This may be IPv4 or IPv6 depending on the ACE configuration.





Field	Description
ACL Name	Displays the name of the ACL to which this ACE will be added. This identifies the ACL context and cannot be changed when editing an existing ACE.
Sequence	Specifies the processing order of the ACE. Lower numbers have higher priority and are evaluated first. Sequence is only configurable when adding a new ACE.
Action	Defines what happens when a packet matches this ACE: • **Permit** – Forward packets that meet the ACE criteria. • **Deny** – Drop packets that meet the ACE criteria. • **Shutdown** – Drop matching packets and administratively disable the port that received them. The port can later be re-enabled from the Port Settings page.
Source MAC	Selects how the source MAC address is matched: • **Any** – Accepts all source MAC addresses. • **User Defined** – Matches only the specified MAC address or a range defined by a MAC + mask.
Destination MAC	Selects how the destination MAC address is matched: • **Any** – Accepts all destination MAC addresses. • **User Defined** – Matches

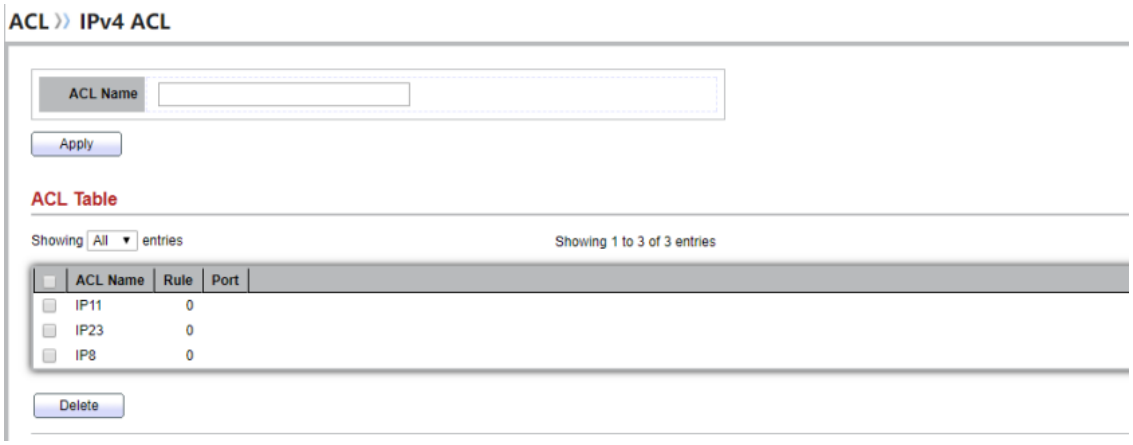
	only the specified destination MAC address or a range defined by a MAC + mask.
Ethertype	Selects how the Ethernet frame type is matched: • **Any** – Accepts all EtherTypes. • **User Defined** – Matches only the specified EtherType value (e.g., 0x0800 for IPv4, 0x86DD for IPv6).
VLAN ID	Selects how VLAN ID is matched: • **Any** – Accepts all VLAN IDs. • **User Defined** – Matches only the specified VLAN ID.
802.1p	Selects how the 802.1p priority value is matched: • **Any** – Accepts all 802.1p values. • **User Defined** – Matches a specific 802.1p value or a range defined by a value + mask.

IPv4 ACL

Use this page to configure IPv4 ACLs, which filter traffic based on Layer 3 and Layer 4 attributes such as IP addresses, protocol types, and TCP/UDP ports.

Navigation: ACL → IPv4 ACL

Field	Description
ACL Name	Name of the IPv4 ACL.



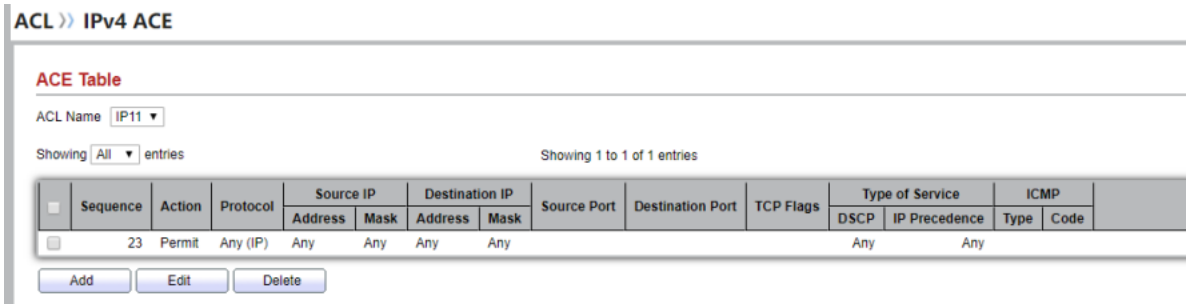
Field	Description
ACL Name	Displays the name of the IPv4 ACL. This identifies the ACL and is used when adding ACE rules or binding the ACL to ports.

Rule	Shows the total number of ACE (Access Control Entry) rules defined within this IPv4 ACL. This provides a quick view of how many match conditions the ACL contains.
Port	

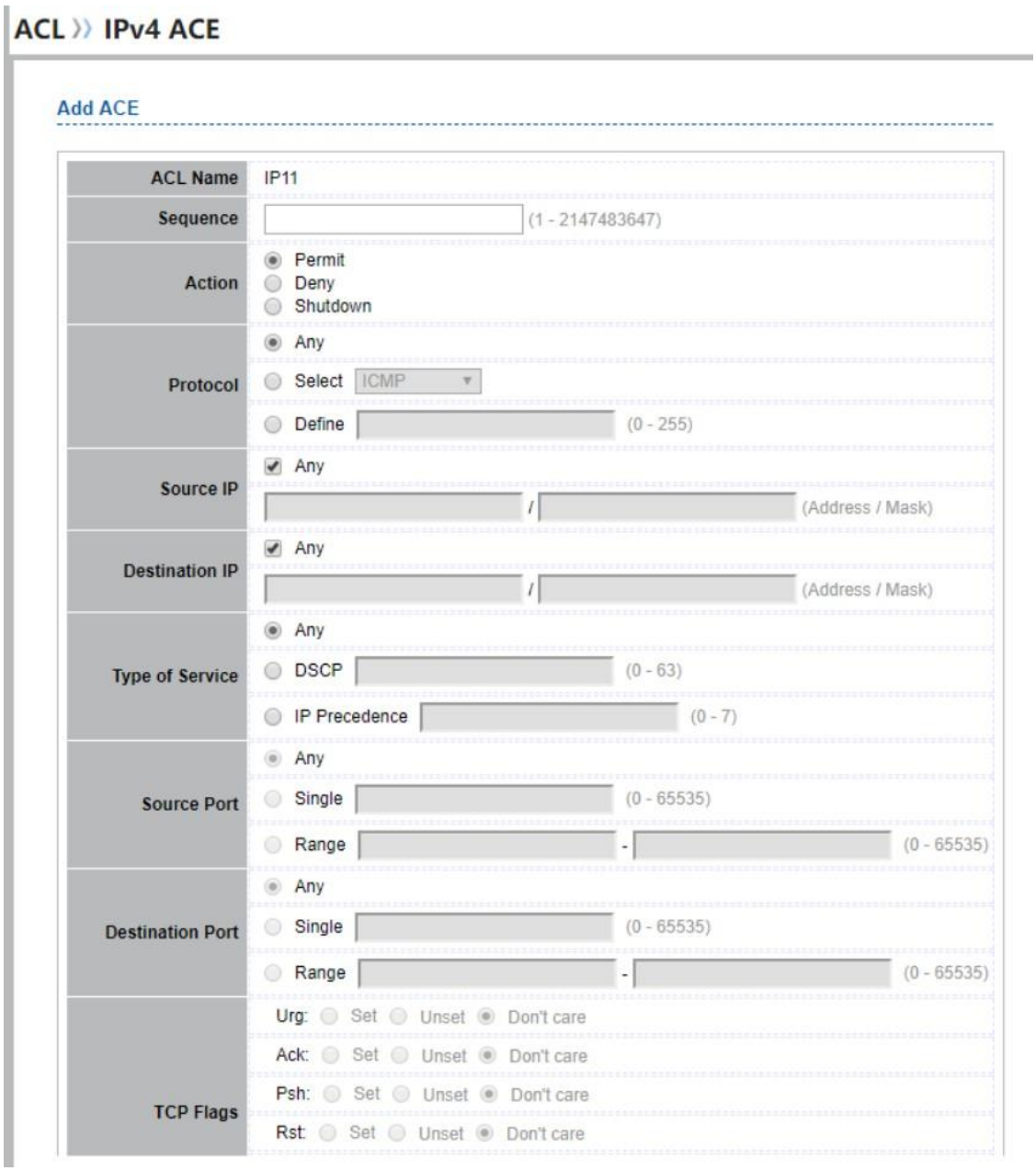
IPv4 ACE

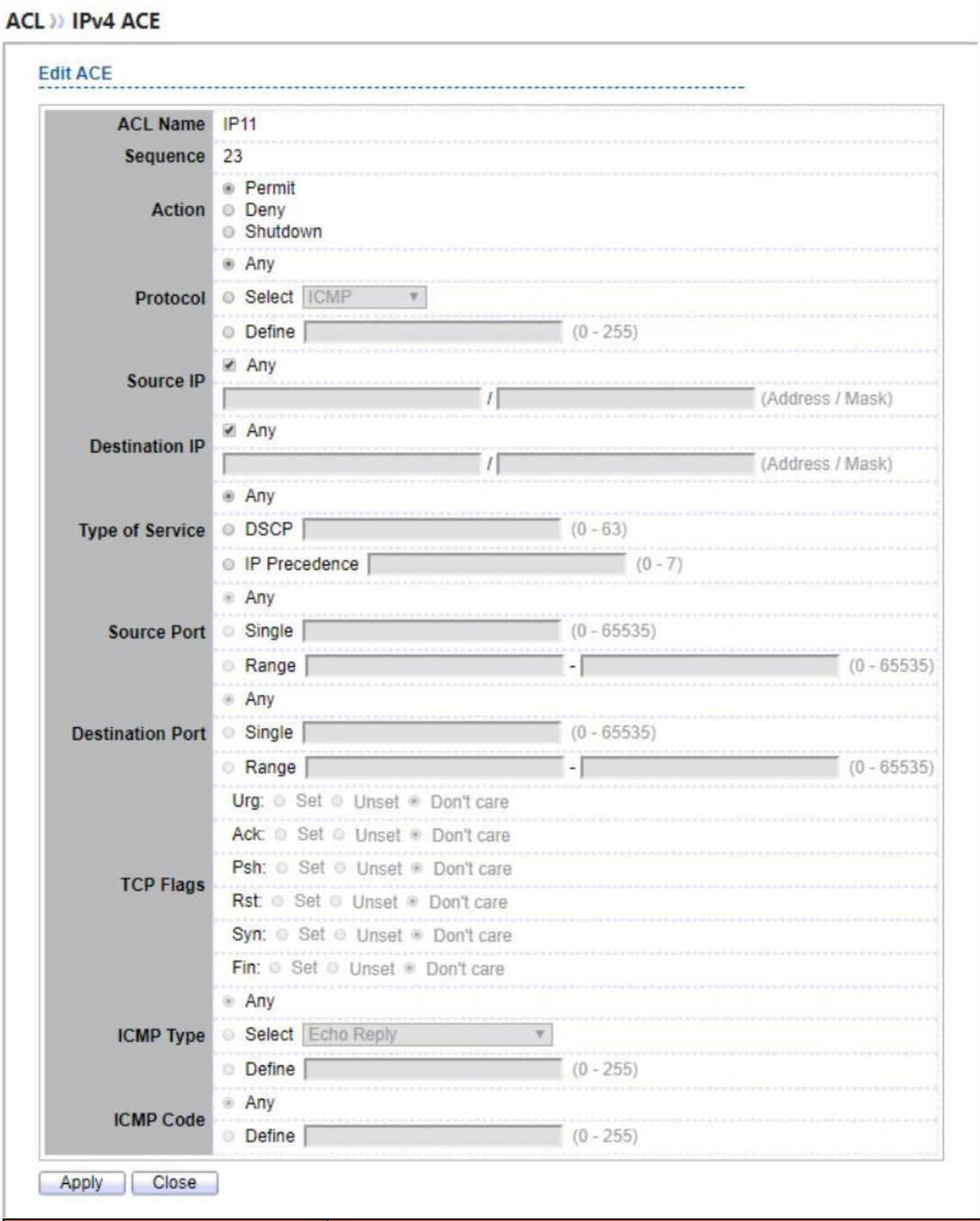
IPv4 ACEs define individual match rules within an IPv4 ACL.

Navigation: ACL → IPv4 ACE



Field	Description
ACL Name	Selects the IPv4 ACL to which this ACE belongs. This determines the ACL context and ensures the ACE is added to the correct rule set.
Sequence	Displays the ACE's processing order within the ACL. Lower sequence numbers have higher priority and are evaluated first. This defines how traffic is matched when multiple ACEs exist.
Action	Shows the action applied when a packet matches this ACE. Options include **Permit**, **Deny**, or **Shutdown** (drop the packet and disable the receiving port).
Protocol	Displays the protocol matched by the ACE. Supported values include **TCP**, **UDP**, **ICMP**, or **Any**, depending on configuration.
Source IP	Shows the source IPv4 address and mask used for matching. This defines the host or subnet from which traffic must originate to match the ACE.
Destination IP	Shows the destination IPv4 address and mask used for matching. This defines the target host or subnet for the ACE.
Source Port	Displays the source port or port range matched by the ACE. Only available when the protocol is **TCP** or **UDP**.
Destination Port	Displays the destination port or port range matched by the ACE. Only available when the protocol is **TCP** or **UDP**.
TCP Flags	Displays the TCP flag conditions matched by the ACE (e.g., SYN, ACK, FIN). Only available when the protocol is **TCP**.
Type of Service	Shows the ToS value matched by the ACE. This may be **DSCP** or **IP Precedence**, depending on configuration.
ICMP	Displays the ICMP type and code matched by the ACE. Only available when the protocol is **ICMP**.


ACL » IPv4 ACE
Add ACE
ACL Name
IP11
Sequence
(1 - 2147483647)
Action
Permit
Deny
Shutdown
Protocol
Any
Select
ICMP
Define
(0 - 255)
Source IP
Any
(Address / Mask)
Destination IP
Any
(Address / Mask)
Type of Service
Any
DSCP
(0 - 63)
IP Precedence
(0 - 7)
Source Port
Any
Single
(0 - 65535)
Range
(0 - 65535)
Destination Port
Any
Single
(0 - 65535)
Range
(0 - 65535)
TCP Flags
Urg: Set Unset Don't care
Ack: Set Unset Don't care
Psh: Set Unset Don't care
Rst: Set Unset Don't care



Field	Description
ACL Name	Displays the name of the IPv4 ACL to which this ACE is being added. This identifies the ACL context and cannot be changed when editing an existing ACE.
Sequence	Specifies the evaluation order of the ACE. Lower sequence numbers have higher priority and are processed first. Only available when adding a new ACE.
Action	Selects the action applied when a packet matches this ACE: • **Permit** – Forward packets that meet the ACE criteria. • **Deny** – Drop packets that meet the ACE criteria. • **Shutdown** – Drop

	matching packets and administratively disable the port that received them. The port can be reactivated from the Port Settings page.
Protocol	Selects the protocol type to match: • **Any (IP)** – Matches all IP protocols. • **Select from list** – Choose a protocol from the predefined list (ICMP, IPinIP, TCP, EGP, IGP, UDP, HMP, RDP, IPv6, IPv6:ROUT, IPv6:FRAG, RSVP, IPv6:ICMP, OSPF, PIM, L2TP). • **Protocol ID to match** – Enter a specific protocol number manually.
Source IP	Selects how the source IPv4 address is matched: • **Any** – Accepts all source IP addresses. • **User Defined** – Matches only the specified IPv4 address or subnet. Enter the source IP address and mask to define the match range.
Destination IP	Selects how the destination IPv4 address is matched: • **Any** – Accepts all destination IP addresses. • **User Defined** – Matches only the specified IPv4 address or subnet. Enter the destination IP address and mask to define the match range.
Source Port	Selects how the source port is matched. Only available when the protocol is **TCP** or **UDP**: • **Any** – Accepts all source ports. • **Single** – Matches a specific TCP/UDP source port. • **Range** – Matches a range of TCP/UDP source ports. Up to eight port ranges can be configured (shared between source and destination).
Destination Port	Selects how the destination port is matched. Only available when the protocol is **TCP** or **UDP**: • **Any** – Accepts all destination ports. • **Single** – Matches a specific TCP/UDP destination port. • **Range** – Matches a range of TCP/UDP destination ports. Uses the same shared range pool as Source Port.
TCP Flags	Selects one or more TCP flags to filter packets (e.g., SYN, ACK, FIN). Only available when the protocol is **TCP**. Filtering by TCP flags provides granular control over session behaviour and enhances security.
Type of Service	Selects the ToS (Type of Service) match criteria: • **Any** – Accepts all ToS values. • **DSCP to match** – Enter a specific DSCP value. • **IP Precedence to match** – Enter an IP Precedence value.
ICMP Type	Selects the ICMP message type. Only available when the protocol is **ICMP**: • **Any** – Accepts all ICMP types. • **Select from list** – Choose a message type by name. • **Protocol ID to match** – Enter the numeric ICMP type value.
ICMP Code	Selects the ICMP code. Only available when the protocol is **ICMP**: • **Any** – Accepts all ICMP codes. • **User Defined** – Enter a specific ICMP code to match.

IPv6 ACL

Use this page to configure IPv6 ACLs, which filter traffic based on IPv6 addresses, extension headers, and Layer 4 attributes.

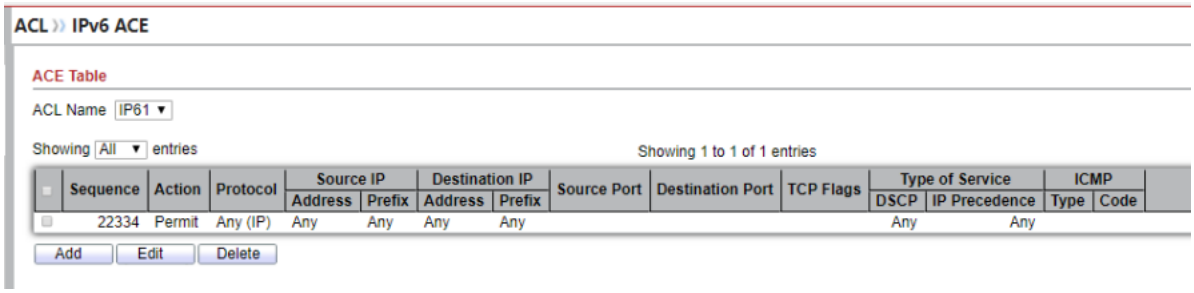
Navigation: ACL → IPv6 ACL

Field	Description
ACL Name	Displays the name of the IPv6 ACL. This identifies the ACL and is used when adding ACE rules or binding the ACL to ports.
Rule	Shows the total number of ACE (Access Control Entry) rules defined within this IPv6 ACL. This provides a quick indication of how many match conditions the ACL contains.
Port	Displays the list of ports where this IPv6 ACL is currently bound. The ACL only affects IPv6 traffic on the ports shown here.

IPv6 ACE

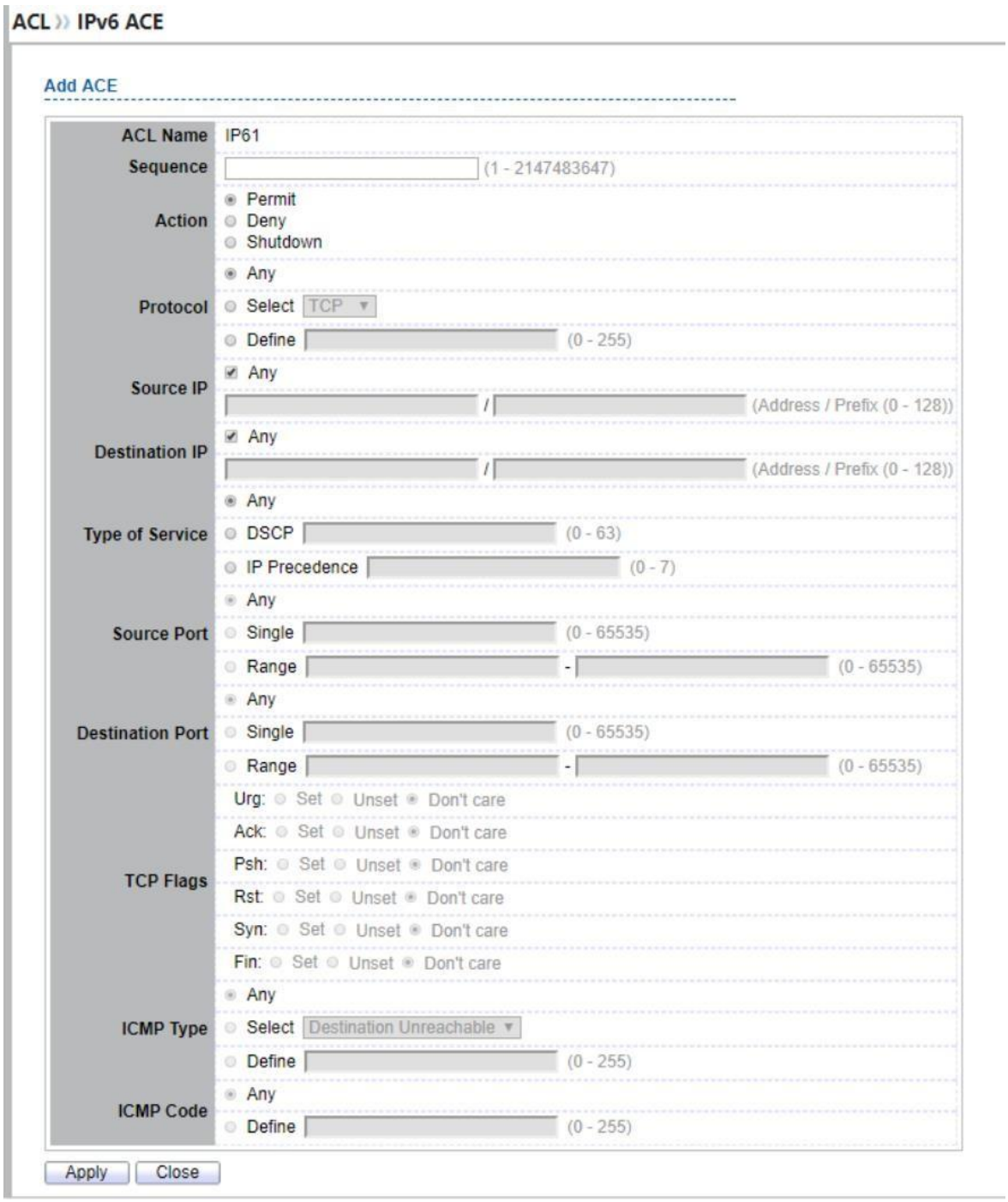
IPv6 ACEs define individual match rules within an IPv6 ACL.

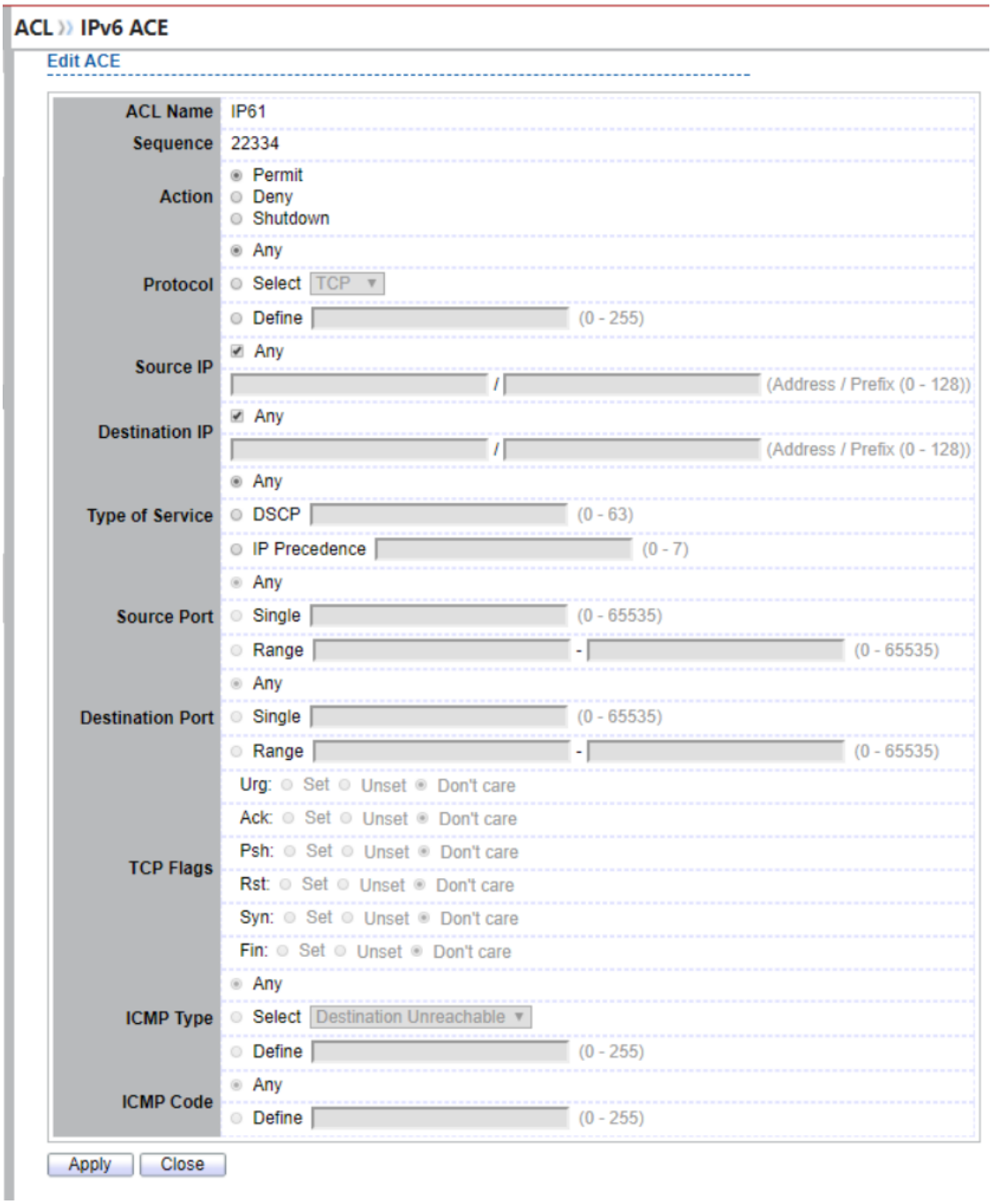
Navigation: ACL → IPv6 ACE



Field	Description
ACL Name	Selects the IPv6 ACL to which this ACE belongs. This identifies the ACL context and ensures the ACE is added to the correct rule set.
Sequence	Displays the ACE's processing order within the ACL. Lower sequence numbers have higher priority and are evaluated first. This determines how traffic is matched when multiple ACEs exist.
Action	Shows the action applied when a packet matches this ACE. Options include **Permit** (forward the packet), **Deny** (drop the packet), or **Shutdown** (drop the packet and administratively disable the receiving port).

Protocol	Displays the protocol matched by the ACE. This may be **TCP**, **UDP**, **ICMPv6**, or any other IPv6-related protocol depending on configuration.
Source IP	Shows the source IPv6 address and prefix length used for matching. This defines the host or subnet from which traffic must originate to match the ACE.
Destination IP	Shows the destination IPv6 address and prefix length used for matching. This defines the target host or subnet for the ACE.
Source Port	Displays the source port or port range matched by the ACE. Only available when the protocol is **TCP** or **UDP**.
Destination Port	Displays the destination port or port range matched by the ACE. Only available when the protocol is **TCP** or **UDP**.
TCP Flags	Displays the TCP flag conditions matched by the ACE (e.g., SYN, ACK, FIN). Only available when the protocol is **TCP**.
Type of Service	Shows the ToS (Type of Service) value matched by the ACE. This may be **DSCP** or **IP Precedence**, depending on configuration.
ICMP	Displays the ICMPv6 type and code matched by the ACE. Only available when the protocol is **ICMP**.


ACL » IPv6 ACE
Add ACE
ACL Name
IP61
Sequence
(1 - 2147483647)
Action
Permit
Deny
Shutdown
Protocol
Any
Select
TCP
Define
(0 - 255)
Source IP
Any
(Address / Prefix (0 - 128))
Destination IP
Any
(Address / Prefix (0 - 128))
Type of Service
Any
DSCP
(0 - 63)
IP Precedence
(0 - 7)
Source Port
Any
Single
(0 - 65535)
Range
(0 - 65535)
Destination Port
Any
Single
(0 - 65535)
Range
(0 - 65535)
TCP Flags
Urg: Set Unset Don't care
Ack: Set Unset Don't care
Psh: Set Unset Don't care
Rst: Set Unset Don't care
Syn: Set Unset Don't care
Fin: Set Unset Don't care
ICMP Type
Any
Select
Destination Unreachable
Define
(0 - 255)
ICMP Code
Any
Define
(0 - 255)
Apply
Close



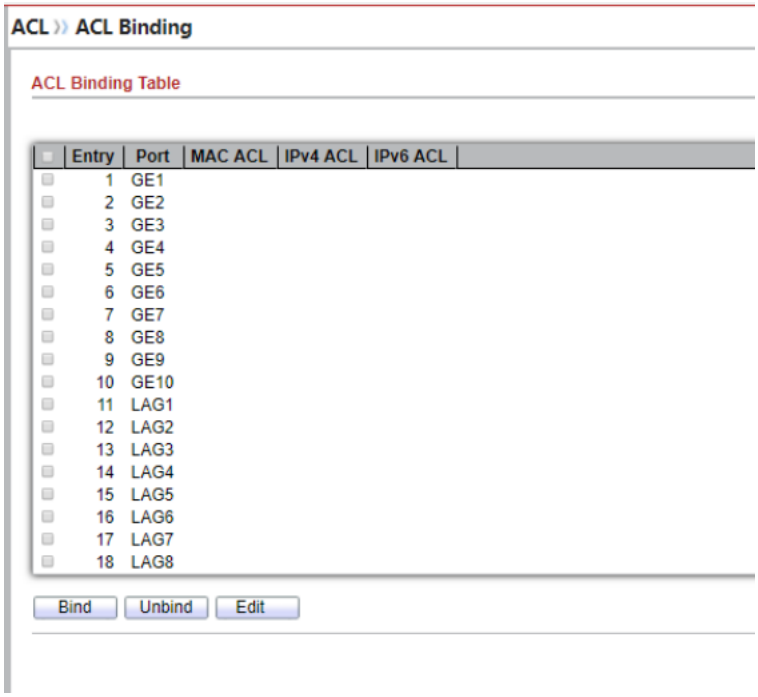
Field	Description
ACL Name	Displays the name of the IPv6 ACL to which this ACE is being added. This identifies the ACL context and cannot be changed when editing an existing ACE.
Sequence	Specifies the evaluation order of the ACE. Lower sequence numbers have higher priority and are processed first. Only available when adding a new ACE.
Action	Selects the action applied when a packet matches this ACE: • **Permit** – Forward packets that meet the ACE criteria. • **Deny** – Drop packets that meet the ACE criteria. • **Shutdown** – Drop

	matching packets and administratively disable the port that received them. The port can be reactivated from the Port Settings page.
Protocol	Selects the protocol type to match: • **Any (IP)** – Matches all IPv6-related protocols. • **Select from list** – Choose one of the following protocols: **TCP**, **UDP**, or **ICMP**. • **Protocol ID to match** – Enter a specific protocol number manually.
Source IP	Selects how the source IPv6 address is matched: • **Any** – Accepts all source IPv6 addresses. • **User Defined** – Matches only the specified IPv6 address or subnet. Enter the source IPv6 address and prefix length to define the match range.
Destination IP	Selects how the destination IPv6 address is matched: • **Any** – Accepts all destination IPv6 addresses. • **User Defined** – Matches only the specified IPv6 address or subnet. Enter the destination IPv6 address and prefix length to define the match range.
Source Port	Selects how the source port is matched. Only available when the protocol is **TCP** or **UDP**: • **Any** – Accepts all source ports. • **Single** – Matches a specific TCP/UDP source port. • **Range** – Matches a range of TCP/UDP source ports. Up to eight port ranges can be configured (shared between source and destination).
Destination Port	Selects how the destination port is matched. Only available when the protocol is **TCP** or **UDP**: • **Any** – Accepts all destination ports. • **Single** – Matches a specific TCP/UDP destination port. • **Range** – Matches a range of TCP/UDP destination ports. Uses the same shared range pool as Source Port.
TCP Flags	Selects one or more TCP flags to filter packets (e.g., SYN, ACK, FIN). Only available when the protocol is **TCP**. Filtering by TCP flags provides granular control over session behaviour and enhances security.
Type of Service	Selects the ToS (Type of Service) match criteria: • **Any** – Accepts all ToS values. • **DSCP to match** – Enter a specific DSCP value. • **IP Precedence to match** – Enter an IP Precedence value.
ICMP Type	Selects the ICMP message type. Only available when the protocol is **ICMP**: • **Any** – Accepts all ICMP types. • **Select from list** – Choose a message type by name. • **Protocol ID to match** – Enter the numeric ICMP type value.
ICMP Code	Selects the ICMP code. Only available when the protocol is **ICMP**: • **Any** – Accepts all ICMP codes. • **User Defined** – Enter a specific ICMP code to match.

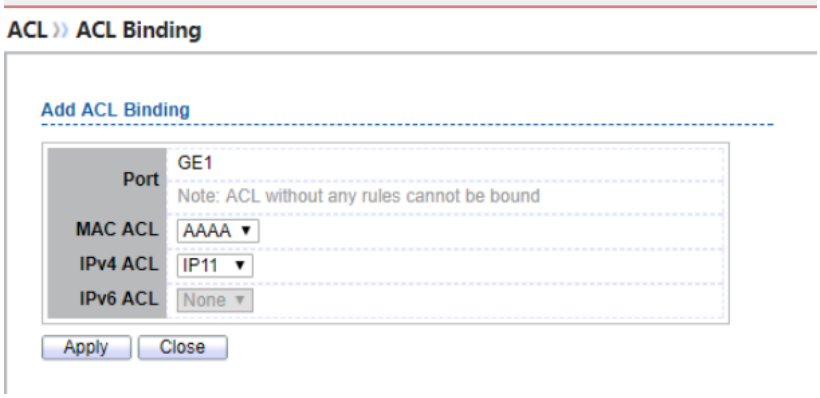
ACL BINDING

ACL Binding applies ACLs to interfaces or globally, determining where the ACL rules take effect.

Navigation: ACL → ACL Binding



Field	Description
Port	Displays the port entry ID. Each row represents a single interface where ACL bindings can be applied.
MAC ACL	Shows the name of the MAC ACL currently bound to the interface. If empty, no MAC-based filtering is applied on this port.
IPv4 ACL	Shows the name of the IPv4 ACL bound to the interface. If empty, the port has no IPv4 ACL rules applied.
IPv6 ACL	Shows the name of the IPv6 ACL bound to the interface. If empty, the port has no IPv6 ACL rules applied.



Field	Description
Port	Displays the port entry ID. This identifies the specific interface where ACL bindings can be applied. Each entry corresponds to a single physical port.
MAC ACL	Selects the MAC ACL to bind to the port. If no MAC ACL is selected, the port will not enforce any MAC-based filtering rules.
IPv4 ACL	Selects the IPv4 ACL to bind to the port. If left empty, the port will not apply any IPv4 ACL rules.
IPv6 ACL	Selects the IPv6 ACL to bind to the port. If left empty, the port will not apply any IPv6 ACL rules.

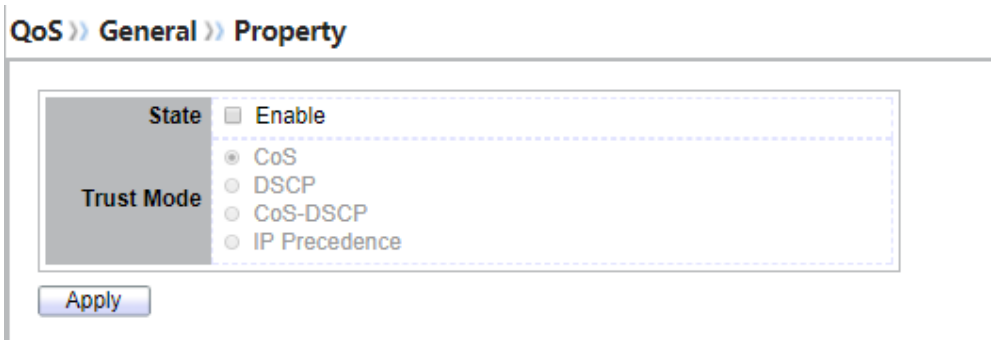
QUALITY OF SERVICE (QOS)

QoS allows you to classify, prioritise, and rate-limit traffic to ensure critical applications receive the bandwidth and latency they require. These pages allow you to configure queue scheduling, traffic classification, mapping tables, and ingress/egress rate limits.

QoS – General

Use this page to configure global QoS behaviour.
Navigation: QoS → General

PROPERTY



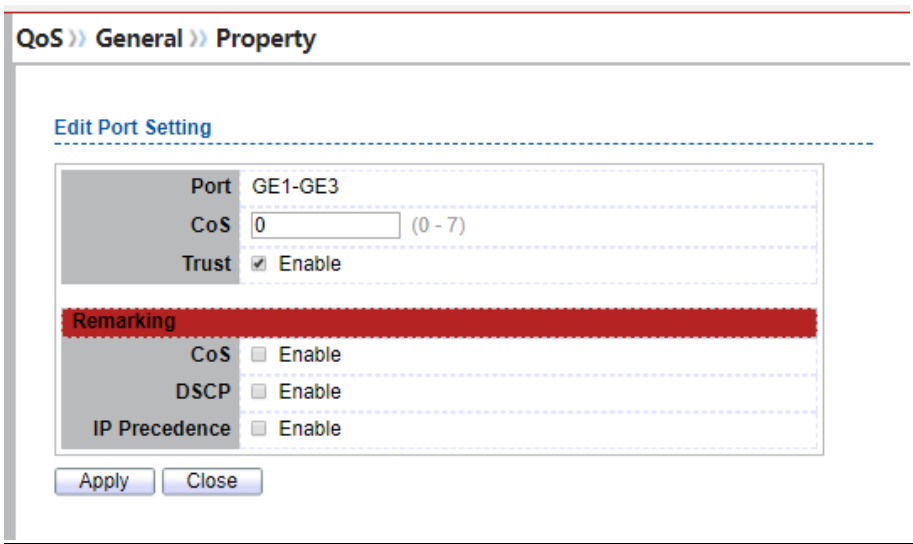
Field	Description
State	Sets the global QoS operating state. When enabled, the switch applies queue scheduling, traffic classification, and priority mapping according to the configured QoS rules. When disabled, all traffic is treated as best-effort with no prioritisation.
Trust Mode	Selects how the switch determines the priority of incoming traffic. The trust mode defines which packet header field is used to map traffic into internal queues: • **CoS** – Traffic is prioritised based on the 802.1p Class of Service value in the VLAN tag. If a packet has no VLAN tag, the port's default CoS value is used. CoS-to-queue mapping is configured per port. • **DSCP** – IP traffic is prioritised based on the DSCP value in the IP header. DSCP-to-queue mapping is configured on the DSCP Mapping page. Non-IP traffic is automatically placed into the best-effort queue. • **CoS-DSCP** – Non-IP traffic uses CoS classification, while IP traffic uses DSCP classification. This mode provides consistent behaviour across mixed traffic types. • **IP Precedence** – Traffic is prioritised based on the IP Precedence bits in the IPv4 header. IP Precedence-to-queue mapping is configured on the IP Precedence Mapping page.

Port Setting Table

Entry	Port	CoS	Trust	Remarking		
				CoS	DSCP	IP Precedence
1	GE1	0	Enabled	Disabled	Disabled	Disabled
2	GE2	0	Enabled	Disabled	Disabled	Disabled
3	GE3	0	Enabled	Disabled	Disabled	Disabled
4	GE4	0	Enabled	Disabled	Disabled	Disabled
5	GE5	0	Enabled	Disabled	Disabled	Disabled
6	GE6	0	Enabled	Disabled	Disabled	Disabled
7	GE7	0	Enabled	Disabled	Disabled	Disabled
8	GE8	0	Enabled	Disabled	Disabled	Disabled
9	GE9	0	Enabled	Disabled	Disabled	Disabled
10	GE10	0	Enabled	Disabled	Disabled	Disabled
11	LAG1	0	Enabled	Disabled	Disabled	Disabled
12	LAG2	0	Enabled	Disabled	Disabled	Disabled
13	LAG3	0	Enabled	Disabled	Disabled	Disabled
14	LAG4	0	Enabled	Disabled	Disabled	Disabled
15	LAG5	0	Enabled	Disabled	Disabled	Disabled
16	LAG6	0	Enabled	Disabled	Disabled	Disabled
17	LAG7	0	Enabled	Disabled	Disabled	Disabled
18	LAG8	0	Enabled	Disabled	Disabled	Disabled

Edit

Field	Description
Port	Port name. Identifies the physical interface where QoS behaviour is configured.
CoS	Port default CoS (Class of Service) priority value. Used when incoming packets have no VLAN tag; determines how untagged traffic is classified into internal queues.
Trust	Port trust state: • **Enabled** – The port follows the global QoS trust mode (CoS, DSCP, CoS-DSCP, or IP Precedence). Incoming packets are classified according to global settings. • **Disabled** – The port ignores global trust mode and treats all traffic as best-effort, regardless of packet markings.
Remarking (CoS)	Port CoS remarking admin state: • **Enabled** – The switch may rewrite the CoS value of outgoing packets based on QoS policies. • **Disabled** – CoS values are transmitted unchanged.
Remarking (DSCP)	Port DSCP remarking admin state: • **Enabled** – DSCP values in outgoing IP packets may be rewritten according to QoS rules. • **Disabled** – DSCP values are preserved and not altered.
Remarking (IP Precedence)	Port IP Precedence remarking admin state: • **Enable** – IP Precedence bits in outgoing IPv4 packets may be rewritten. • **Disable** – IP Precedence values are transmitted unchanged.

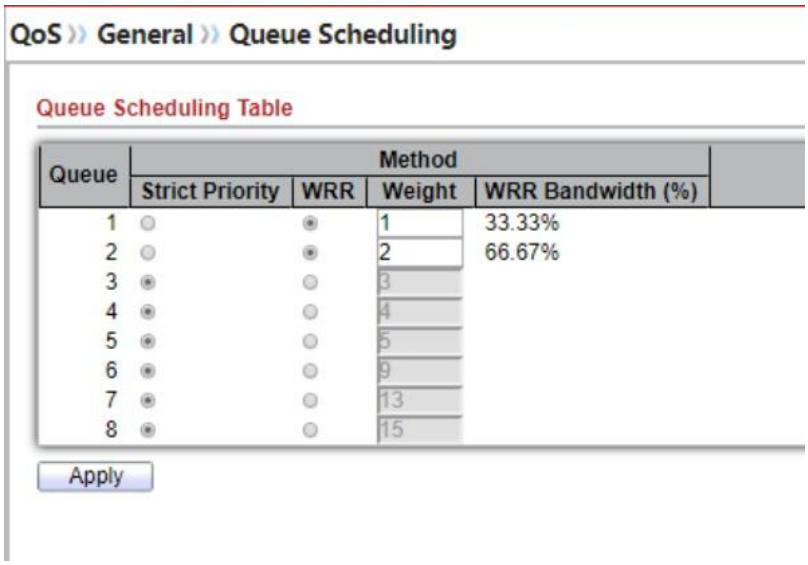


Field	Description
Port	Select the port or list of ports to apply QoS settings to. Each entry corresponds to a physical interface.
CoS	Sets the default CoS (802.1p) priority value for the selected ports. This value is used when incoming packets do not contain a VLAN tag with a priority field.
Trust	Sets the port trust state: • **Enabled** – The port follows the global QoS trust mode (CoS, DSCP, CoS-DSCP, or IP Precedence). • **Disabled** – The port ignores global trust mode and treats all traffic as best-effort.
Remarking (CoS)	Sets whether the port rewrites the CoS value on outgoing packets: • **Enabled** – CoS remarking is allowed. • **Disabled** – CoS values are transmitted unchanged.
Remarking (DSCP)	Sets whether the port rewrites the DSCP value on outgoing IP packets: • **Enabled** – DSCP remarking is allowed. • **Disabled** – DSCP values are preserved.
Remarking (IP Precedence)	Sets whether the port rewrites the IP Precedence bits on outgoing IPv4 packets: • **Enable** – IP Precedence remarking is allowed. • **Disable** – IP Precedence values are transmitted unchanged.

QUEUE SCHEDULING

Queue scheduling determines how packets are dequeued from egress queues.

Navigation: QoS → Queue Scheduling

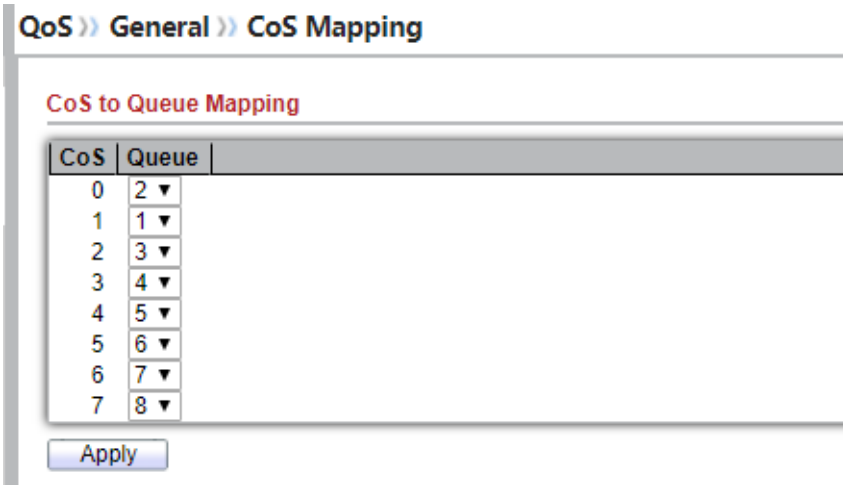


Field	Description
Queue	Queue ID to configure.
Strict Priority	Sets the queue to Strict Priority (SP). SP queues are serviced first, starting from the highest priority queue.
WRR	Sets the queue to Weighted Round Robin (WRR). WRR queues are serviced proportionally based on their configured weight.
Weight	WRR weight assigned to the queue. Higher weights allow more frames to be transmitted per WRR cycle.
WRR Bandwidth	Percentage of bandwidth allocated to the WRR queue.

COS MAPPING

CoS mapping allows incoming 802.1p priority values to be mapped to internal queue priorities.

Navigation: QoS → CoS Mapping



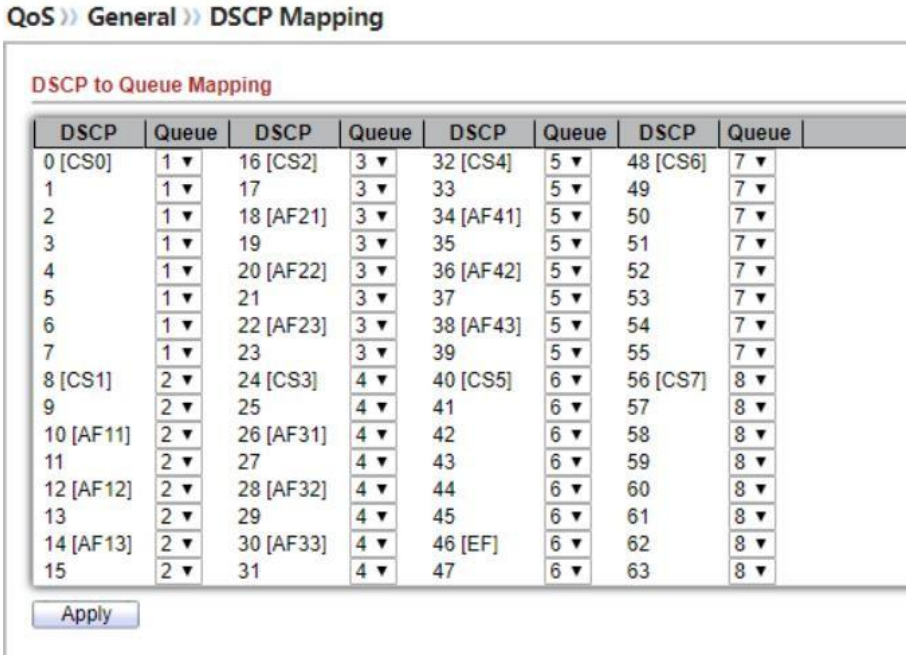
Field	Description
CoS	Incoming 802.1p CoS value (0–7).
Queue	Queue ID assigned to this CoS value.

Field	Description
Queue	Queue ID.
CoS	CoS value to remark for traffic leaving this queue.

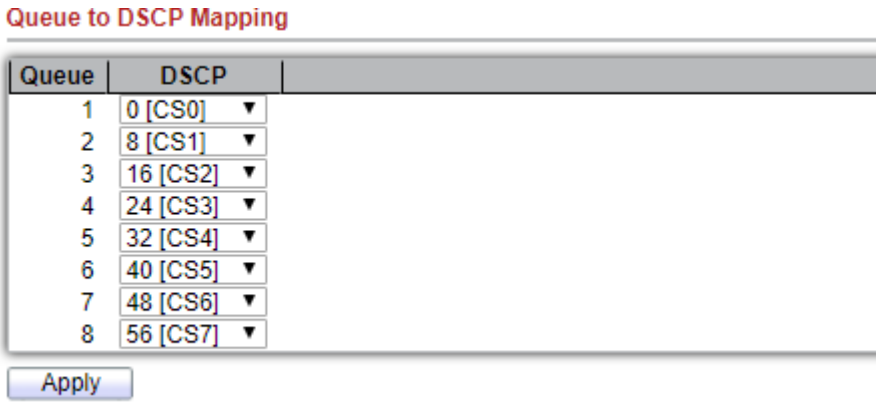
DSCP MAPPING

DSCP mapping allows incoming DSCP values to be mapped to internal queue priorities.

Navigation: QoS → DSCP Mapping



Field	Description
DSCP Value	Specifies the Differentiated Services Code Point value used to classify incoming IP traffic.
Queue	Selects the egress queue to which traffic with the specified classification value is assigned.

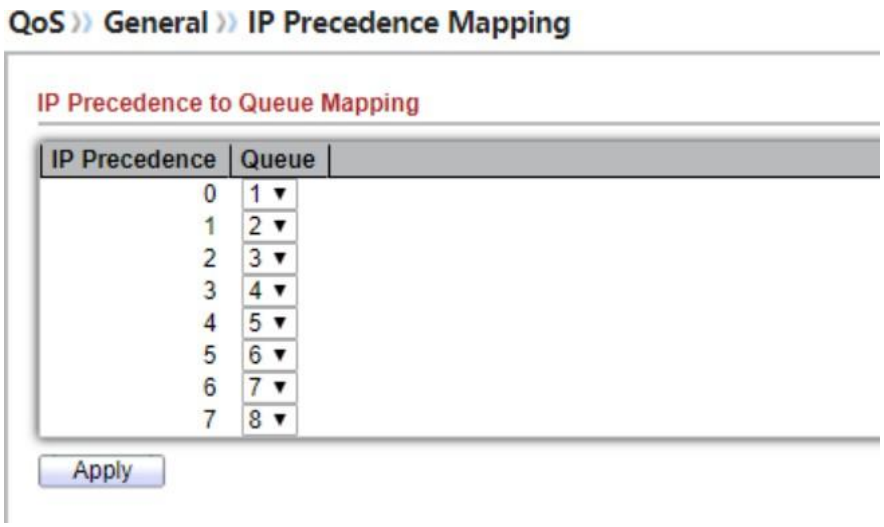


Field	Description
Queue	Queue ID. Identifies the egress queue whose DSCP remarking value is being configured.
DSCP	Select the DSCP value to remark for traffic leaving this queue. This value overwrites the packet's original DSCP marking on egress.

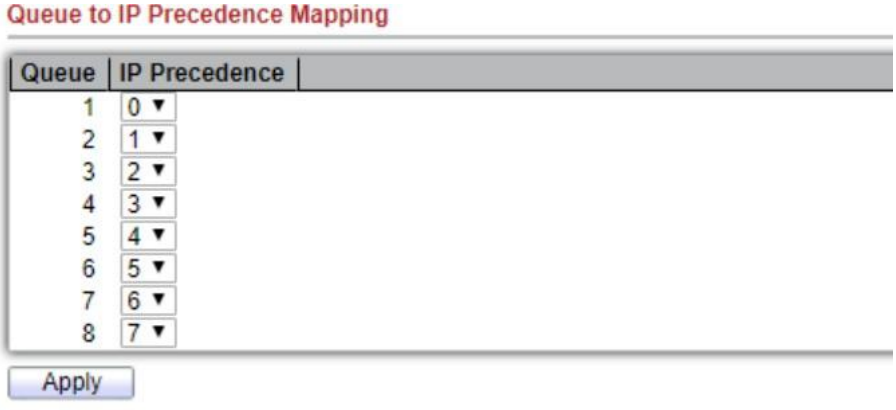
IP PRECEDENCE MAPPING

IP Precedence mapping allows IPv4 precedence bits to be mapped to internal queue priorities.

Navigation: QoS → IP Precedence Mapping



Field	Description
IP Precedence	Specifies the three-bit IP precedence value used to classify incoming IPv4 traffic.
Queue	Selects the egress queue to which traffic with the specified classification value is assigned.



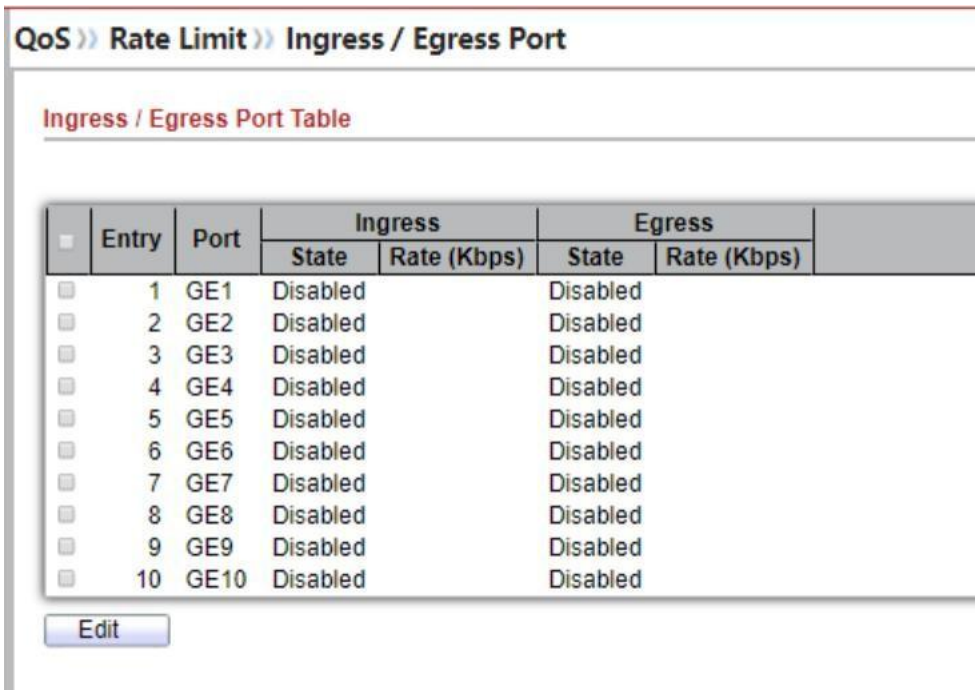
Field	Description
Queue	Selects the egress queue to which traffic with the specified classification value is assigned.
IP Precedence	Specifies the three-bit IP precedence value used to classify incoming IPv4 traffic.

Rate Limit

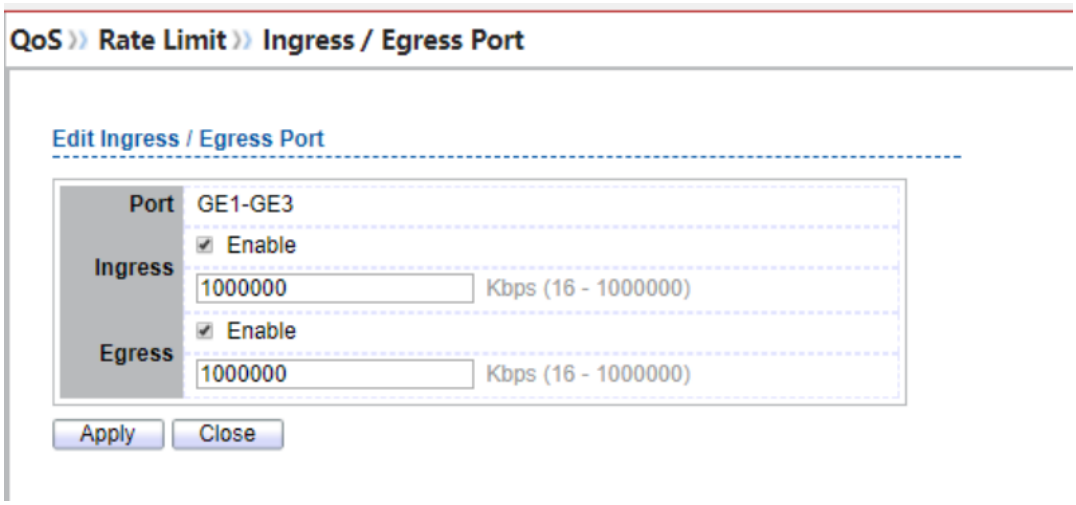
Rate limiting allows you to control ingress and egress bandwidth per port or per queue.
Navigation: QoS → Rate Limit

INGRESS / EGRESS PORT RATE LIMIT

Use this page to configure rate limits for traffic entering or leaving a port.



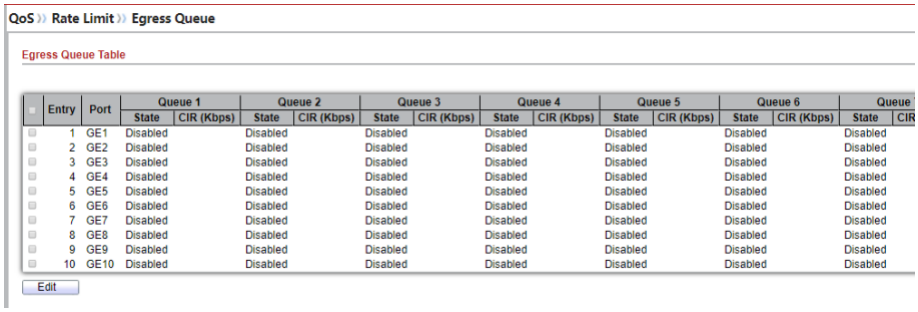
Field	Description
Port	Identifies the physical interface to which the rate limit applies.
Ingress Rate	Sets the maximum inbound traffic rate permitted on the selected port.
Egress Rate	Maximum allowed egress bandwidth.
Burst Size	Maximum burst size allowed.



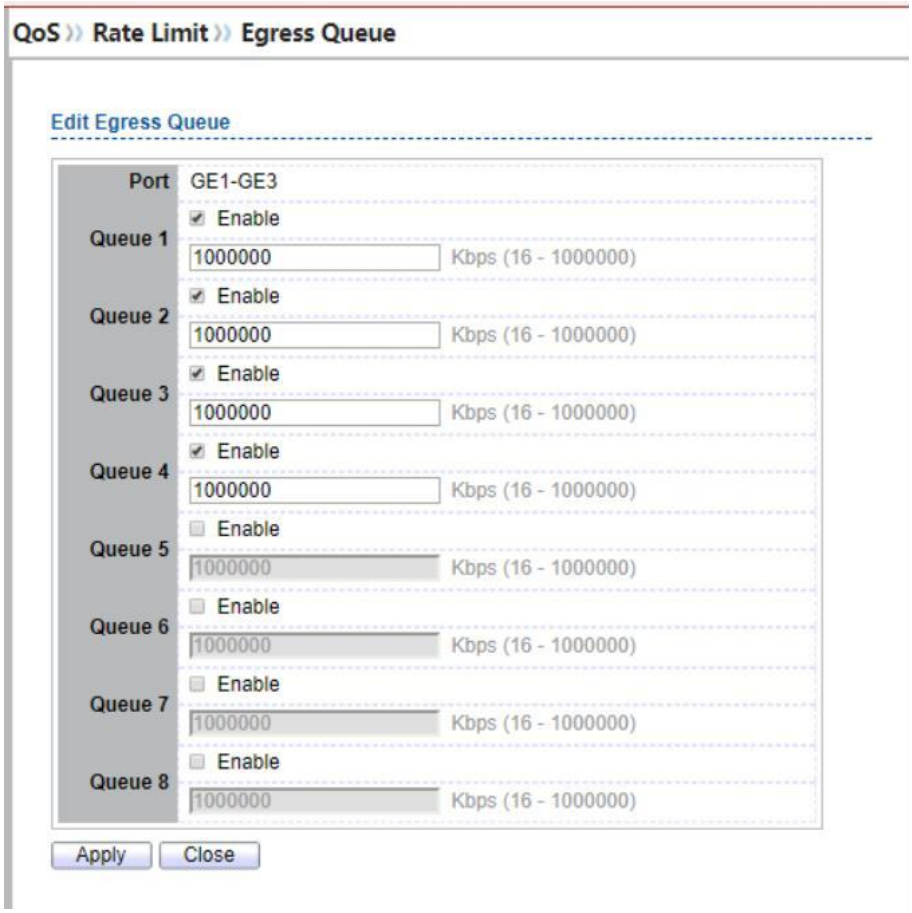
Field	Description
Port	Selected port.
Ingress Rate	Configurable ingress bandwidth limit.
Egress Rate	Configurable egress bandwidth limit.
Burst Size	Optional burst size configuration.

EGRESS QUEUE RATE LIMIT

Use this page to configure rate limits for individual egress queues.



Field	Description
Port	Port name.
Queue	Queue index.
Rate	Maximum allowed bandwidth for the queue.
Burst Size	Maximum burst size allowed.



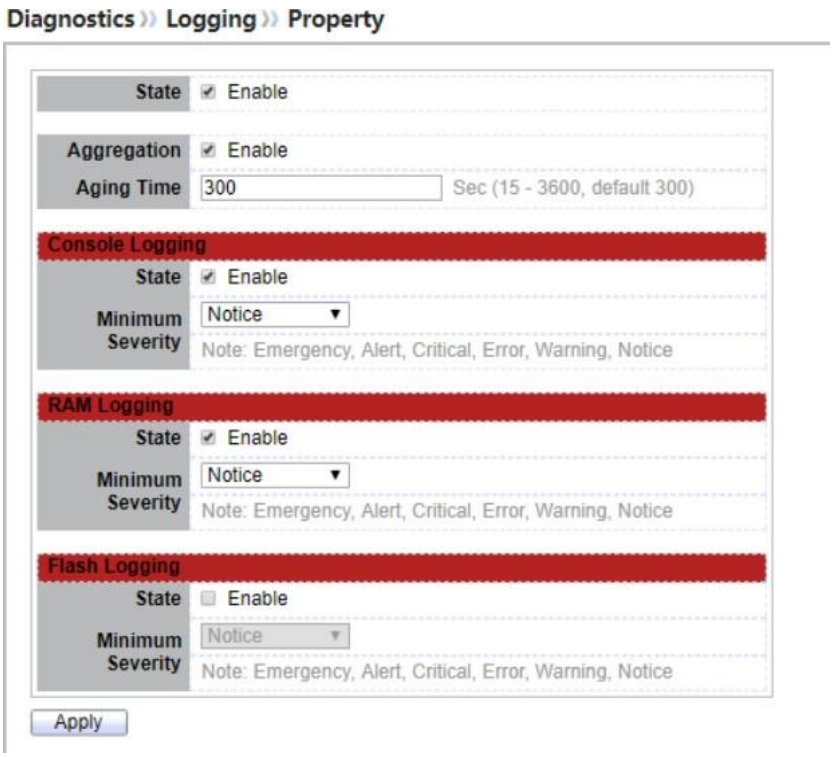
Field	Description
Port	Selected port.
Queue	Selected queue.
Rate	Configurable queue bandwidth limit.
Burst Size	Optional burst size configuration.

DIAGNOSTICS

The Diagnostics pages provide tools for monitoring, testing, and troubleshooting switch operation. These functions help verify connectivity, inspect packet behaviour, test copper and fibre interfaces, and analyse protocol activity.

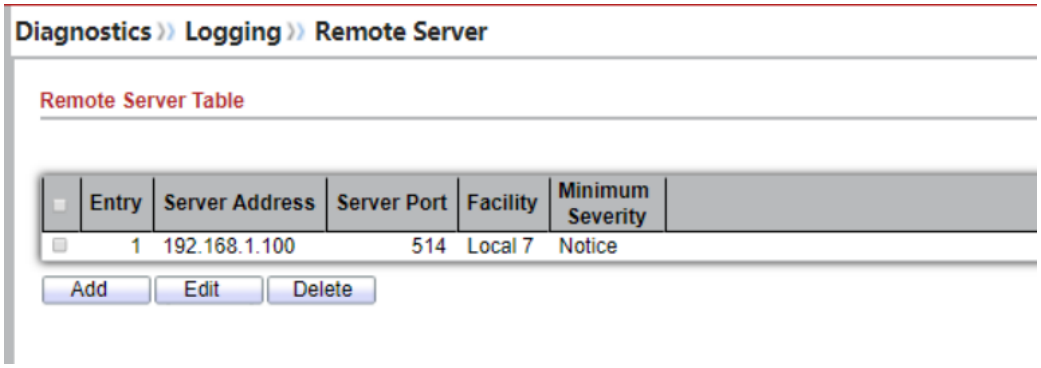
LOGGING

Use this page to configure remote logging servers and manage system log behaviour.
Navigation: Diagnostics → Logging → Property



Field	Description
State	Enables or disables remote logging.
Server Address	IPv4 address of the syslog server.
Server Port	UDP port used for syslog messages (default 514).
Facility	Syslog facility code used for classification.
Severity	Minimum severity level sent to the server.

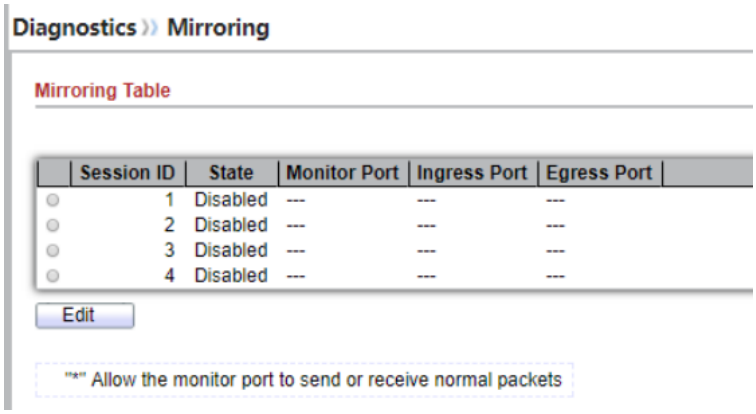
REMOVE SERVER



Field	Description
Server Address	The IP address of the remote logging server. This is the destination where syslog messages will be sent.
Server Ports	The UDP port number used by the remote logging server. Typically port **514**, unless a custom port is configured.
Facility	The syslog facility assigned to outgoing log messages. Supported values include: **local0**, **local1**, **local2**, **local3**, **local4**, **local5**, **local6**, **local7**. Facilities allow external systems to classify logs by source or purpose.
Severity	The minimum severity level of messages sent to the remote server. Only messages at or above this level are transmitted. Severity levels include: • **Emergency** – System is unusable. • **Alert** – Immediate action required. • **Critical** – Critical system condition. • **Error** – Error condition detected. • **Warning** – Warning condition. • **Notice** – Normal operation, but noteworthy event. • **Informational** – General device information. • **Debug** – Detailed diagnostic information.

MIRRORING

Port mirroring allows traffic from one or more ports to be copied to a destination port for analysis.
Navigation: Diagnostics → Mirroring

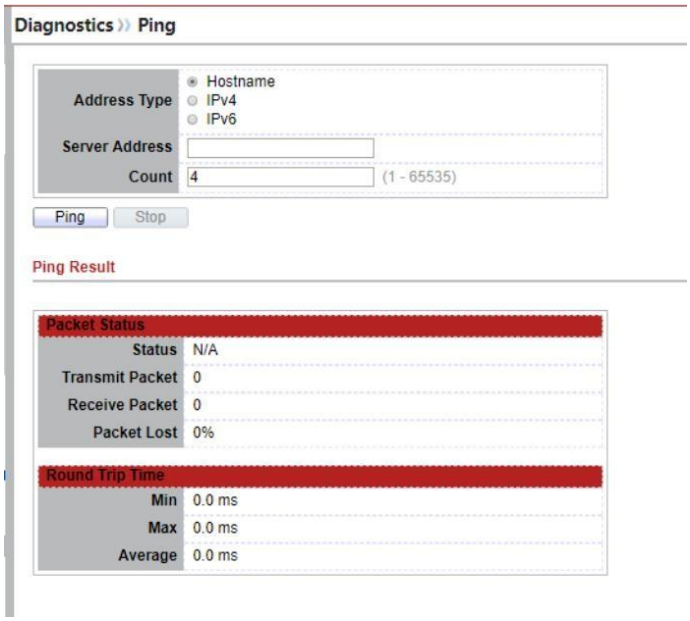


Field	Description
Session ID	Select the mirror session ID. Each session defines a unique mirroring configuration applied to the switch.
State	Select the mirror session state. • **Enabled** – Activates port-based mirroring for the session. • **Disabled** – Disables the mirror session.
Monitor Port	Select the destination (monitor) port that receives mirrored traffic. You may also specify whether the monitor port is allowed to send or receive normal network traffic while mirroring is active.
Ingress Port	Select the source **RX** ports whose inbound traffic will be mirrored to the monitor port.
Egress Port	Select the source **TX** ports whose outbound traffic will be mirrored to the monitor port.

PING

Ping sends ICMP Echo Requests to test network reachability.

Navigation: Diagnostics → Ping

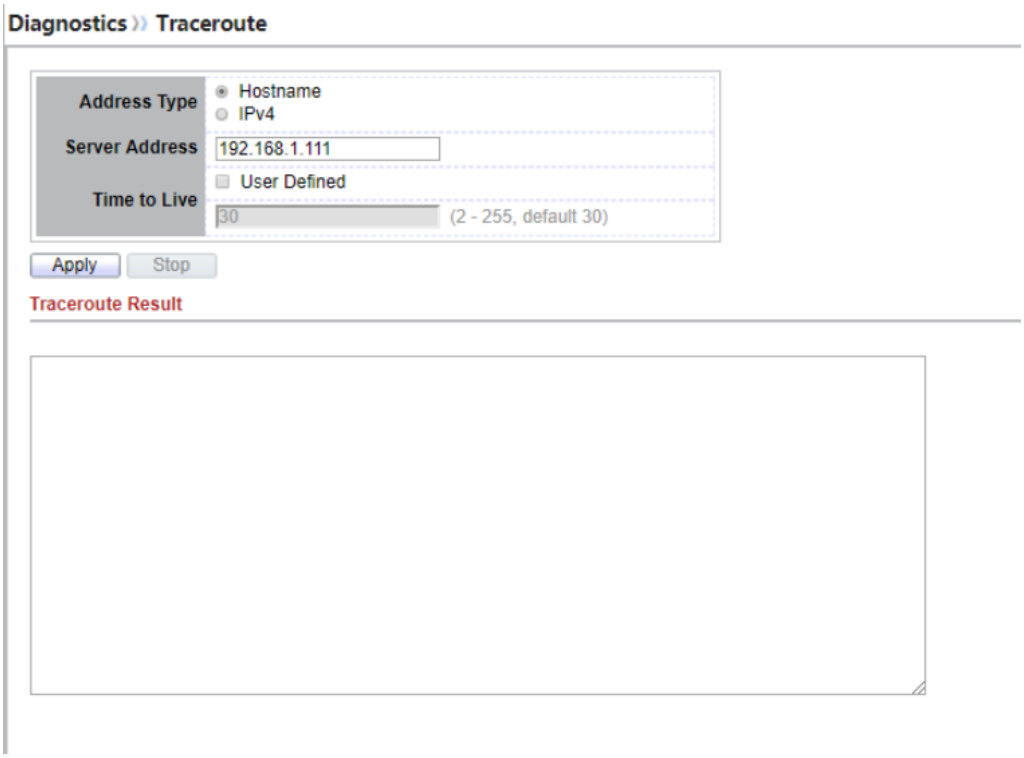


Field	Description
Address Type	Specifies the type of address used for the ping request. Options include **Hostname**, **IPv4**, or **IPv6**. This determines how the destination is interpreted and resolved.
Server Address	The actual destination to ping. Enter a valid Hostname, IPv4 address, or IPv6 address depending on the selected Address Type.
Count	Specifies the number of ICMP Echo Requests to send. Higher values provide more detailed reachability and latency information.

TRACEROUTE

Traceroute identifies the path packets take to a destination.

Navigation: Diagnostics → Traceroute

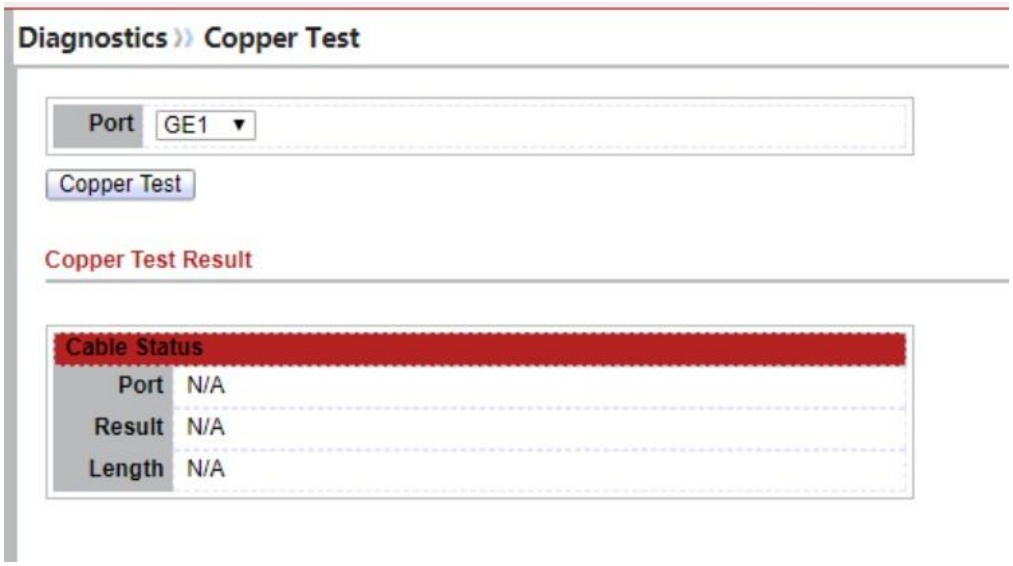


Field	Description
Address Type	Specifies the type of destination address used for the traceroute operation. Options include **Hostname** or **IPv4**, determining how the target is resolved.
Server Address	The actual destination to trace. Enter a valid Hostname or IPv4 address depending on the selected Address Type.
Time to Live	Specifies the maximum number of hops (TTL) the traceroute will probe. This defines how far the trace will attempt to reach through intermediate network devices.

COPPER TEST

Copper Test diagnoses physical issues on copper Ethernet ports.

Navigation: Diagnostics → Copper Test

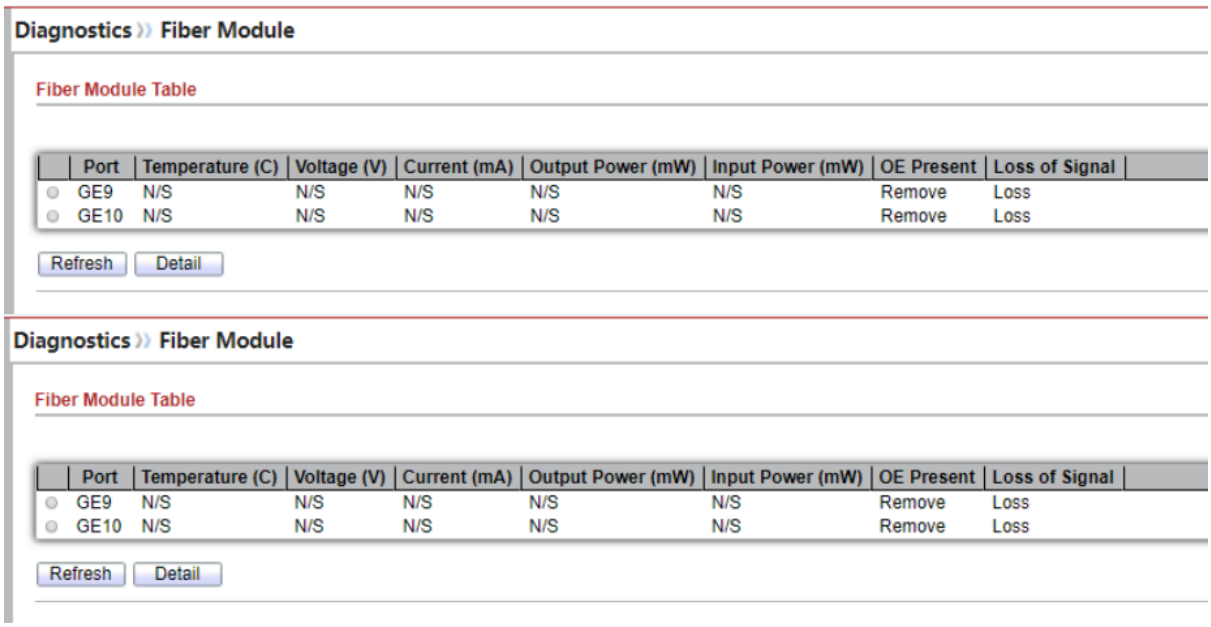


Field	Description
Port	Specify the interface on which the copper test will be performed. The selected port is used to measure cable status, detect faults, and estimate cable length conditions.
Port	The interface on which the copper test was performed. Identifies the physical port used for cable diagnostics.
Result	The outcome of the copper test. Possible results include: • **OK** – Cable pair is correctly terminated and functioning normally. • **Short Cable** – Cable pair is shorted. • **Open Cable** – Cable pair is open; no link partner detected. • **Impedance Mismatch** – Terminating impedance is outside the acceptable reference range. • **Line Drive** – Indicates abnormal electrical characteristics detected on the line.
Length	The estimated distance (in meters) from the port to the location on the cable where the fault was detected. Useful for pinpointing physical cable issues.

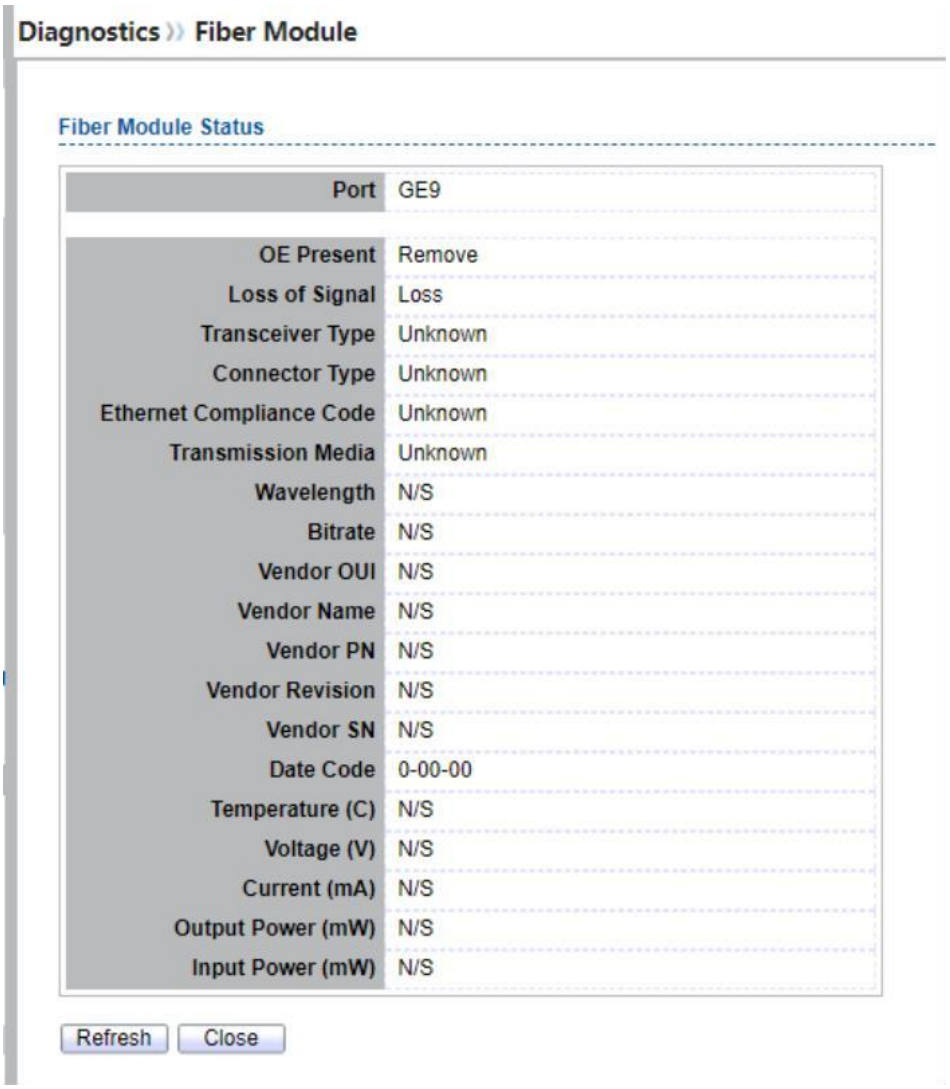
FIBER MODULE

Displays diagnostic information for installed SFP/SFP+ modules.

Navigation: Diagnostics → Fiber Module



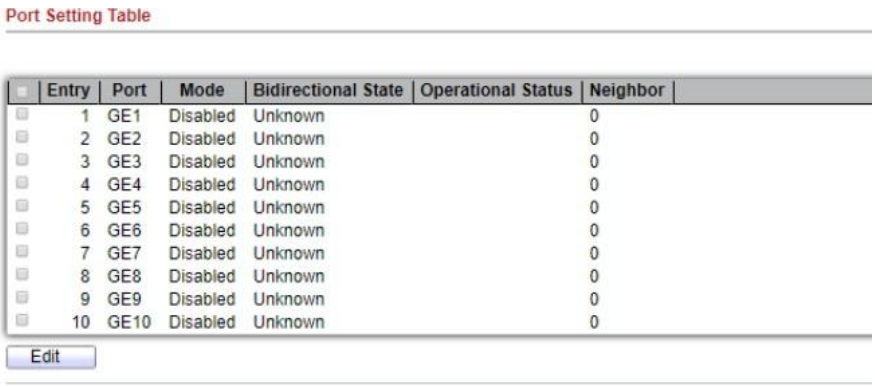
Field	Description
Port	Interface or port number where the SFP/SFP+ module is installed. Identifies the transceiver being monitored.
Temperature	Internally measured transceiver temperature. Useful for detecting overheating or abnormal thermal conditions.
Voltage	Internally measured supply voltage delivered to the module. Helps verify stable power conditions.
Current	Measured TX bias current. Indicates the electrical drive level of the transmitter laser.
Output Power	Measured TX optical output power (in milliwatts). Shows the strength of the transmitted optical signal.
Input Power	Measured RX optical input power (in milliwatts). Indicates the received optical signal level from the link partner.
Transmitter Fault	Displays the current TX fault state. Indicates whether the transmitter is reporting an error condition.
OE Present	Indicates that the transceiver has powered up successfully and is ready for data transmission.
Loss of Signal	Shows whether the module is currently detecting a loss of optical signal on the receive side.
Refresh	Refreshes the page to update all diagnostic readings.
Detail	Displays detailed diagnostic information for the selected port, including extended SFF-8472 parameters when supported.


Diagnostics ›› Fiber Module
Fiber Module Status
Port GE9
OE Present Remove
Loss of Signal Loss
Transceiver Type Unknown
Connector Type Unknown
Ethernet Compliance Code Unknown
Transmission Media Unknown
Wavelength N/S
Bitrate N/S
Vendor OUI N/S
Vendor Name N/S
Vendor PN N/S
Vendor Revision N/S
Vendor SN N/S
Date Code 0-00-00
Temperature (C) N/S
Voltage (V) N/S
Current (mA) N/S
Output Power (mW) N/S
Input Power (mW) N/S
Refresh
Close

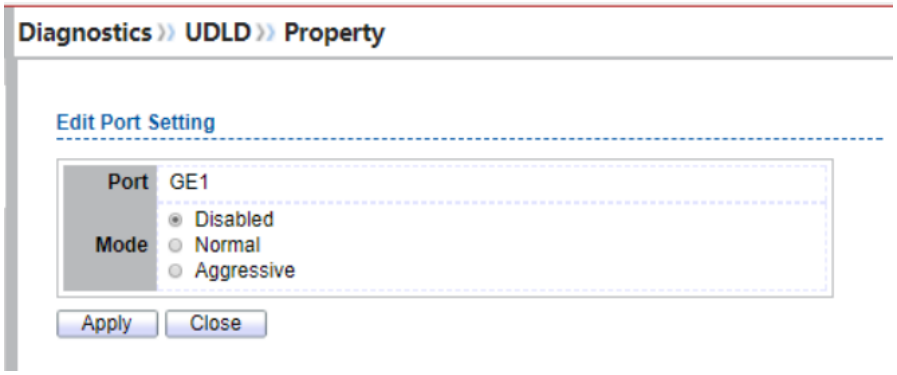
UDLD (Unidirectional Link Detection)

UDLD detects unidirectional link failures that can cause network loops.

Navigation: Diagnostics → UDLD → Property

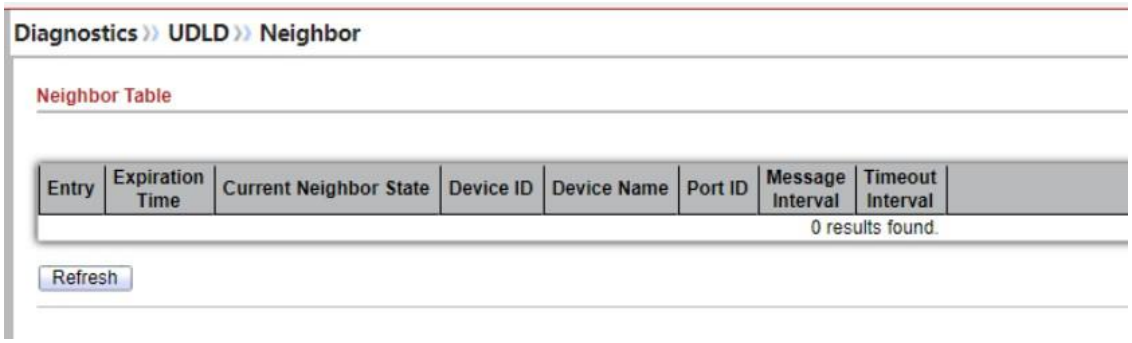


Field	Description
Port	Displays the port ID for this UDLD entry. Identifies the interface being monitored for UDLD status.
Mode	Displays the UDLD running mode configured on the interface. Modes include **Disabled**, **Normal**, or **Aggressive**, determining how the port reacts when neighbour information ages out.
Bidirectional State	Shows the current bidirectional link state of the interface. Indicates whether UDLD has confirmed two-way communication with the neighbour.
Operational Status	Displays the operational status of UDLD on the interface, reflecting whether the UDLD process is functioning normally or has detected a fault.
Neighbour	Displays the number of UDLD neighbours detected on the interface. Useful for verifying correct link partner detection.



Field	Description
Port	Displays the selected port being edited. Identifies the interface for which UDLD settings are being modified.
Mode	Select the UDLD running mode for the interface. Options include: • **Disabled** – UDLD is turned off on this interface.

	• **Normal** – Standard UDLD behavior. The port transitions to the ***Link Up One*** phase after the last neighbor ages out. • **Aggressive** – Enhanced UDLD behavior. The port transitions to the ***Re-Establish*** phase after the last neighbor ages out, providing faster detection and recovery from unidirectional link failures.



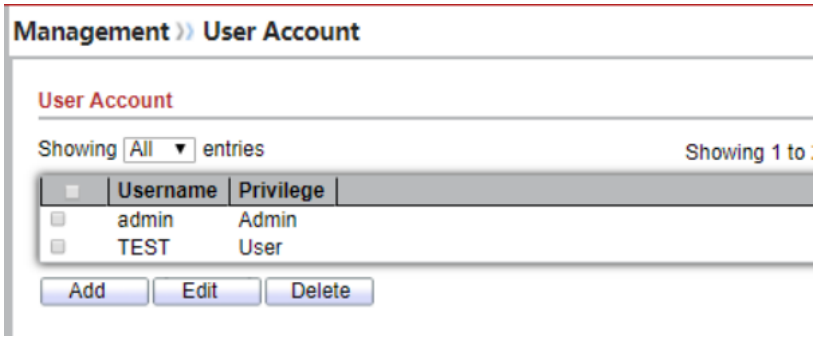
Field	Description
Entry	Displays the neighbor entry index. Each entry represents a detected UDLD neighbor associated with the interface.
Expiration Time	Shows the remaining time before the neighbor information ages out. When this timer expires, UDLD considers the neighbor unreachable unless refreshed.
Current Neighbor State	Displays the current operational state of the neighbor (e.g., active, aged, or unreachable). Indicates the health of the UDLD relationship.
Device ID	Displays the unique device ID of the detected neighbor. Helps identify the remote switch or device participating in UDLD.
Device Name	Displays the neighbor's device name, providing a human-readable identifier for easier management.
Port ID	Displays the port ID on the neighbor device that is connected to the local interface. Useful for verifying correct physical connectivity.
Message Interval	Shows the interval at which the neighbor sends UDLD messages. Helps confirm synchronization and expected message frequency.
Timeout Interval	Displays the timeout interval for the neighbor. If no UDLD messages are received within this period, the neighbor is considered lost.

MANAGEMENT

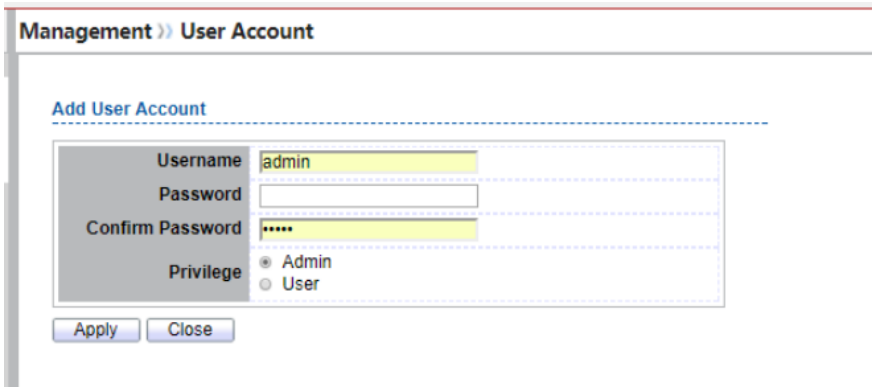
The Management pages allow you to configure system firmware, user accounts, configuration files, SNMP parameters, and RMON monitoring. These functions ensure the switch can be administered securely, updated reliably, and monitored effectively.

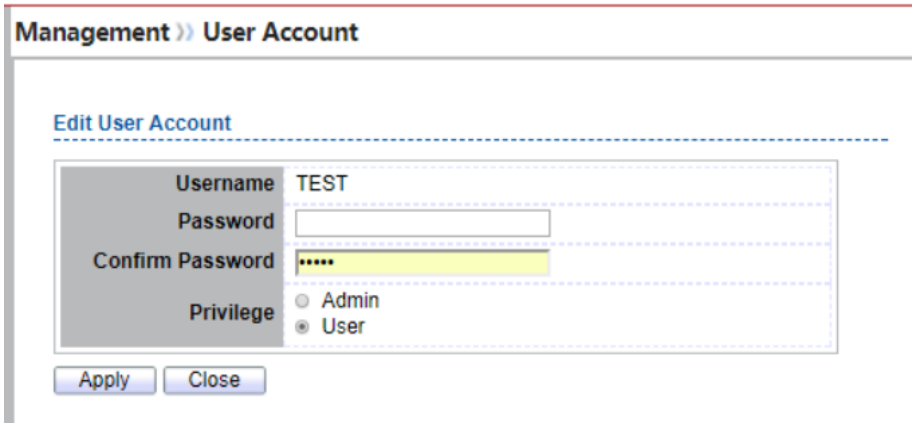
USER ACCOUNTS

Use this page to manage local user accounts for switch access.
Navigation: Management → User Account



Field	Description
Username	User name of the account. Identifies the local management user configured on the switch.
Privilege	Select the privilege level for the account. • **Admin** – Full access to all switch settings. Privilege value = **15**. • **User** – Read-only access. Can view settings but cannot modify them. Privilege value = **1**.

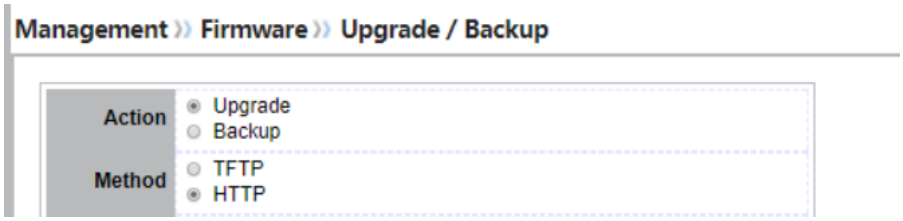




Field	Description
sername	User name of the account. Identifies the management user being created or modified.
Password	Set the password for the account. This defines the authentication credential used during login.
Confirm Password	Re-enter the same password as in the **Password** field to ensure accuracy and prevent configuration errors.
Privilege	Select the privilege level for the account. • **Admin** – Full access to all switch settings. Privilege value = **15**. • **User** – Read-only access. Can view settings but cannot modify them. Privilege value = **1**.

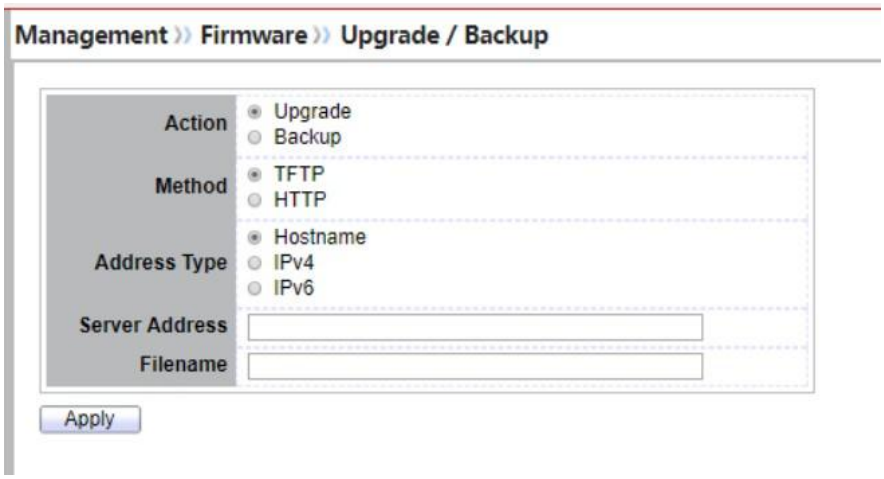
FIRMWARE

Use this page to upgrade firmware, back up firmware images, and manage active firmware versions.
Navigation: Management → Firmware → Upgrade / Backup



Field	Description
Action	Firmware operation to perform. Options include: • **Upgrade** – Upload a new firmware image from a remote host to the device under test (DUT). • **Backup** – Download (backup) the current firmware image from the DUT to a remote host.
Method	Select the method used for firmware upgrade or backup. Options include:

	• **TFTP** – Uses a TFTP server for transferring firmware images. • **HTTP** – Uses a web browser to upload firmware directly from the local PC.
Filename	When using the **HTTP** method, select the firmware image file stored on your local PC. This is the file that will be uploaded to the device.

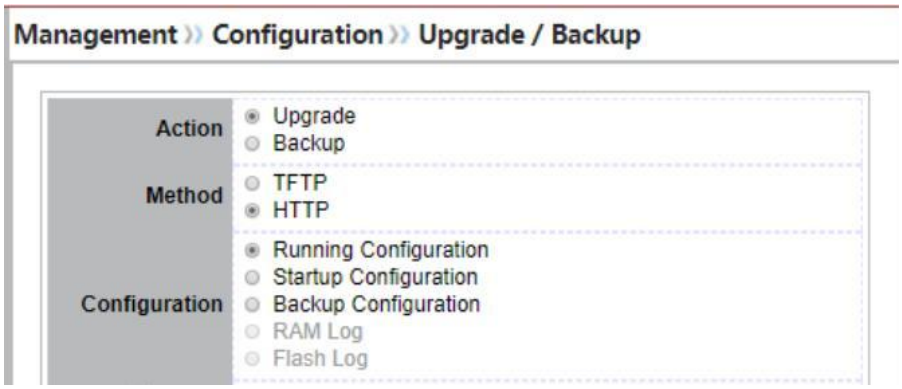


Displays information about the currently running firmware.

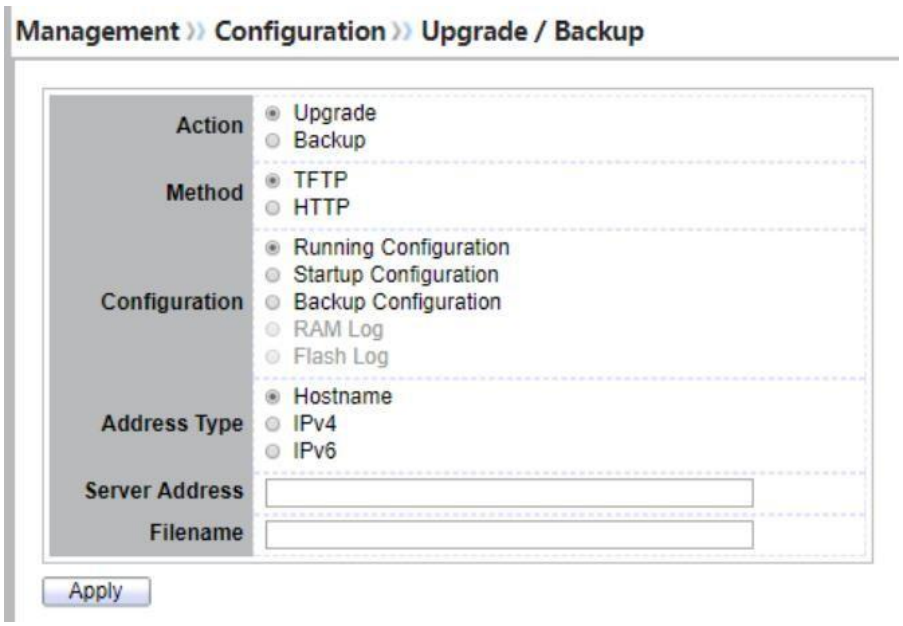
Field	Description
Action	Select the firmware operation to perform. Options include: • **Upgrade** – Upload a new firmware image from a remote host to the device under test (DUT). • **Backup** – Download (backup) the current firmware image from the DUT to a remote host.
Method	Select the transfer method used for firmware upgrade or backup. Options include: • **TFTP** – Uses a TFTP server to transfer firmware images. • **HTTP** – Uses a web browser to upload firmware directly from the local PC. ***(Note: This field appears again because TFTP-specific fields only apply when TFTP is selected.)***
Address Type	Specify the address type for the TFTP server. Options include: • **Hostname** – Use a domain name as the server address. • **IPv4** – Use an IPv4 address. • **IPv6** – Use an IPv6 address.
Server Address	Specify the TFTP server address. Enter a valid Hostname, IPv4, or IPv6 address depending on the selected Address Type.
Filename	The firmware image file name stored on the remote TFTP server. This is the file that will be downloaded (upgrade) or uploaded (backup) via TFTP.

Configuration

Use this page to manage configuration files, including backup, restore, and saving to flash.
Navigation: Management → Configuration → Upgrade / Backup



Field	Description
Action	Select the firmware operation to perform. Options include: • **Upgrade** – Upload a new firmware image from a remote host to the device under test (DUT). • **Backup** – Download (backup) the current firmware image from the DUT to a remote host.
Method	Select the transfer method used for firmware upgrade or backup. Options include: • **TFTP** – Uses a TFTP server to transfer firmware images. • **HTTP** – Uses a web browser to upload firmware directly from the local PC.
Configuration	Select the configuration type to apply during upgrade: • **Running Configuration** – Merge the uploaded configuration into the current running configuration. • **Startup Configuration** – Replace the startup configuration file stored in flash. • **Backup Configuration** – Replace the backup configuration file stored on the device.
Filename	When using the **HTTP** method, select the configuration file stored on your local PC. This is the file that will be uploaded to the device.

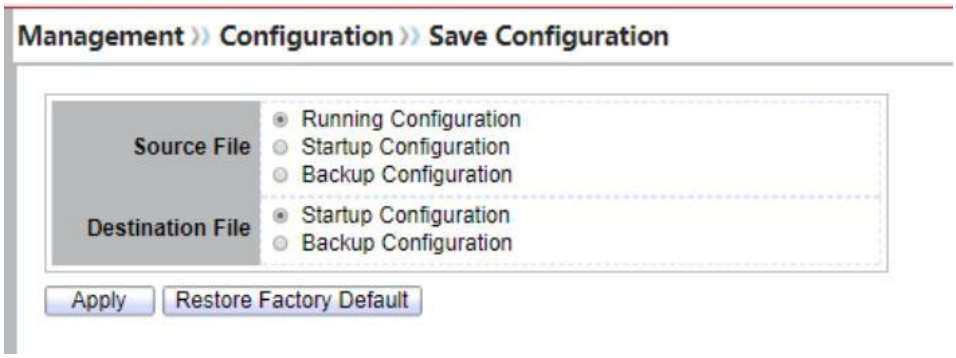


Field	Description
Action	Select the firmware operation to perform. Options include: • **Upgrade** – Upload a new firmware image from a remote host to the device under test (DUT). • **Backup** – Download (backup) the current firmware image from the DUT to a remote host.
Method	Select the transfer method used for firmware upgrade or backup. Options include: • **TFTP** – Uses a TFTP server to transfer firmware images. • **HTTP** – Uses a web browser to upload firmware directly from the local PC.
Configuration	Select the configuration type to apply during upgrade: • **Running Configuration** – Merge the uploaded configuration into the current running configuration. • **Startup Configuration** – Replace the startup configuration file stored in flash. • **Backup Configuration** – Replace the backup configuration file stored on the device.
Address Type	Specify the address type for the TFTP server. Options include: • **Hostname** – Use a domain name as the server address. • **IPv4** – Use an IPv4 address. **IPv6** – Use an IPv6 address.
Server Address	Specify the TFTP server address. Enter a valid Hostname, IPv4, or IPv6 address depending on the selected Address Type.
Filename	The firmware image file name stored on the remote TFTP server. This is the file that will be downloaded (upgrade) or uploaded (backup) via TFTP.

SAVE CONFIGURATION

To display the **Save Configuration** page, navigate to: **Management → Configuration → Save Configuration**

This page allows the user to manage configuration files stored on the device. You can save the current running configuration, review stored configuration files, and use the **Restore Factory Default** function to reset the device to its factory settings.

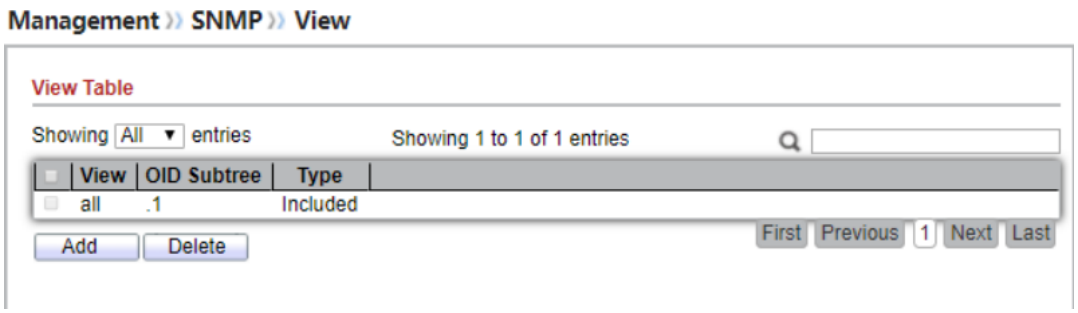


Field	Description
Source File	Select the source configuration file to copy. Options include: • **Running Configuration** – Copy the current running configuration to the selected destination. • **Startup Configuration** – Copy the startup configuration file to the selected destination. • **Backup Configuration** – Copy the backup configuration file to the selected destination.
Destination File	Select the destination configuration file. Options include: • **Startup Configuration** – Save the copied file as the startup configuration. • **Backup Configuration** – Save the copied file as the backup configuration.

SNMP

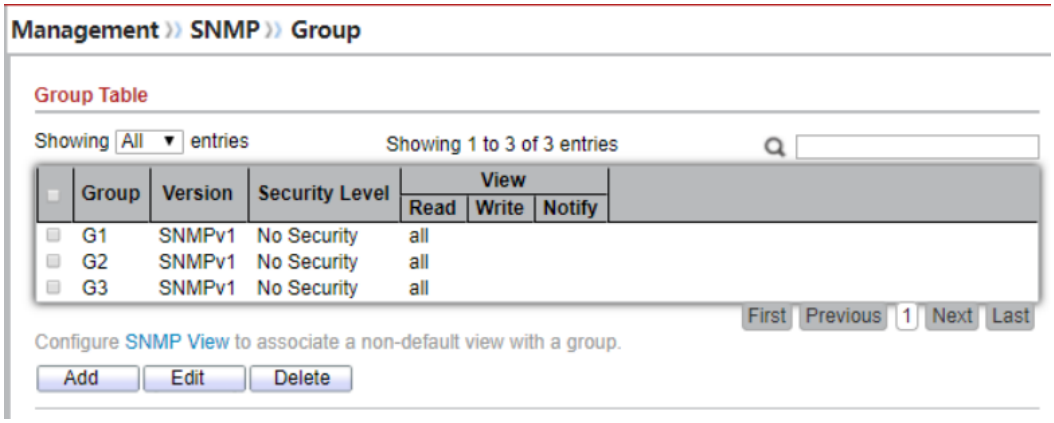
Use this page to configure SNMP parameters, including views, groups, communities, users, engine ID, traps, and notifications.
Navigation: Management → SNMP → View.

SNMP VIEW



Field	Description
View	The SNMP view name. Maximum length is 30 characters. Defines the logical grouping of MIB objects that can be included or excluded for SNMP access control.
Subtree OID	Specifies the ASN.1 subtree Object Identifier (OID) to be included in or excluded from the SNMP view. Determines which portion of the MIB hierarchy the view applies to.
View Type	Select whether the specified subtree OID is **included** or **excluded** from the SNMP view. Used to control SNMP manager access to specific MIB objects.

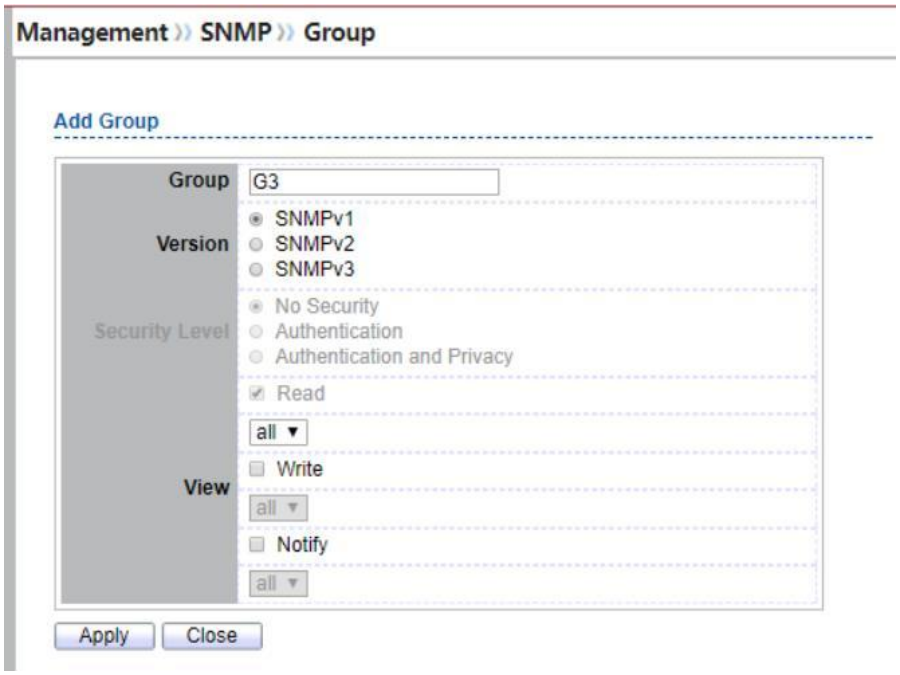
SNMP GROUP



Defines SNMP group permissions.

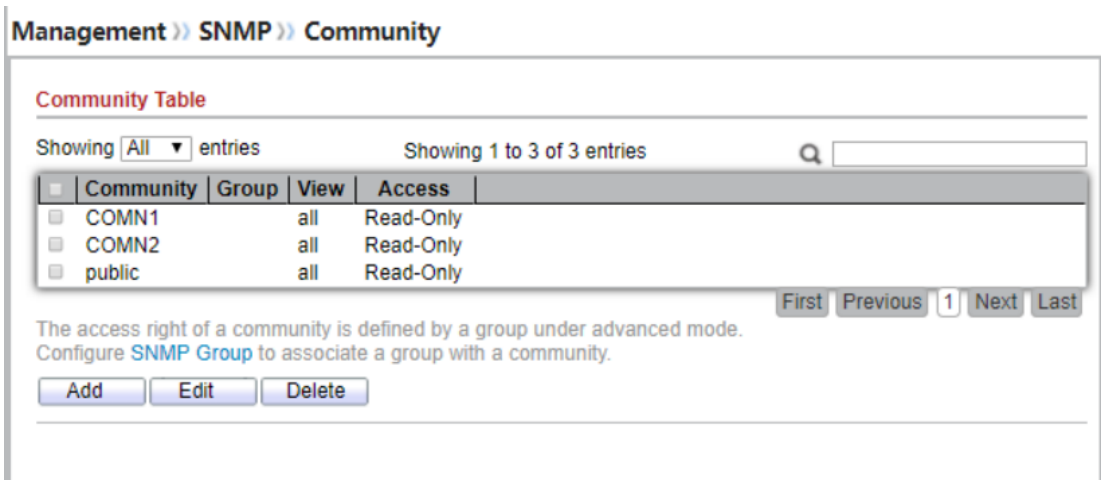
Field	Description
Group	Specify the SNMP group name. Maximum length is 30 characters. The group defines a set of access rules applied to SNMP users.
Version	Specify the SNMP version used by the group. Options include: • **SNMPv1** – SNMP Version 1. • **SNMPv2** – Community-based SNMP Version 2c. • **SNMPv3** – User-based security model (USM) with authentication and privacy options.
Security Level	Specify the SNMP security level for the group. Options include: • **No Security** – No packet authentication is performed.

	• **Authentication** – Packet authentication without encryption. • **Authentication and Privacy** – Packet authentication with encryption.
View (Read)	The SNMP view name assigned for **read** access. Determines which MIB objects the group can retrieve.
View (Write)	The SNMP view name assigned for **write** access. Determines which MIB objects the group can modify.
Notify	The SNMP view name used for **notifications**. Only traps containing objects included in this view will be sent to SNMP managers.

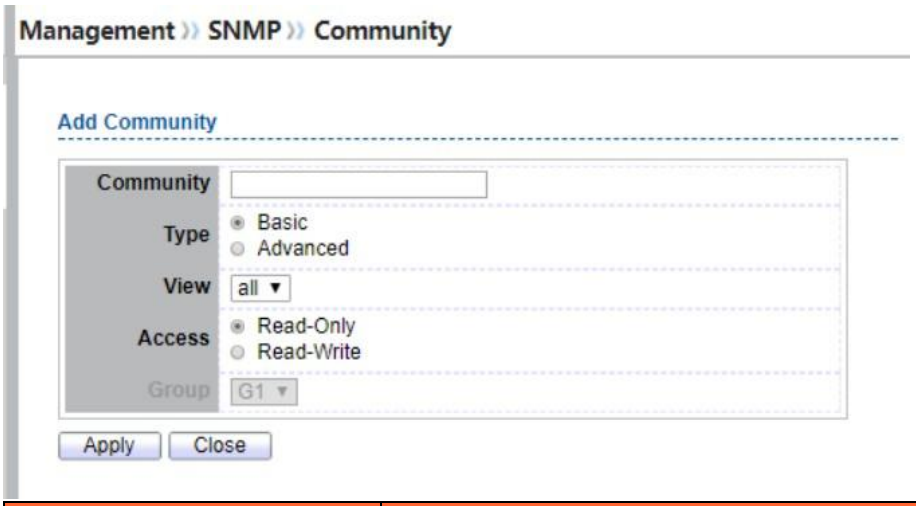


Field	Description
Security Level	Specify the SNMP security level for the user. Options include: • **No Security** – No packet authentication is performed. • **Authentication** – Packet authentication without encryption. • **Authentication and Privacy** – Packet authentication with encryption.
View (Read)	Select the **read view** name when the ***Read*** option is enabled. Determines which MIB objects the user can retrieve.
View (Write)	Select the **write view** name when the ***Write*** option is enabled. Determines which MIB objects the user can modify.
View (Notify)	Select the **notify view** name when the ***Notify*** option is enabled. Determines which MIB objects are included in SNMP notifications (traps) sent to managers.

SNMP COMMUNITY



Field	Description
Community	The SNMP community name. Maximum length is 20 characters. Defines the community string used for SNMP access.
Community Mode	Select the SNMP community mode. Options include: • **Basic** – The community directly specifies the SNMP view and access rights. • **Advanced** – The community is associated with an SNMP group, which defines access rights and available MIB objects.
Group Name	Specify the SNMP group configured via the ***snmp group*** command. The group determines which MIB objects are available to the community when operating in **Advanced** mode.
View Name	Specify the SNMP view that defines the set of MIB objects available to the community when operating in **Basic** mode.
Access Right	Select the SNMP access mode. Options include: • **Read-Only** – Allows retrieval of MIB objects only. • **Read-Write** – Allows both retrieval and modification of MIB objects.



Field	Description
Community	The SNMP community name. Maximum length is 20 characters. Defines the community string used for SNMP access.
Type	Select the SNMP community mode. Options include: • **Basic** – The community directly specifies the SNMP view and access rights. • **Advanced** – The community specifies an SNMP group, which defines the available MIB objects.
View	Specify the SNMP view that defines the set of MIB objects available to the community when operating in **Basic** mode.
Access	Select the SNMP access mode. Options include: • **Read-Only** – Allows retrieval of MIB objects only. • **Read-Write** – Allows both retrieval and modification of MIB objects.
Group	Specify the SNMP group configured by the user. The group defines the MIB objects available to the community when operating in **Advanced** mode.

SNMP User (SNMPv3)

To configure and display SNMP users, navigate to: **Management → SNMP → User**

This page allows the user to create, modify, and view SNMP users on the device. SNMPv1/v2c and SNMPv3 parameters can be configured here, including user names, group assignments, security levels, authentication methods, and privacy settings.

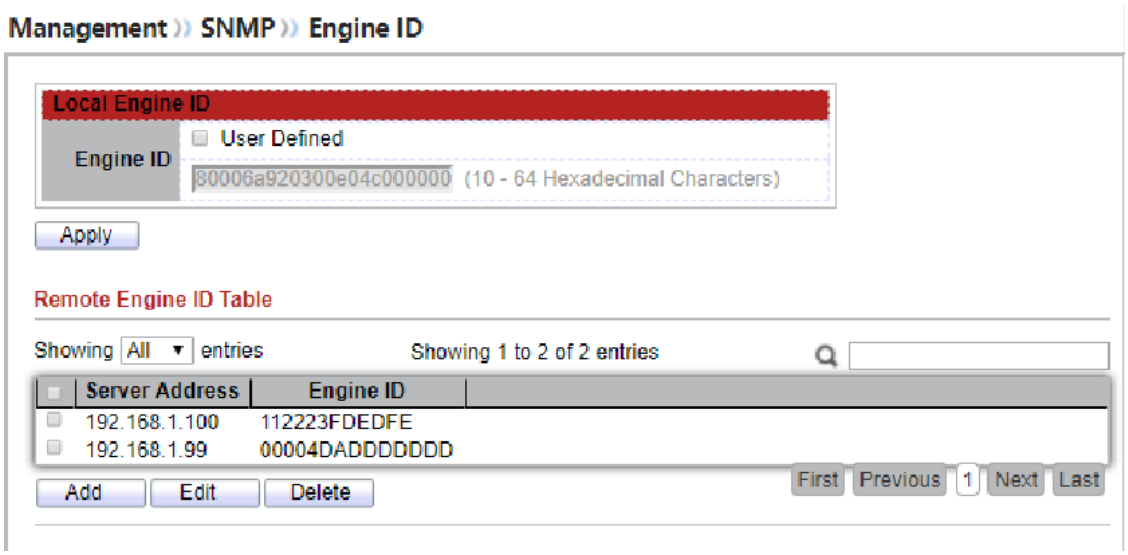
Field	Description
User	Specify the SNMP user name on the host that connects to the SNMP agent. Maximum length is 30 characters. For SNMPv1 or SNMPv2c, the user name must match the community name.

Group	Specify the SNMP group to which the SNMP user belongs. The group defines the access rights and available MIB objects for the user.
Security Level	Select the SNMP security level (privilege mode). Options include: • **No Security** – No packet authentication is performed. • **Authentication** – Packet authentication without encryption. • **Authentication and Privacy** – Packet authentication with encryption.
Authentication Method	Select the authentication protocol, available when the Security Level is **Authentication** or **Authentication and Privacy**. Options include: • **None** – No authentication required. • **MD5** – Use the HMAC-MD5-96 authentication protocol. • **SHA** – Use the HMAC-SHA-96 authentication protocol.

ENGINE ID

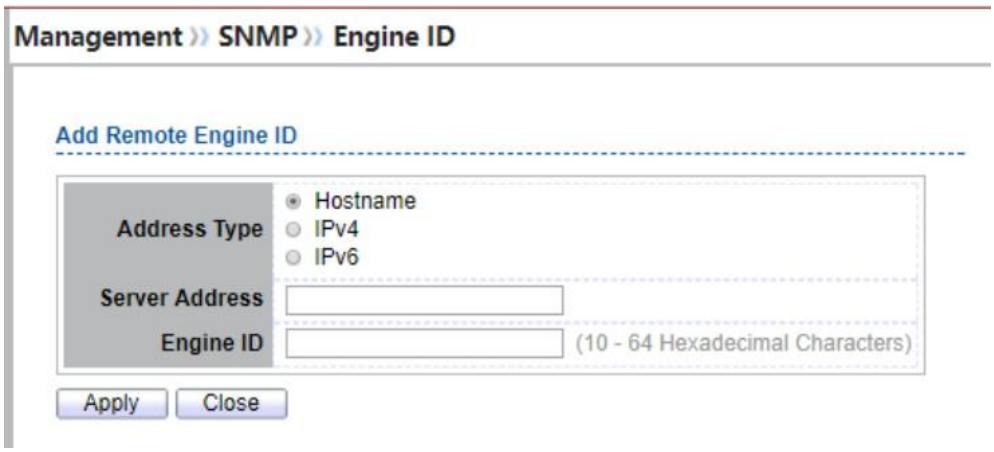
To configure and display the SNMP local and remote Engine IDs, navigate to: **Management → SNMP → Engine ID**

This page allows the user to view and configure the device's local SNMP Engine ID and specify the remote Engine ID used when communicating with external SNMP managers. The Engine ID is required for SNMPv3 operations, including authentication, privacy, and secure message processing.

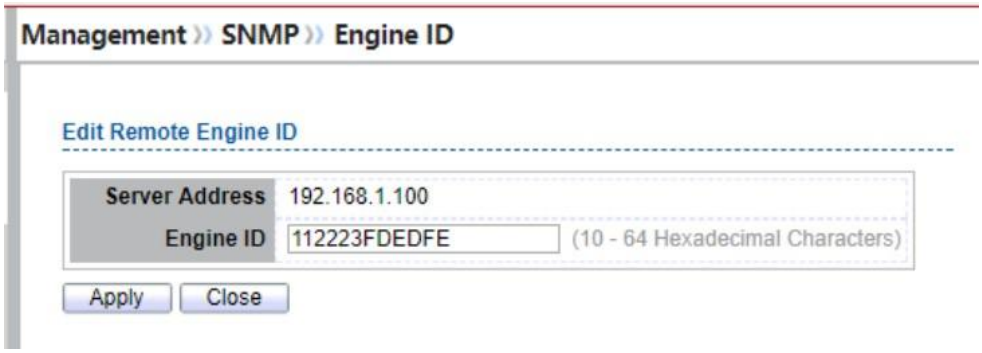


Field	Description
Engine ID	If **User Defined** is checked, the local SNMP Engine ID is manually configured by the user. If unchecked, the device uses the default Engine ID, which is generated from the device MAC address and the Enterprise ID. The user-defined Engine ID must be between **10**

	and 64 hexadecimal characters, and the total number of characters must be **even** (hex pairs).



Field	Description
Address Type	Select the address type for the remote host. Options include:**Hostname** – Use a domain name as the server address. • **IPv4** – Use an IPv4 address. • **IPv6** – Use an IPv6 address.
Server Address	Specify the remote host that communicates with the SNMP agent. Enter a valid Hostname, IPv4, or IPv6 address depending on the selected Address Type.
Engine ID	Specify the remote SNMP Engine ID. The Engine ID must be between **10 and 64 hexadecimal characters**, and the total number of characters must be **even** (hex pairs).



Field	Description
Server Address	Edit the remote host address. Enter a valid Hostname, IPv4, or IPv6 address depending on the configuration of the remote SNMP manager.
Engine ID	Specify the remote SNMP Engine ID. The Engine ID must be between **10 and 64 hexadecimal characters**, and the total number

	of characters must be **even** (hex pairs). This value uniquely identifies the remote SNMP engine for SNMPv3 communication.

TRAP EVENT

To configure and display SNMP trap events, navigate to: **Management → SNMP → Trap Event**

This page allows the user to enable or disable specific SNMP trap notifications generated by the device.

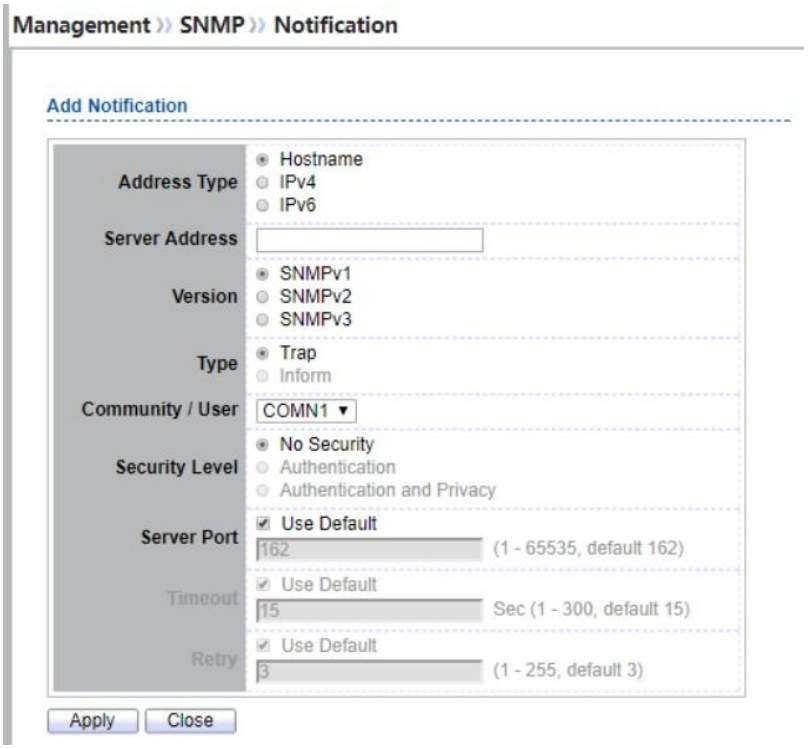
Field	Description
Authentication Failure	Generates an SNMP authentication failure trap when the community string does not match or when an SNMPv3 user authentication password is incorrect.
Link Up/Down	Generates a trap when a device port transitions to **Link Up** or **Link Down** status.
Cold Start	Generates a trap when the device performs a reboot initiated by the user (software reboot).
Warm Start	Generates a trap when the device reboots due to a power interruption (power-down reboot).

NOTIFICATION

To configure the hosts that receive SNMPv1/v2/v3 notifications, navigate to: **Management → SNMP → Notification**

This page displays all configured SNMP notification recipients and allows the user to add, edit, or remove trap/inform destinations.

Field	Description
Server Address	IP address or hostname of the SNMP trap/inform recipient.
Server Port	UDP port number used by the recipient server.
Timeout	Timeout value for SNMP informs.
Retry	Number of retry attempts for SNMP informs.
Version	Specify the SNMP notification version: • **SNMPv1** – Version 1 notification. • **SNMPv2** – Version 2 notification. • **SNMPv3** – Version 3 notification.
Type	Notification type: • **Trap** – Send SNMP traps to the host. • **Inform** – Send SNMP informs to the host.
Community/User	SNMP community or user name. For SNMPv3, this is the **user name**; for SNMPv1/v2c, this is the **community name**.
UDP Port	UDP port number used for notification delivery.
Timeout	Timeout value for SNMP informs.
Security Level	SNMP trap/inform packet security level: • **No Security** – No authentication. • **Authentication** – Authentication without encryption. • **Authentication and Privacy** – Authentication with encryption.

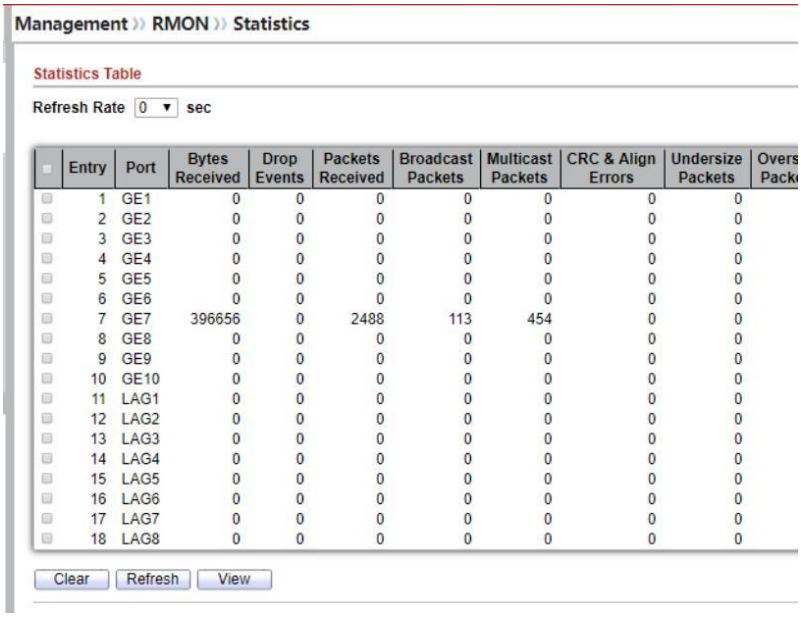


Field	Description
Address Type	Select the address type for the notification recipient: Hostname / IPv4 / IPv6.
Server Address	IP address or hostname of the SNMP trap/inform recipient.
Version	Specify the SNMP notification version: • **SNMPv1** – Version 1 notification. • **SNMPv2** – Version 2 notification. • **SNMPv3** – Version 3 notification.
Type	Notification type: • **Trap** – Send SNMP traps. • **Inform** – Send SNMP informs (not available for SNMPv1).
Community/User	SNMP community or user name. For SNMPv3, this is the **user name**; for SNMPv1/v2c, this is the **community name**.
Security Level	SNMP notification packet security level. The selected level must be **less than or equal to** the security level of the specified community/user: • **No Security** – No authentication. • **Authentication** – Authentication without encryption. • **Authentication and Privacy** – Authentication with encryption.
Server Port	UDP port number for the recipient. If **Use Default** is checked, the port is **162**; otherwise, the user specifies the value.
Timeout	Timeout value for SNMP informs. If **Use Default** is checked, the value is **15**; otherwise, the user specifies the value.
Retry	Retry count for SNMP informs. If **Use Default** is checked, the value is **3**; otherwise, the user specifies the value.

RMON

RMON provides extended monitoring capabilities for traffic statistics, history, events, and alarms.
Navigation: Management → RMON → Statistics.

RMON STATISTICS



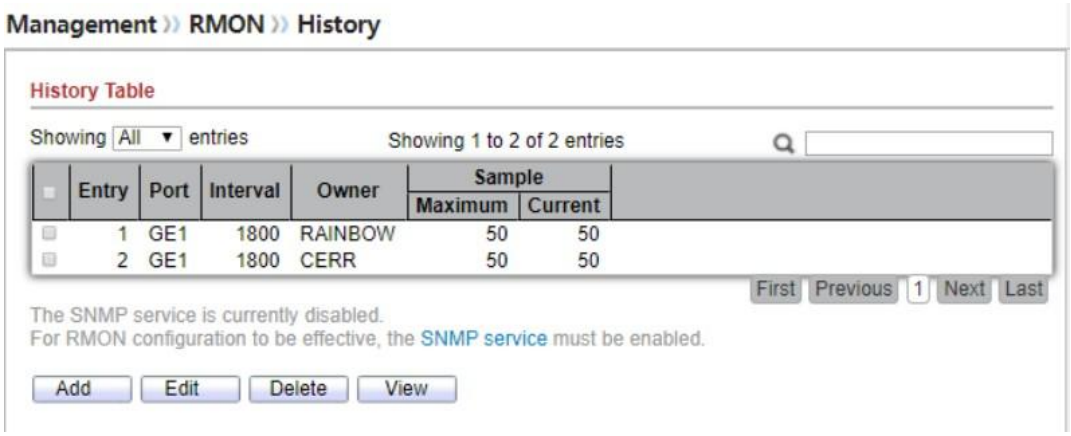
Field	Description
Port	The port for which RMON statistics are displayed.
Bytes Received	Total number of octets received, including bad packets and FCS octets, but excluding framing bits.
Drop Events	• Number of packets that were dropped.
Packets Received	• Total number of packets received, including bad packets, Multicast packets, and Broadcast packets.
Broadcast Packets	Number of good Broadcast packets received. Multicast packets are not included.
Multicast Packets	• Number of good Multicast packets received.
CRC & Align Errors	Number of CRC errors and Alignment errors detected.
Undersize Packages	Number of packets received that were smaller than 64 octets.
Oversize Packages	Number of packets received that were larger than 1518 octets.
Fragments	Number of fragments received (packets less than 64 octets, excluding framing bits, but including FCS octets).
Jabbers	Number of received packets longer than 1632 octets. Jabber packets include FCS octets and meet the following criteria: • Packet length exceeds MRU. • Packet has an invalid CRC. • No RX error event detected. If Jumbo Frames are enabled, the Jabber threshold increases to the maximum Jumbo Frame size.
Collision	Number of collisions detected on the port.
Frames of 64 Bytes	Number of received frames containing exactly 64 bytes.

Frames of 65 to 127 Bytes	Number of received frames containing 65 to 127 bytes.
Frames of 128 to 255 Bytes	Number of received frames containing 128 to 255 bytes.
Frames of 256 to 511 Bytes	Number of received frames containing 256 to 511 bytes.
Frames of 512 to 1023 Bytes	Number of received frames containing 512 to 1023 bytes.
Frames Greater than 1024 Bytes	Number of received frames containing 1024 to 1518 bytes.
Clear	Clear all RMON statistics for the selected port(s).
View	Display RMON statistics for the specified port.

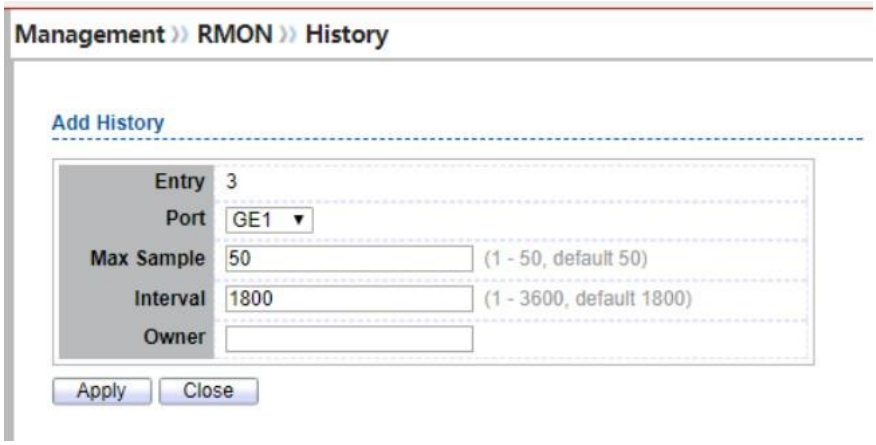
RMON History

To configure and display RMON history, navigate to: **Management → RMON → History**

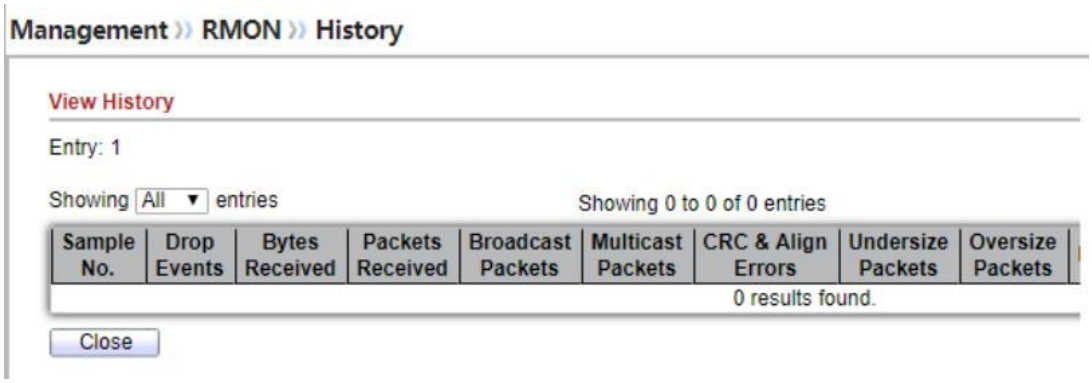
This page allows the user to create, edit, delete, and view RMON history entries. Each entry defines a sampling interval and bucket count used to record historical interface statistics.



Field	Description
Port	The port for which RMON history samples are collected.
Interval	Number of seconds for each sample interval.
Owner	Owner name of the history entry (0–31 characters).
Sample Maximum	Maximum number of buckets that can be stored.
Sample Current	Current number of buckets stored.



Field	Description
Port	Specify the port for the RMON history entry.
Max Sample	Specify the maximum number of buckets to store.
Interval	Specify the number of seconds for each sample.
Owner	Specify the owner name (0–31 characters).



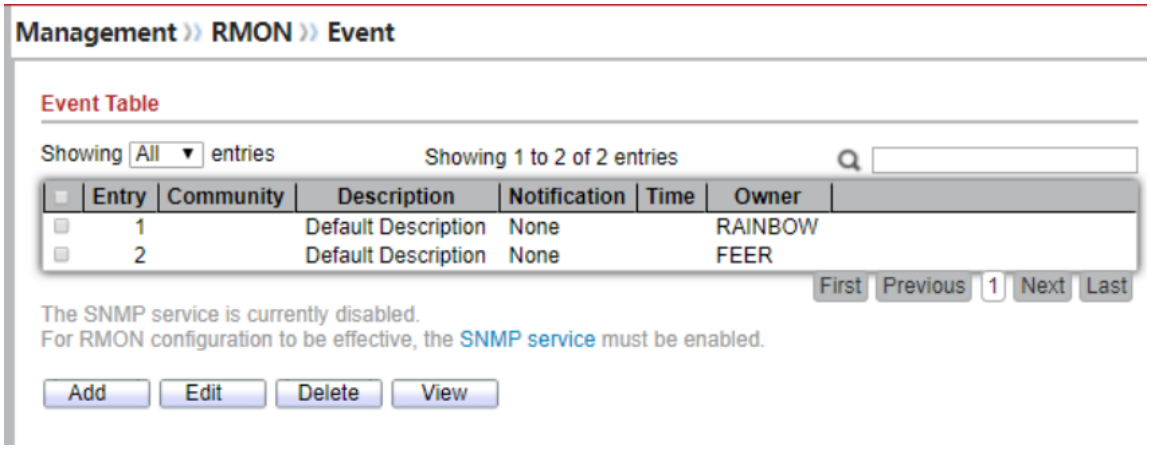
Field	Description
Port	The port for which RMON statistics are displayed.
Bytes Received	Number of octets received, including bad packets and FCS octets, but excluding framing bits.
Drop Events	• Number of packets that were dropped.
Packets Received	• Number of packets received, including bad packets, Multicast packets, and Broadcast packets.
Broadcast Packets	Number of good Broadcast packets received (Multicast packets not included).
Multicast Packets	• Number of good Multicast packets received.
CRC & Align Errors	Number of CRC and Alignment errors detected.
Undersize Packages	Number of packets received that were smaller than 64 octets.
Oversize Packages	Number of packets received that were larger than 1518 octets.
Fragments	Number of fragments received (packets less than 64 octets, excluding framing bits, but including FCS octets).

Jabbers	Number of received packets longer than 1632 octets. Jabber packets meet the following criteria: • Packet length exceeds MRU. • Packet has an invalid CRC. • No RX error event detected. If Jumbo Frames are enabled, the Jabber threshold increases to the maximum Jumbo Frame size.
Collision	Number of collisions detected on the port.
Utilization	Percentage of current interface traffic compared to the maximum traffic the interface can handle.

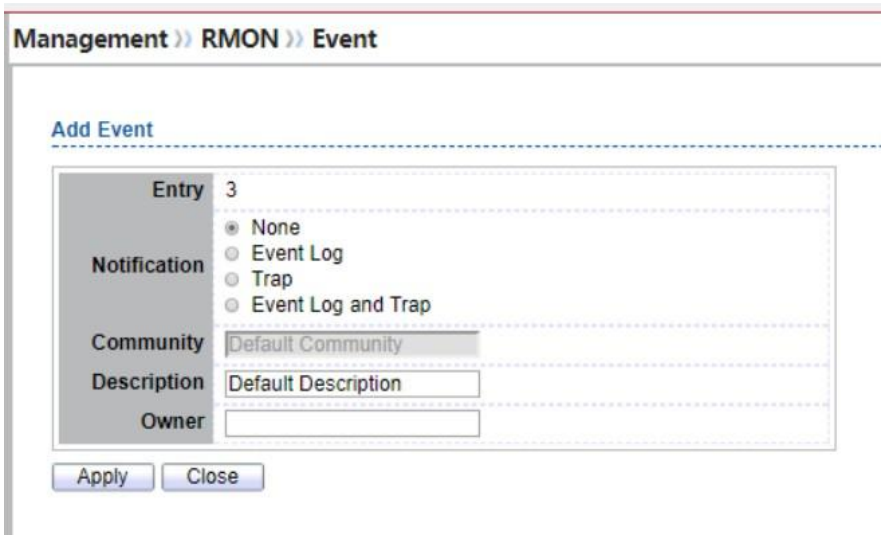
RMON EVENT

To configure and display RMON events, navigate to: **Management → RMON → Event**

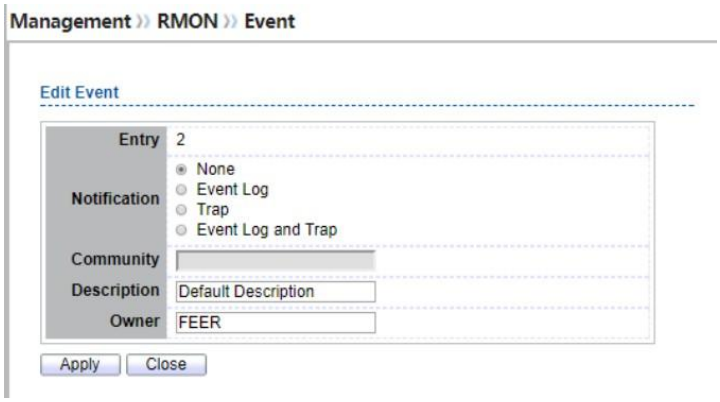
This page allows the user to define event actions, specify notification types, and review triggered event logs. Events can generate log entries, SNMP traps, or both.



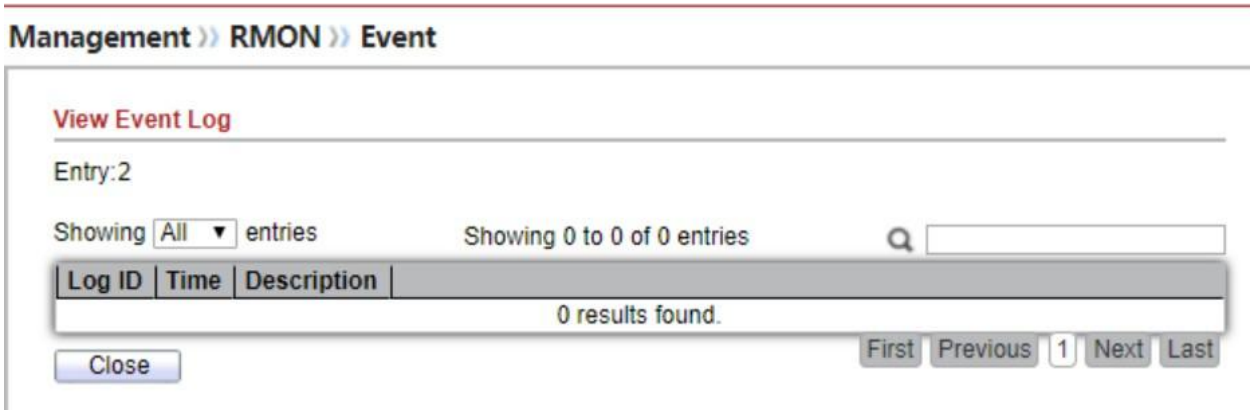
Field	Description
Community	SNMP community string used when the notification type includes **Trap**.
Description	Description of the event.
Notification	Notification type for the event: • **None** – No notification. • **Event Log** – Log the event in the RMON Event Log table. • **Trap** – Send an SNMP trap. • **Event Log and Trap** – Log the event and send an SNMP trap.
Time	The time at which the event was triggered.
Owner	Owner name for the event.



Field	Description
Community	Specify the SNMP community when the notification type is **Trap** or **Event Log and Trap**.
Description	Specify the description for the event.
Notification	Notification type for the event: • **None** – No notification. • **Event Log** – Log the event in the RMON Event Log table. • **Trap** – Send an SNMP trap. **Event Log and Trap** – Log the event and send an SNMP trap.
Owner	Specify the owner name for the event.



Field	Description
Community	SNMP community string used when the notification type includes **Trap**.
Description	Description of the event.
Notification	Notification type for the event: • **None** – No notification. • **Event Log** – Log the event in the RMON Event Log table. • **Trap** – Send an SNMP trap. • **Event Log and Trap** – Log the event and send an SNMP trap.
Owner	Owner name for the event.

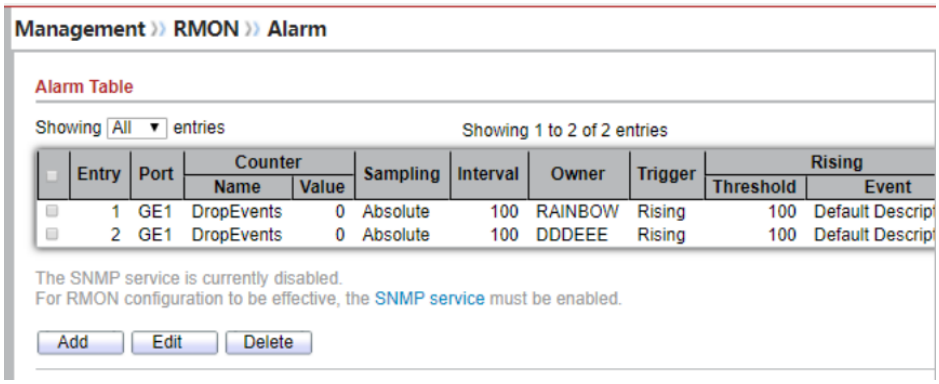


Field	Description
Log ID	Unique identifier for the event log entry.
Time	The time at which the event was triggered.
Description	Description of the event.

RMON ALARM

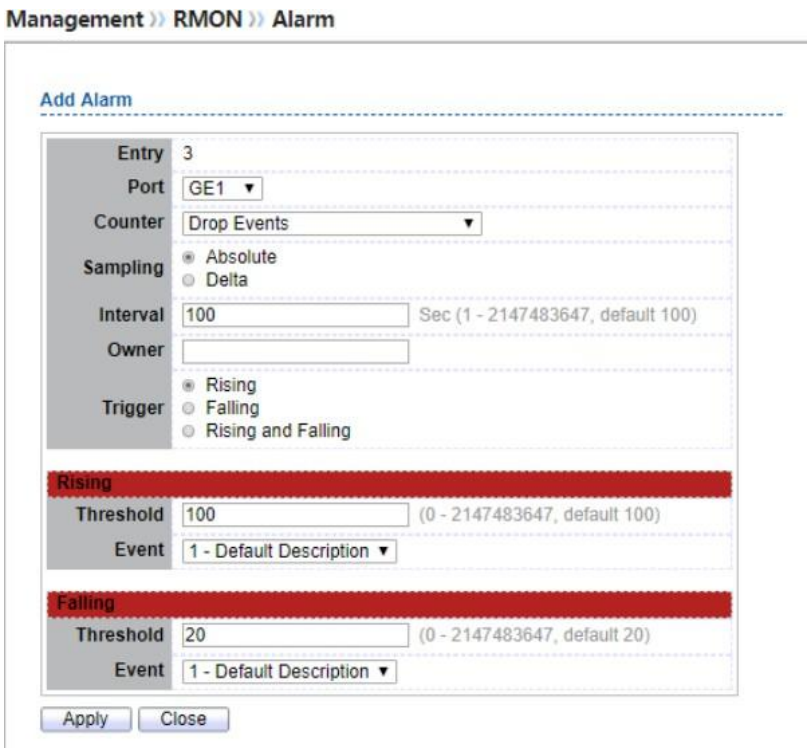
To configure and display RMON alarms, navigate to: **Management → RMON → Alarm**

This page allows the user to create threshold-based alarms for interface statistics. Each alarm monitors a selected counter and triggers rising or falling events based on configured thresholds.



Field	Description
Port	The port on which the RMON alarm is configured.
Counter	The statistic counter used for sampling. Available counters include: • **DropEvents** – Total number of dropped packet events. • **Octets (Received Bytes)** – Total number of received octets. • **Pkts (Received Packets)** – Total number of received packets. • **BroadcastPkts** – Number of received broadcast packets. • **MulticastPkts** – Number of received multicast packets • **CRCAlignError** – Number of CRC and alignment errors.

	• **UndersizePkts** – Number of undersized packets (< 64 octets). • **OversizePkts** – Number of oversized packets (> 1518 octets). • **Fragments** – Number of packet fragments (< 64 octets including FCS). • **Jabbers** – Number of jabber packets (> 1632 octets, invalid CRC, no RX error). • **Collisions** – Number of collisions detected. • **Pkts64Octets** – Number of 64-byte frames. • **Pkts65to127Octets** – Number of frames sized 65–127 bytes. • **Pkts128to255Octets** – Number of frames sized 128–255 bytes. • **Pkts256to511Octets** – Number of frames sized 256–511 bytes. • **Pkts512to1023Octets** – Number of frames sized 512–1023 bytes. • **Pkts1024to1518Octets** – Number of frames sized 1024–1518 bytes.
Sampling	Sampling method used for threshold comparison: • **Absolute** – Compares the counter value directly against thresholds at the end of each sampling interval. • **Delta** – Compares the difference between the current and previous sample values against thresholds.
Interval	Number of seconds for each sampling interval.
Owner	Owner name for the alarm entry.
Trigger	Type of event triggering (rising or falling).
Rising Threshold	Threshold value that triggers a rising event.
Rising Event	Event triggered when the rising threshold is exceeded.
Falling Threshold	Threshold value that triggers a falling event.
Falling Event	Event triggered when the falling threshold is crossed.



Field	Description
Port	The port on which the RMON alarm is configured.
Counter	The statistic counter used for sampling. Available counters include: • **DropEvents** – Total number of dropped packet events. • **Octets (Received Bytes)** – Total number of received octets. • **Pkts (Received Packets)** – Total number of received packets. • **BroadcastPkts** – Number of received broadcast packets. • **MulticastPkts** – Number of received multicast packets • **CRCAlignError** – Number of CRC and alignment errors. • **UndersizePkts** – Number of undersized packets (< 64 octets). • **OversizePkts** – Number of oversized packets (> 1518 octets). • **Fragments** – Number of packet fragments (< 64 octets including FCS). • **Jabbers** – Number of jabber packets (> 1632 octets, invalid CRC, no RX error). • **Collisions** – Number of collisions detected. • **Pkts64Octets** – Number of 64-byte frames. • **Pkts65to127Octets** – Number of frames sized 65–127 bytes. • **Pkts128to255Octets** – Number of frames sized 128–255 bytes.

	• **Pkts256to511Octets** – Number of frames sized 256–511 bytes. • **Pkts512to1023Octets** – Number of frames sized 512–1023 bytes. • **Pkts1024to1518Octets** – Number of frames sized 1024–1518 bytes.
Sampling	Sampling method used for threshold comparison: • **Absolute** – Compares the counter value directly against thresholds at the end of each sampling interval. • **Delta** – Compares the difference between the current and previous sample values against thresholds.
Interval	Number of seconds for each sampling interval.
Owner	Owner name for the alarm entry.
Trigger	Type of event triggering (rising or falling).
Rising Threshold	Threshold value that triggers a rising event.
Rising Event	Event triggered when the rising threshold is exceeded.
Falling Threshold	Threshold value that triggers a falling event.
Falling Event	Event triggered when the falling threshold is crossed.

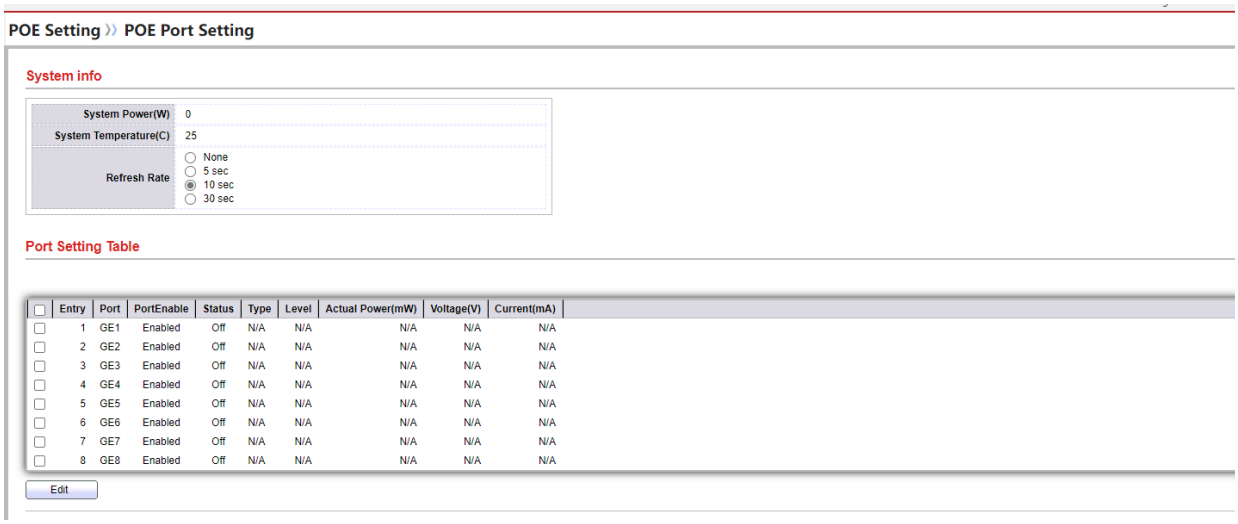
POE SETTINGS

The PoE (Power over Ethernet) pages allow you to configure power delivery behaviour for each PoE-capable port. These settings ensure that connected devices such as IP cameras, wireless access points, and VoIP phones receive stable and controlled power according to their requirements.

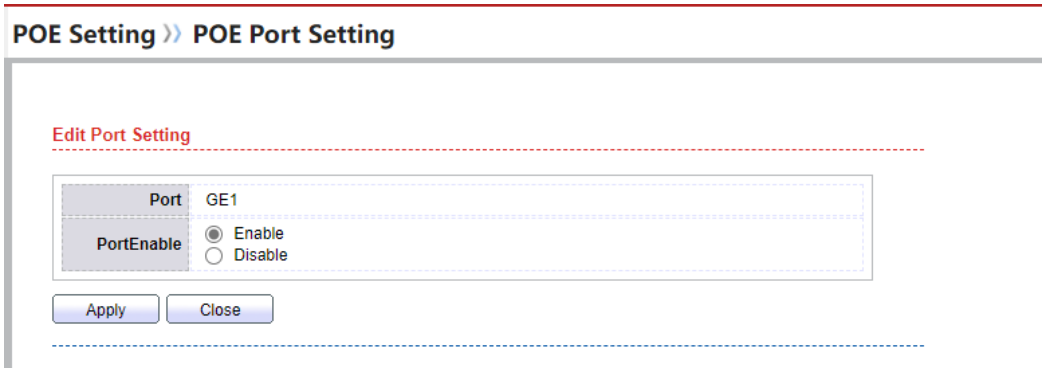
POE PORT SETTING

Use this page to configure PoE behaviour on individual ports, including power state, priority, and maximum wattage allocation.

Navigation: PoE → PoE Port Setting → PoE Port Table

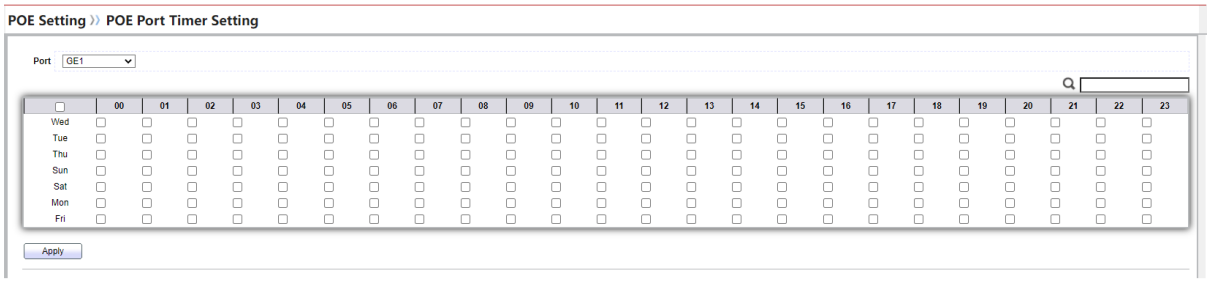


To configure a specific port, first select the port from the table. Then click the Edit button located in the table header to modify the PoE settings for that port.



POE PORT TIMER SETTING

Use this page to configure scheduled PoE behaviour, allowing ports to automatically enable or disable power at specific times. This is useful for energy savings or scheduled device resets.
Navigation: PoE → PoE Port Timer Setting



Field	Description
Port	Select the PoE port to configure the timer schedule.
Weekly Schedule Grid	A 7-day × 24-hour grid allowing PoE power scheduling. Each row represents a day (Monday–Sunday), and each column represents an hour (00–23). Check a box to enable PoE power for that hour; leave it unchecked to disable PoE power during that time.
Apply	Save and activate the configured PoE timer schedule for the selected port.

ACCESSORIES

1Gbps Fibre transmission

Part Code	Description
SIL-SFP0-01-25-X850-0-5D	1G Multimode 850nm SFP, 550m
SIL-SFP0-01-25-X131-10XD	1G Singlemode 1310nm SFP, 10km
SIL-SFP0-01-25-X131-40XD	1G Singlemode 1310nm SFP, 40km
SIL-SFP0-01-25-X155-80XD	1G Singlemode 1550nm SFP, 80km
1Gbps BiDi	
SIL-SFP0-01-25-B131-10XD	1G SM 1310nm TX FP 10km with DDM, 1550nm RX
SIL-SFP0-01-25-B155-10XD	1G SM 1550nm TX FP 10km with DDM, 1310nm RX
SIL-SFP0-01-25-B139-10XD	1G SM 1310nm TX FP 10km with DDM, 1490nm RX
SIL-SFP0-01-25-B149-10XD	1G SM 1490nm TX FP 10km with DDM, 1310nm RX
SIL-SFP0-01-25-B131-40XD	1G SM 1310nm TX DFB 40km with DDM, 1550nm RX
SIL-SFP0-01-25-B155-40XD	1G SM 1550nm TX DFB 40km with DDM, 1310nm RX
SFP to Ethernet	
SIL-SFP0-01-25-XXXT-0-1	1G RJ45 Copper SFP, 100m

Power supplies

Part Code	Description
SIL NDR-120-48 (48V 2.5A)	120W 48V 2.5A Industrial Din Rail Power Supply
SIL NDR-240-48 (48V 5A)	240W 48V 5A Industrial Din Rail Power Supply
SIL NDR-480-48 (48V 10A)	480W 48V 10A Industrial Din Rail Power Supply

TECHNICAL PARAMETERS

Power supply

Input voltage: 12V～56V (redundant dual power)

PSE Power: 0～30W

POE Pin: 1/2+, 3/6-

*** Series 5 Commercial Switches are mains powered by IEC connector**

Copper Port

Connector: RJ-45 connector

Data Rate: 10/100MbpsAuto, 10/100/1000Mbps Auto

Twisted Pair cable: Cat5 UTP cable

Transmission distance: 100 metres

Fibre Port

Connector: SC (default), FC/ST/SFP (optional)

Data Rate: 155Mbps, 1.25Gbps

Fibre Type: SM 9/125μm, MM 50/125μm、62.5/125μm

Transmission distance: 20km ~ 120km

Environment

SIL 716E8C4M & SIL 716S8C4M

Storage temperature: -40~75℃

Operating temperature: -40~75℃

Relative humidity: 5%-90%

SIL 54424MP

Storage temperature: -20~70℃

Operating temperature: 0~50℃

Relative humidity: 5%-90%

Mechanism

Enclosure: IP40, Black, Metal shell

Mounting: DIN-rail, Wall

Agreement

IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3x

IEEE 802.3af, IEEE 802.3at

STANDARDS

EMI FCC Part 15 Subpart B Class A

EN61000-4-2（ESD）

EN61000-4-3（RS）

EN61000-4-4（EFT）

EN61000-4-5（Surge）

EN61000-4-6（CS）

EN61000-4-8

EN61000-4-11

IEC60068-2-27

IEC60068-2-32

IEC60068-2-6

EN60950-1

WARNINGS

This product is only suitable for indoor applications.

Ensure that the dust caps are placed over the Fibre interface connectors when not in use.

Do not stare directly into the fibre transmitter as this is very dangerous and can cause serious damage to your eyes.

Optical fibre transceivers must be used in pairs.

Single optical fibre transceivers must be used in pairs (A, B)

A: TX1310/RX1550nm B: TX1550/RX1310nm.

TROUBLESHOOTING

If you have no connection then please check that the corresponding network devices are using the same transfer rate as the Ethernet Switch (10Mbps, 100Mbps or 1000Mbps).

If you have excessive power loss in the fibre, please check and clean the fibre connectors and ports.

RESPONSIBILITY NOTE

1. SilverNet Ltd will repair or replace any product that fails within the terms of the limited warranty in effect at the time of purchase.
2. If the product has been purchased via one of our distribution partners, it should be returned to the place of purchase as their terms may differ from ours.
3. If you use a Power Supply that is not provided by SilverNet and the device is damaged, then this is not covered under the product warranty.
4. Please follow this manual when using our power supply.
5. We will not cover any damage to our equipment or persons that is caused by any changes to this equipment without prior authorisation from us.
6. We will replace any defective equipment which fails within the warranty period.

WARRANTY

The Series 7 industrial gigabit PoE+ managed switches come with a 5-year warranty as standard. For full terms and conditions of warranty please go to **www.silvernet.com/terms-and-conditions/**

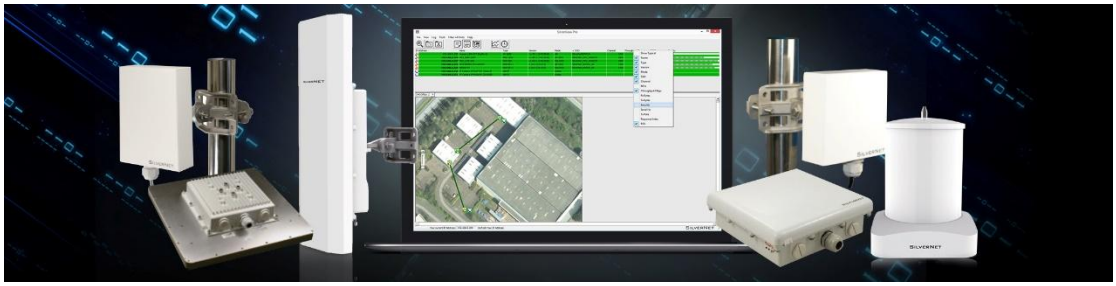
CONTACT SILVERNET

Email us at support@silvernet.com
Call our support team on **08712233067**
www.silvernet.com

COPYRIGHT INFORMATION

OTHER SILVERNET PRODUCTS

Pro Range



Industrial Network Transmission

Intelligent Wi-Fi Solutions

Industry Leading Technical Support